POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea

Cybersecurity e Gamification

Sensibilizzare sulle tematiche della Cybersecurity grazie all'utilizzo di Gamification e Human Computer Interaction nel progetto "Payload Please"

Relatori
Prof. Antonio Lioy
Prof. Andrea Atzeni

Candidato
Alessandro Rio

Anno accademico 2022-2023

Alla mia famiglia

† A mio nonno Ernesto

Sommario

Il lavoro descritto all'interno di questa tesi si concentra sull'applicazione della Gamification alle tematiche della Cybersecurity, sfruttando anche l'applicazione dei concetti di Human Computer Interaction. La problematica maggiore in questi ultimi anni, per quanto riguarda la sicurezza informatica, è la presenza del cosiddetto "anello debole" nella catena difensiva, rappresentato dall'essere umano. Uno dei punti deboli su cui gli attaccanti fanno leva per portare a buon fine il loro attacco è la natura dell'uomo di aiutare il prossimo in qualunque occasione: basta guardare quelli che sono gli attacchi più utilizzati al giorno d'oggi, ovvero Phishing e Social Engineering. Tutto questo, dunque, cosa significa? Negli anni ci sono stati miglioramenti incredibili dal punto di vista delle tecnologie utilizzate, questo è certo, ma se coloro che le devono utilizzare non sanno minimamente quale sia il loro utilizzo, risulta tutto inutile. Il lavoro di tesi parte proprio da questo punto: gli attacchi più comuni che vengono effettuati negli ultimi anni. Dopo questa presentazione si passa quindi a proporre una possibile soluzione al problema dell'anello debole, ritrovandola nell'applicazione della Gamification. Essa non è altro che l'utilizzo di elementi ludici, solitamente presenti all'interno dei videogiochi, a fini didattici e formativi in modo da permettere ai "giocatori" di apprendere dei concetti completamente sconosciuti in maniera più veloce e, soprattutto, divertente. L'analisi delle ricerche che riportano esempi di applicazione nel campo della Cybersecurity e degli elementi ludici più utilizzati, ha portato a stabilire quelli che sono gli innumerevoli vantaggi presentati dai ricercatori sull'applicazione della Gamification, al fine di diffondere la sensibilizzazione verso un argomento così complesso, come la Cybersecurity. Se però esiste un lato luminoso, ce ne sarà di sicuro uno oscuro che nascerà da esso. Infatti, l'analisi continua, prendendo in esame alcuni studi sugli effetti negativi della Gamification, i quali riportano delle problematiche abbastanza importanti, tra i tanti la possibilità di far allontanare definitivamente gli utenti dalla sicurezza informatica, causata da un errato approccio della Gamification che ha portato all'indifferenza e al rigetto dell'argomento.

La ricerca si è quindi spostata nell'individuare un elemento che potesse in qualche modo diminuire la probabilità di arrivare a questo, trovandola all'interno degli studi di Human Computer Interaction. Essi scelgono un approccio di tipo "User-Centered Design", ponendo al centro di ogni cosa l'utente e ciò di cui necessita per risolvere le proprie problematiche. Il motivo che spinge ad approcciarsi al processo della HCI è quello di limitare i fallimenti del prodotto finale grazie ai vari passaggi da seguire per arrivarci. Tramite l'applicazione della Human Computer Interaction alle tematiche della Gamification, è possibile limitare gli errori di un suo utilizzo nella sensibilizzazione alle tematiche della sicurezza informatica. Infatti, quello su cui si va a lavorare effettivamente sono i bisogni rilevati durante la fase iniziale, denominata "Needfinding", eseguita all'interno di questo lavoro di tesi attraverso un questionario preparato per analizzare le conoscenze base sulla Cybersecurity delle persone a cui è stato fornito, le loro opinioni sulle maggiori problematiche di questo argomento e le loro preferenze sui vari elementi ludici. Il target scelto per l'analisi di questi fattori, tuttavia, risulta essere molto ristretto. Infatti, sono soltanto tre le categorie di "personas" che sono state prese in considerazione all'interno della tesi, le quali però rappresentano la prima linea di difesa contro gli attaccanti informatici: gli esperti di Cybersecurity, gli studenti universitari dell'orientamento di Cybersecurity e, infine, i lavoratori non esperti di Cybersecurity ma che necessitano di una formazione basilare, al fine di non trovarsi inermi davanti ad eventuali attacchi. Una volta creato il questionario e raccolte le risposte di circa sessanta persone, si è passato all'analisi dei loro bisogni descritti al suo interno e alle preferenze sugli elementi ludici. A questo punto è stato possibile dare vita, seppure solamente in forma cartacea, al primo prototipo di "Payload Please": il suo scopo è quello di testare le conoscenze delle persone

a cui viene somministrato, attraverso l'utilizzo di simulazioni di attacchi e di sensibilizzazione verso alcune tematiche della sicurezza informatica, cercando di non rendere mai la cosa troppo facile da catalogare come l'una o l'altra. Il suo funzionamento è leggermente diverso dagli esempi analizzati all'interno dei paper sull'applicazione della Gamification alla Cybersecurity; infatti, la sua simulazione si articola in due fasi:

- In primo luogo, gli utenti a cui viene sottoposta la simulazione sono completamente ignari di quello che sta succedendo. Non essendo a conoscenza di Payload Please, è possibile analizzare le reazioni più genuine di ognuno di loro, cercando di sfruttare il più possibile il concetto di cooperazione durante i vari test. Alla fine della simulazione viene rivelata a tutti la verità e si descrivono tutti i bonus e malus guadagnati, ovvero le azioni corrette e sbagliate nel rispondere alle diverse casistiche presentate, con un punteggio finale e che verrà utilizzato per stilare una classifica;
- La seconda fase viene proposta dopo che è stata svelata a tutti la presenza di Payload Please. Nel caso in cui l'ambiente dove è stato applicato sia idoneo a livello di stress ed impegni, si passa a riproporre la simulazione con argomenti diversi che ricompensano il vincitore del nuovo test con un premio. Qui la cooperazione risulta ancora disponibile, niente e nessuno la vieterà mai, ma quello in cui si sfocerà quasi sicuramente è la competizione. Sono stati analizzati anche alcuni paper che riportavano come essa, nelle giuste dosi, possa spronare a dare il meglio e superare i propri limiti, cosa tra l'altro anche descritta da alcuni partecipanti al questionario sulla Cybersecurity e la Gamification.

Dopo la prima fase di testing su carta, sono state raccolte le opinioni e i possibili miglioramenti dagli stessi partecipanti, per poi arrivare alla creazione di un primo prototipo informatico: esso sfrutta alcuni programmi come Nexphisher e PhishMailer per la creazione di siti falsi, i quali simulano attacchi di phishing. Inoltre, sono state create due tipologie di form di raccolta dati: nel primo ci si concentra sulla sensibilizzazione su tematiche di Cybersecurity, come autenticazione biometrica o a multifattore, nel secondo si cerca di appropriarsi di informazioni personali che possono essere sfruttate per possibili attacchi di brute force, con lo scopo di scoprire la password della vittima. Il mezzo utilizzato in questo primo prototipo per la diffusione dei vari test di Payload Please è la e-mail, richiesta agli utenti per ricevere le varie simulazioni e analizzare i loro comportamenti. Per concludere il lavoro, sono stati riportati altri cambiamenti possibili sulla base dei test informatici eseguiti che porterebbero ad un ulteriore miglioramento del sistema di Payload Please, quali l'inserimento nella classifica finale di una descrizione di casi reali per ogni simulazione proposta all'utente, la partecipazione di personale tecnico, per rendere i test più realistici, e l'aggiunta di altri argomenti nella simulazione (GDPR, VPN, firewall, computer forensics) per coprire un panorama più ampio della Cybersecurity. Durante lo svolgimento delle varie modalità di test per Payload Please, ci si è preposti degli obiettivi e, grazie all'aiuto dei partecipanti, è stato possibile raggiungere alcuni di essi. Il fattore del divertimento è stato uno di quelli con il miglior risultato, cogliendo in pieno l'obiettivo della Gamification e rendendo le simulazioni molto più efficaci. Altro elemento che ha avuto un risvolto positivo è stato "l'elemento sorpresa" messo in atto durante la prima fase dei test, il quale ha evidenziato la genuinità delle azioni degli utenti e fatto emergere le loro principali lacune: molti di loro, infatti, hanno confessato che i malus ricevuti alla fine corrispondevano ad errori a cui erano soliti incappare. Tra le cose meno efficaci c'è da annoverare l'elemento competitivo: esso, infatti, non è risultato essere particolarmente determinante ai fini delle simulazioni, lasciato a margine rispetto ad altri elementi ludici come la cooperazione o il sistema di punteggi (bonus e malus), fattori questi risultati, invece, fruttuosi. Come possibile implementazione futura è stata lasciata la creazione del prodotto finito, il quale dovrebbe sfruttare alcuni programmi in più rispetto alla versione precedente e che non è stato possibile utilizzare momentaneamente a causa di alcuni problemi esterni e, nell'immediato, impossibili da risolvere, lasciando uno spiraglio aperto verso l'ingresso nel mondo della realtà virtuale e aumentata, in modo da creare un'esperienza più "futuristica". La base però rimane sempre la stessa: sensibilizzare gli utenti sulle tematiche della sicurezza informatica e su come riconoscere i possibili attacchi, in modo da eliminare una volta per tutte l'etichetta di anello debole, ormai da troppo tempo legata all'essere umano.

Ringraziamenti

Per prima cosa colgo l'occasione per esprimere la mia gratitudine nei confronti del Professore Antonio Lioy e del Professore Andrea Atzeni, i quali mi hanno permesso di poter lavorare su una tematica così attuale e importante per il percorso di studi che ho scelto e, soprattutto, per il supporto durante la stesura della tesi.

Vorrei poi ringraziare tutti coloro che hanno speso parte del loro tempo nel rispondere al mio questionario per condividere le loro opinioni e preferenze, elementi che sono stati fondamentali per il proseguimento del lavoro.

Un ringraziamento speciale va ai ragazzi e ragazze che si sono offerti per provare prima il prototipo di carta e successivamente quello informatico. Le loro critiche costruttive sono state d'aiuto, in quanto hanno permesso di migliorare il prodotto durante le varie fasi di testing.

Colgo l'occasione per ringraziare la mia famiglia, sempre pronta a sostenermi e a diventare la mia ancora di salvezza nei momenti più difficili della mia carriera universitaria e non; i miei amici di sempre, che sono riusciti a migliorare anche le mie giornate più negative e ad essere presenti nel momento del bisogno.

Infine, un saluto e un abbraccio ai miei due nonni che non ci sono più, sono sicuro che in questo momento siano particolarmente orgogliosi e felici del traguardo che sono riuscito a raggiungere anche grazie al loro supporto.

Indice

Capitolo 1

Gli attacchi più comuni

In questa parte si andranno ad analizzare quelle che sono le principali minacce informatiche che colpiscono sia privati cittadini che aziende e verranno inquadrati i metodi che vengono utilizzati per compiere tali atti. A riprova del fatto che l'uomo venga ancora oggi sfruttato come "anello debole" sono i mezzi più utilizzati dagli attaccanti [1]: phishing via e-mail, spear-phishing, social engineering, tutti attacchi che riconoscono in esso il punto perfetto dove mettere radici per diffondersi poi a macchia d'olio. Anche se si dovesse avere il software, l'hardware e le patch appropriate in funzione, il fattore umano lascia comunque un punto scoperto per l'accesso, portandolo ad essere il mezzo di trasmissione più utilizzato. Andiamo quindi a sviscerare quelli che sono gli attacchi più comuni.

1.1 Ogni viaggio inizia con un solo passo

Lo studio presente in questa tesi fonda le sue radici su un obiettivo fisso: bisogna rendere le persone più consapevoli di quanto la sicurezza informatica sia ormai fondamentale per la nostra società. Il numero degli attacchi continua ad aumentare e la pandemia di Covid-19 non ha fatto altro che accelerare la sua crescita, grazie anche all'utilizzo sempre più diffuso dello smart working per contenere il contagio. Ma perché tutta questa enfasi nella Cybersecurity? Se da un lato gli attaccanti sono sempre di più, dall'altro lato ci sono sempre più modi per contrastarli: così come per il virus abbiamo avuto la diffusione di vari vaccini per evitare il contagio, anche per la sicurezza informatica abbiamo dei mezzi per difenderci sempre migliori. Hardware molto costosi in alcuni casi e all'avanguardia, questo è vero, ma cosa succede quando ad utilizzarli è una persona che non ha la più pallida idea di come funzionino? Questo è il primo pensiero degli attaccanti: se non si può attaccare la parte macchina, passiamo alla parte umana, più debole ed esposta. Questo non è altro che la stessa cosa che è successa con il virus, il quale ha iniziato a presentare diverse varianti che in qualche modo andavano a superare le difese create tramite i vaccini. La più grande differenza tra l'uomo e il freddo acciaio, oltre al fatto che uno è un essere vivente e l'altro no, è la capacità di provare emozioni ed essere facilmente raggirabili da esse. Per questo motivo ancora oggi si effettua una correlazione tra l'uomo e l'anello debole della catena della sicurezza informatica, punto dolente da molti anni ormai. Se però da una parte possediamo le emozioni che ci portano ad essere "deboli" da questo punto di vista, dall'altra abbiamo anche il libero arbitrio, il quale ci permette di scegliere di non rimanere in questa situazione e di voltare pagina. È necessario diffondere una maggiore consapevolezza degli argomenti della Cybersecurity, in modo da contenere l'enorme macchia d'olio diffusa dagli hacker e in questo sono in aiuto la Gamification e la Human Computer Interaction. Grazie ad esse, infatti, è possibile insegnare un concetto alle persone, anche in maniera divertente, con la prima e rendere i sistemi di sicurezza più accessibili a tutti e meno complicati con la seconda. I tentativi di adempiere all'arduo compito di cambiare la mentalità delle persone a riguardo è già stato avviato da tempo, esempi come quello proposto da Kaspersky [17] al giorno d'oggi ne esistono molti ed ognuno di essi ha raccolto grande approvazione. Ci sono anche le problematiche da trattare della Gamification, questo è ovvio, ma con l'applicazione della Human Computer Interaction e dei suoi principi, è possibile la

creazione di un sistema "User-Centered" che tenga conto delle difficoltà degli utenti e che possa andar a sopperire agli aspetti negativi della Gamification [23]. Quella che si avvia non è di certo un processo breve, bensì si rivela essere molto lungo e tortuoso a volte, ma si sa: ogni grande viaggio inizia con un solo passo, questo non è altro che il primo di molti altri.

1.2 Il Phishing

Il Phishing [2] è un tipo di truffa effettuata su internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso fingendosi un ente affidabile. Solitamente il phishing avviene tramite e-mail o attraverso un altro tipo di comunicazione fraudolenta, allo scopo di attirare la vittima nella propria trappola. Il messaggio viene creato il più veritiero possibile, quindi anche il mittente stesso deve essere credibile agli occhi della vittima, la quale, nel caso in cui venga ingannata con successo, potrebbe fornire all'attaccante informazioni riservate, spesso inserite all'interno di un sito web truffa. Alcune volte, oltre alla diffusione di questi dati, si può avere anche l'installazione di un malware all'interno del computer del malcapitato. Un attacco di phishing può manifestarsi sotto varie forme, esistono molteplici tecniche che i criminali informatici utilizzano per realizzare i loro schemi [3]:

E-mail Phishing: probabilmente la tipologia più comune di phishing, che spesso comporta una tecnica "spray and pray", ovvero spara e prega, in cui gli hacker impersonano un'identità o un'organizzazione legittima e inviano e-mail di massa a tutti gli indirizzi che riescono ad ottenere. Queste e-mail spesso informano il destinatario che un account personale è stato compromesso e che deve rispondere immediatamente. L'obiettivo è suscitare una determinata azione da parte della vittima, come fare clic su un collegamento dannoso che porta a una pagina di accesso falsa. Dopo aver inserito le proprie credenziali, le vittime purtroppo consegnano le proprie informazioni personali direttamente nelle mani del truffatore.

Smishing: si tratta di phishing che viene messo in pratica tramite SMS e agisce in modo analogo all'attacco classico via e-mail: gli aggressori inviano messaggi da quelle che sembrano fonti legittime (come aziende fidate) che contengono collegamenti dannosi. I link potrebbero essere camuffati da codice coupon (20% di sconto sul tuo prossimo ordine ad esempio) o un'offerta per vincere un premio come i biglietti per un concerto.

Vishing: noto anche come phishing vocale, è simile allo smishing in quanto un telefono viene utilizzato anche in questo caso come veicolo per un attacco, ma invece di sfruttare le vittime tramite messaggio di testo, lo si fa attraverso una telefonata. Una chiamata vishing spesso trasmette un messaggio vocale automatico da quella che dovrebbe sembrare un'istituzione legittima, come una banca o un ente governativo. Gli aggressori solitamente informano la vittima della presenza di un debito di una grande quantità di denaro, che l'assicurazione auto è scaduta o che la carta di credito ha attività sospette che devono essere risolte immediatamente.

Pharming: proviene dalla combinazione tra "phishing" e "farming", coinvolge gli hacker che sfruttano i meccanismi della navigazione Internet per reindirizzare gli utenti a siti Web dannosi, spesso prendendo di mira i server DNS (Domain Name System). Gli hacker che si dedicano al pharming riescono così a reindirizzare le vittime verso siti Web fraudolenti con indirizzi IP falsi.

Purtroppo, non esiste alcuna tecnologia di sicurezza informatica che sia in grado di prevenire attacchi di phishing, una delle modalità migliori per proteggersi dal caderne vittima è studiare esempi di phishing in azione. Ma, in generale, è importante riconoscere questi segnali di avvertimento per scoprire un potenziale attacco:

- Un'e-mail che chiede di confermare le informazioni personali che sembra autentica ma è totalmente inaspettata, è probabile che si tratti di una fonte inaffidabile;

- Le parole errate, la grammatica scadente o uno strano modo di esprimersi sono un segnale d'allarme immediato di un tentativo di phishing;
- Se un messaggio sembra essere stato progettato per far impaurire la vittima e agire immediatamente, è bene procedere con cautela poiché essa risulta essere una manovra comune tra i criminali informatici;
- Messaggi imprevisti che richiedono l'apertura di un allegato sconosciuto;
- Se si viene contattati per quello che sembra essere un affare irripetibile, probabilmente è falso.

1.3 I Malware

Si è parlato della possibilità, grazie ad un attacco phishing, di installare sul dispositivo della vittima un malware, ovvero un software malevolo che descrive un codice/programma dannoso per il sistema. Ostili, invasivi e volutamente maligni, i malware cercano di invadere, danneggiare o disattivare computer, sistemi, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni del dispositivo [4]. Il loro scopo è quello di lucrare illecitamente a spese degli utenti e, sebbene non possano danneggiare gli hardware fisici di un sistema o le attrezzature di rete, possono rubare, criptare o eliminare i dati, alterare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione. I malware non sono prevedibili, ognuno colpisce con una diversa modalità di attacco, da quelli più subdoli e furtivi a quelli più dirompenti e violenti. I "sintomi" che si possono avvertire a causa di questi software malevoli sono ad esempio:

- Il computer funziona più lentamente. Uno dei principali effetti dei malware è la riduzione della velocità del sistema operativo, sia nella navigazione su Internet che nel semplice utilizzo delle applicazioni.
- Un'ondata di irritanti annunci pubblicitari, che non dovrebbe comparire, riempie lo schermo. La presenza di pop-up imprevisti è il sintomo tipico di un'infezione malware. Si tratta di un malware noto con il nome di adware. I pop-up, inoltre, spesso nascondono altre minacce malware. Insomma, se dovesse comparire una scritta come: "Congratulazioni, hai vinto una lettura gratuita dei tarocchi" in un pop-up, è meglio evitare di fare clic. Per quanto gratuito sia il premio promesso dall'annuncio, il prezzo da pagare si rivelerà molto alto.
- Il sistema continua a chiudersi, bloccarsi o mostrare una schermata blu di errore (BSOD), che talvolta viene visualizzata sui dispositivi Windows in seguito a un errore irreversibile.
- Si nota una misteriosa perdita di spazio su disco, probabilmente legata a un malware abusivo che si nasconde nel disco rigido. Al contrario, l'attività del sistema su internet subisce un inspiegabile aumento.
- L'utilizzo delle risorse di sistema è insolitamente elevato e la ventola del computer inizia a girare all'impazzata; sono tutti segni di attività malware che sfruttano le risorse di sistema in background.
- La homepage del browser cambia senza alcuna autorizzazione. Allo stesso modo, alcuni link indirizzano a pagine web indesiderate. Generalmente, questo succede quando si fa clic su quei pop-up che scaricano software indesiderati. Allo stesso modo, il browser potrebbe subire un forte rallentamento.
- Toolbar, estensioni o plugin compaiono inaspettatamente nel browser.
- L'antivirus smette di funzionare e diventa impossibile aggiornarlo, il che lascia il sistema alla mercé dell'infido malware che l'ha disabilitato.
- A volte, invece, si verificano degli attacchi malware dolorosamente evidenti, volutamente plateali. È il famoso caso dei ransomware, che si presentano all'utente e lo informano di aver preso possesso dei suoi dati, chiedendo un riscatto per la restituzione dei file.

- Anche se tutto sembra funzionare correttamente, non è il caso di compiacersi, perché non sempre "nessuna notizia è una buona notizia". I malware più potenti possono nascondersi in profondità, conducendo i propri sporchi affari senza sollevare sospetti mentre rubano password, si appropriano di file sensibili o utilizzano un PC per diffondersi su altri computer.

Ovviamente di malware ne esistono di diversi tipi, ognuno dei quali si comporta ed agisce in modi diversi [5]:

Worm: sono un tipo di malware in grado di replicarsi da un computer all'altro, senza infettare altri oggetti presenti nel medesimo computer. Possono diffondersi attraverso le reti sfruttando le vulnerabilità di ciascun dispositivo. Al pari di altri tipi di malware, i worm possono danneggiare il dispositivo utilizzando tutta la larghezza di banda e recapitando payload di codice dannoso.

Adware: abbreviazione di advertising-supported software (software sovvenzionato da pubblicità). Talvolta l'utente può fornire per errore il proprio consenso al download di un programma adware, responsabile della comparsa sul browser di annunci pop-up illegittimi. A volte gli hacker creano pacchetti malware unendo lo spyware all'adware, rendendo così quest'ultimo particolarmente pericoloso. Bisogna sempre assicurarsi quindi di non cliccare mai su annunci pubblicitari online che appaiono sospetti.

Spyware: si differenzia dalle altre categorie di malware in quanto non riflette una definizione di natura tecnica. Si tratta invece di un termine generico assegnato a programmi malevoli di vario tipo, quali adware, riskware e Trojan. Lo spyware è in grado di monitorare le attività online della vittima, osservare quali tasti sta premendo e raccogliere i suoi dati personali.

Virus: è un tipo di malware capace di auto-replicarsi e diffondersi in tutto il sistema informatico preso di mira.

Bot: vengono creati per eseguire in modo automatico operazioni specifiche. Alcuni bot presentano funzionalità e scopi del tutto legittimi, ad esempio, si possono utilizzare per eseguire la scansione dei siti web e raccogliere il loro contenuto per la successiva indicizzazione nei motori di ricerca. Se usati con intenti malevoli, i bot possono raccogliere e sottrarre i dati personali dell'utente, che poi vengono sfruttati dai cybercriminali.

Ransomware: blocca l'accesso al dispositivo o tiene in ostaggio i file, a scopo ricattatorio. Gli hacker utilizzano il ransomware per richiedere il pagamento di un riscatto da parte dell'utente, prospettando la possibilità, per quest'ultimo, di acquisire nuovamente il controllo del proprio dispositivo, cosa che nella maggior parte dei casi non avverrà.

Rootkit: è un programma utilizzato dai criminali informatici per eludere il rilevamento mentre ottengono l'accesso non autorizzato al computer-vittima. Gli hacker si avvalgono dei rootkit per accedere da remoto e sottrarre i dati dell'utente.

Cavallo di Troia: con questo termine, solitamente abbreviato in Trojan, si indica un malware che si camuffa in veste di file del tutto normale, ma esegue poi alcune operazioni dannose sul computer. Quando si scarica un Trojan è ben difficile rendersi conto che, in realtà, si sta aprendo la strada all'installazione di un pericoloso malware. Essi sono in grado di eseguire una vasta gamma di funzioni dannose, tra cui il furto dei dati.

1.4 Social Engineering

Con social engineering [6] si intende l'arte di manipolare le persone con lo scopo di "iniettare" il malware all'interno di un'organizzazione, superando qualsiasi sistema di controllo e ottenendo così informazioni riservate. Questa forma di minaccia, detta anche "human hacking", è una delle tecniche più utilizzate per carpire dati sensibili e informazioni personali a scopo fraudolento. A metà tra psicologia e ingegneria, è considerata una manipolazione della tendenza umana di fidarsi e di rilasciare informazioni che a noi possono sembrare di poco conto, ma che per l'attaccante si

rivelano molto importanti. Anche un solo bit rilasciato può creare una falla nel sistema. Essendo che questa tecnica non fa uso di particolari strumenti, non esiste antivirus o firewall che può difenderci da questa subdola minaccia, proprio perché l'attacco ricade su noi uomini e sulla nostra tendenza a fidarci del prossimo. Nello specifico, solitamente le tipologie di attacco di questo tipo sono riconducibili a tre categorie:

- Human based, basate sul contatto diretto tra attaccante e vittima;
- Computer based, che presuppongono l'utilizzo di strumenti informatici e competenze tecniche;
- Mobile based, sottoinsieme di quelle computer based e che riguarda la diffusione capillare delle tecnologie mobile che veicolano i malware.

Esistono poi diverse tattiche per poter mettere in pratica le categorie appena descritte:

Impersonation: si fa uso di una falsa identità con l'obiettivo di ingannare la propria vittima al punto di convincerla a consentire l'accesso in totale fiducia ad aree riservate, informazioni private o a sistemi informativi aziendali. Può sfruttare diverse tattiche di persuasione psicologica come il Tailgating, ovvero sfruttare l'entrata di una persona autorizzata per poter accedere prima che si chiuda l'ingresso, o il Piggybacking, ovvero tentare con l'empatia e riuscendo a persuadere una persona ad aprire questa porta.

Vishing: sottocategoria di Impersonation, consente di effettuare un attacco sfruttando la comunicazione telefonica, lasciando così l'attaccante nascosto agli occhi della vittima e approfittando del poco tempo solitamente messo a disposizione durante una conversazione telefonica per spingere la persona a dare le informazioni che si stavano cercando.

Reverse Social Engineering (RSE): è una tecnica molto particolare per il modus operandi che si applica. Per prima cosa, l'attaccante crea la situazione disfunzionale (fase di sabotaggio), successivamente l'hacker si presenta come il risolutore del problema (fase di interazione) ed infine si arriva ad un contatto attivo con la vittima, dove sarà proprio quest'ultima a rivolgersi a lui spontaneamente, facilitando così il buon esito dell'attacco.

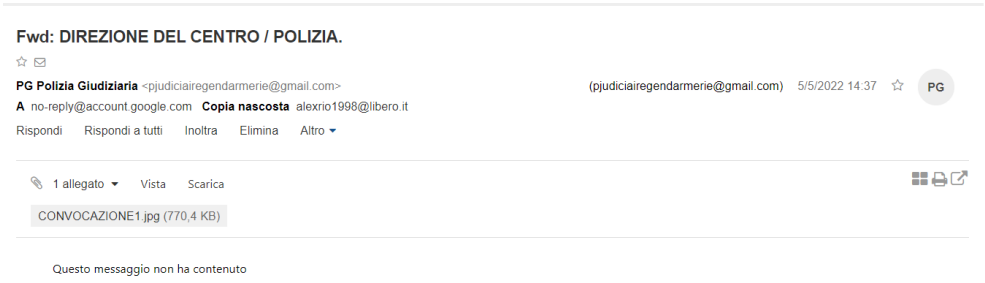
1.5 Un classico esempio di Phishing

Il corretto uso del Social Engineering è fondamentale affinché un attacco phishing vada a buon segno, sono due cose quindi complementari tra di loro. Quello che verrà presentata adesso è un tipico esempio di attacco e-mail phishing, andando quindi a sviscerarne le caratteristiche appena descritte e come riconoscerlo nel pratico. In data 05/05/2022 nella mia casella di posta privata è apparsa una mail nella sezione posta in arrivo un po' strana come è possibile notare nella Fig. 1.1.

Figura 1.1: La mail presente all'interno della sezione "Posta in arrivo".

Due cose subito saltano all'occhio: il mittente, tale "PG Polizia Giudiziaria" e l'oggetto della mail dove viene riportata la scritta "Fwd", la quale sta ad indicare che tale elemento è stato inoltrato, probabilmente non per la prima volta. Spinti dalla curiosità, si può essere tentati di aprire tale mail, anche perché inconsciamente si pensa che sia una cosa importante leggendo il nome della polizia. L'interno della mail risulta essere come mostrato in Fig. 1.2

Una mail completamente vuota contenente soltanto un allegato con un nome strano: "CONVOCAZIONE1.jpg". A questo punto si dovrebbe avere già l'idea ben chiara che quella che stiamo vedendo adesso è tutto all'infuori di una mail vera. Mettendosi nei panni però di una persona poco esperta e anche impaurita dalla possibile mail scritta dalla polizia per qualcosa di grave, si va a visualizzare il contenuto del file. Esso appare come mostrato nella Fig. 1.3.


Fwd: DIREZIONE DEL CENTRO / POLIZIA.

PG Polizia Giudiziaria <pjudiciairegendarmerie@gmail.com> (pjudiciairegendarmerie@gmail.com) 5/5/2022 14:37

A no-reply@account.google.com Copia nascosta alexrio1998@libero.it

Rispondi Rispondi a tutti Inoltra Elimina Altro

1 allegato Vista Scarica

CONVOCAZIONE1.jpg (770,4 KB)

Questo messaggio non ha contenuto

Figura 1.2: Il contenuto della mail fraudolenta mostrato una volta aperta.


REPVBBLICA ITALIANA

DIREZIONE CENTRALE DELLA POLIZIA GIUDIZIARIA
BRIGATA DI PROTEZIONE MINORI

Alla tua attenzione:

Sono la signora **Nunzia Ciardi**, Direttore del Dipartimento di Polizia Postale e delle Comunicazioni, Capo della Brigata per la protezione dei minori (BPM).

Ti contatto poco dopo un sequestro informatico di infiltrazione informatica.
Autorizzato, in particolare in materia di pedopornografia, pedofilia, cyberpornografia, esibizionismo, traffico sessuale dal 2009.

Siete oggetto di numerosi procedimenti legali in vigore:

- Pornografia Infantile
- Pedofilia
- Esibizionismo
- Cyberpornografia

Per tua informazione, la legge n° 2007-293 del 5 marzo 2007 del codice penale aumenta le pene quando le proposizioni, le aggressioni sessuali o gli stupri potrebbero essere stati commessi utilizzando Internet e tu hai commesso i reati dopo essere stato preso di mira internet (sito pubblicitario), poi durante gli scambi di posta elettronica.

Le tue foto di nudo che invii a minori tramite il tuo indirizzo IP sono state registrate dal nostro cyber poliziotto e costituiscono una prova dei tuoi reati.

Sei pregato di farti sentire via email scrivendoci le tue giustificazioni affinché vengano messe in esame e verificate al fine di valutare le sanzioni; questo entro un termine rigoroso di 72 ore.

Trascorso tale termine, saremo obbligati a inviare la nostra denuncia al **Sig. Edmondo BRUTI LIBERATI**, Procuratore della Repubblica di Milano e specialista in cybercrime per redigere un mandato di cattura nei vostri confronti, inviarlo alla polizia più vicina al vostro luogo di residenza per il vostro arresto e denunciarti come molestatore sessuale.

Il tuo file verrà anche inviato ai media per la diffusione dove la tua famiglia, i tuoi cari e tutta l'Italia vedranno cosa stai facendo davanti al tuo computer o cellulare.

Ora sei stato avvisato.

Cordiali saluti,
Signora. Nunzia Ciardi

Direttore del Dipartimento di Polizia Postale e delle Comunicazioni
Capo della Brigata per la Protezione dei Minor

Direzione Centrale Della Polizia Giudiziaria
Brigata Di Protezione Minori
Via Tuscolana 1558 00173 Roma

Figura 1.3: Il contenuto dell'allegato presente nella mail fraudolenta.

Analizziamo punto per punto questa lettera famosa da parte del nostro "amico" poliziotto, senza considerare il fatto che la polizia invia le comunicazioni solo tramite posta cartacea e mai via e-mail. La prima cosa che salta all'occhio è proprio la prima parte dell'immagine: in un documento di polizia ufficiale non si utilizza mai la seconda persona, tanto meno ci si presenta dicendo di essere "la signora Nunzia Ciardi", bensì ci si aspetta una presentazione più formale.

Stesso discorso si applica sotto quando si cita il "Sig. Edmondo Bruti Liberati" come Procuratore della Repubblica di Milano. Analizzando poi il corpo del testo, notiamo tutte le caratteristiche che sono state già descritte in precedenza riguardo ad un generico attacco di phishing (§ 1.2): errori grammaticali, come nella frase "dopo essere stato preso di mira internet", minacce, ad esempio quando viene richiesta una mail di giustificazione entro 72 ore, pena l'invio delle foto di nudo al Procuratore di Milano per redigere un mandato di cattura o la stessa frase finale "Ora sei stato avvisato". Questi sono i dettagli che saltano, o meglio dovrebbero saltare all'occhio subito, poi ci sono altri piccoli dettagli come l'utilizzo di due diversi loghi della polizia postale, quello in alto a destra, il più nuovo, e i due in basso, vecchi e in disuso, o ancora la filigrana sullo sfondo che rappresenta il vecchio logo della Polizia di Stato italiana in vigore fino al 1991, come si può vedere dal sito della polizia stessa, e per finire il logo in alto a sinistra inserito senza alcuno scopo se non quello di intimidire ulteriormente la vittima, trattandosi del logo dell'unità specializzata sicurezza voli sensibili della Polizia di Stato Aeroporto di Roma-Fiumicino [7]. Facendo qualche ricerca su internet sul mittente, si viene a scoprire che questa mail è stata segnalata già in precedenza anche dalla gendarmeria francese [8], andando quindi a giustificare gli errori grammaticali presenti: probabilmente il mittente ha semplicemente copiato il testo tradotto dal francese in italiano utilizzando un traduttore online e cambiando solamente i nomi delle persone e delle città (Fig. 1.4).

DIRECTION GÉNÉRALE DE LA POLICE JUDICIAIRE
DIRECTION DE PROTECTION DES MINEURES

Attention ! ARNAQUE

Paris le 05 Octobre 2020

A votre attention:

Je suis **Mme YVETTE BERTRAND**, commissaire divisionnaire, chef de la brigade de protection des mineurs (BPM), je vous contacte peu après une saisie informatique de la Cyber-infiltration (autorisée, notamment en matière de pédopornographie, pédophilie, Cyber pornographie, exhibitionniste, trafic sexuelle depuis 2014) pour vous informer que vous faites l'objet de plusieurs Poursuites Judiciaires en vigueur:

_ La pédopornographie
_ La pédophilie
_ L'exhibitionniste
_ La Cyber pornographie
_ Le trafic sexuelle

Pour votre information, La loi de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez commis les infractions après avoir été ciblé sur internet (site d'annonce), puis pendant des échanges Mails (Messagerie Instantané) avec plusieurs mineurs, les photos dénudées de vous que vous envoyez aux mineurs ont été enregistrés par notre cyber-gendarme et constituent les preuves de vos infractions.

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications pour qu'elles soient mises en examen et vérifiés afin d'évaluer les sanctions, cela dans un délai strict de 72 heures. Passé ce délai nous nous verrons dans l'obligation de transmettre notre rapport à **Mme Myriam Quéméner** procureur adjoint au tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, le transmettre à la Gendarmerie la plus proche de votre lieu de résidence pour votre arrestation et vous fiché comme délinquant sexuel, transmettre votre dossier à plusieurs chaînes de télévision nationale d'information pour une diffusion ou votre famille, vos proches et toutes la France entière verront ce que vous faites devant votre ordinateur.

Pour tous informations écrivez à cette adresse : protection.mineurs@secretary.net

Maintenant vous êtes prévenu.
Cordialement,
Mme YVETTE BERTRAND, Commissaire Divisionnaire,
Chef de la brigade de protection des mineurs (BPM)

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE
BRIGADE DE PROTECTION DES MINEURS
Adresse: 12 QUAI DE GESVRES 75004 Paris

Figura 1.4: L'originale documento per il tentativo di phishing scritto in francese.

1.5.1 La lezione che si impara

Per le persone con poca esperienza di internet e dei suoi contenuti, questa lettera minacciosa viene scambiata automaticamente per vera poiché si è portati a credere quasi ciecamente a ciò che viene detto, anche se proviene da un totale sconosciuto in rete. Serve quindi iniziare a solcare il percorso di attenzione alla sicurezza in primis per le aziende, che sono ogni giorno prese di mira dagli attaccanti, ma anche per le persone private, le quali magari hanno già avuto esperienza con queste cose ma si sono trovate completamente spiazzate ed impreparate. Quindi ora la domanda su cui concentrarsi è: come insegnare i rischi dei contenuti che arrivano da internet e come riconoscere più facilmente dei falsi, senza andare nel panico e cedere ai ricatti dei criminali? La prima risposta che ci arriva è quella di seguire un classico corso di formazione sulla Cybersecurity, ma nel caso in cui venga seguito non per propria volontà può risultare poco producente, ad esempio nel caso di un dipendente non addetto alla sicurezza costretto dai suoi superiori. Bisognerebbe trovare un modo per rendere il tutto più accessibile, meno pesante e, perché no, anche divertente sotto qualche aspetto. Effettivamente questa cosa esiste già: la Gamification. Chi ha detto che divertendosi non si possa imparare.

Capitolo 2

La Gamification

Al giorno d'oggi i dipendenti delle aziende, e non solo, sono diventati sempre di più l'anello debole nella difesa contro gli attacchi informatici [9]. La regola base del buon senso non può rimanere l'unico elemento di difesa contro tecniche di attacco sempre più sofisticate, in quanto molto spesso gli attacchi provengono da vere e proprie organizzazioni di natura criminale in grado di fare leva su grandi risorse economiche e tecnologiche. Per questo motivo le aziende nell'ultimo decennio hanno iniziato, anche se non come ci si augurerebbe, ad investire risorse per assicurarsi che le "best practice" sulla sicurezza non vadano disattese e che nei loro dipendenti si crei una cultura più attenta alla sicurezza in generale, riferita non solo alla protezione di informazioni aziendali ma anche a tutto ciò che può essere esposto a rischi grazie all'utilizzo delle tecnologie ICT. Ultimamente nelle aziende si sta osservando la tendenza di creare e rendere più efficace il processo di Cybersecurity: come creare un meccanismo autonomo e continuo di self-reinforcement per i propri dipendenti? Come assicurare nel tempo una costante attenzione ai comportamenti e un aumento della consapevolezza sul tema sicurezza e sulla sua importanza? Una risposta a questa esigenza la si può trovare nell'applicazione di tecniche di Gamification al campo della sicurezza. Ovviamente esse potrebbero essere sfruttate anche per i privati cittadini, così da renderli più consci di quello con cui entrano in contatto ogni giorno e per rendere per davvero la Cybersecurity un processo in continuo aggiornamento e miglioramento aperto a tutti.

2.1 La Gamification: definizione e tecniche utilizzate

Il termine, com'è facile intuire, deriva dalla parola "Game", cioè gioco, anche associato al semplice divertimento, senza scopi particolari. La Gamification, tuttavia, non è semplicemente questo: traendo vantaggio dall'interattività concessa dai mezzi moderni ed ovviamente dai principi alla base del concetto stesso di divertimento, essa rappresenta uno strumento estremamente efficace in grado di veicolare messaggi di vario tipo, a seconda delle esigenze, e di indurre a comportamenti attivi da parte dell'utenza, permettendo di raggiungere specifici obiettivi, personali o d'impresa [10]: al centro di questo approccio si colloca l'utente ed il suo coinvolgimento attivo. Bisogna anche fare una distinzione tra Gamification e Serious games: la prima fa uso di elementi ludici come strategia per risolvere un problema al fine di ottenere un maggior coinvolgimento degli utenti in determinate attività tramite il gioco, ma in contesti estranei ad esso; i secondi creano un'esperienza ludica a fini didattici e formativi, in modo che i giocatori possano apprendere nuove conoscenze ed informazioni più velocemente anche di concetti completamente sconosciuti che diventeranno semplicissimi da assimilare. Gli obiettivi tipici che si riescono a conseguire grazie all'impiego della Gamification sono ad esempio il miglioramento della gestione dei clienti, il consolidamento della fedeltà ad un brand o l'improvement del rendimento e delle performance complessive da parte di dipendenti e partner. A prima vista sembra essere un approccio leggero e sperimentale, ma in realtà è ormai largamente diffuso ed affidabile, cresciuta praticamente di pari passo insieme al mercato videoludico. Ma cosa si intende precisamente con Gamification? Com'è possibile sfruttarne i paradigmi traducendoli in esempi concreti con obiettivi chiari e precisi, come nel nostro caso l'apprendimento dei concetti della Cybersecurity? Possiamo definirla come un insieme

di regole mutuate dal mondo dei videogiochi con l'obiettivo di applicare meccaniche ludiche ad attività che non hanno a che fare con il gioco: è possibile influenzare e modificare il comportamento delle persone, favorendo la nascita ed il consolidamento di interesse attivo da parte degli utenti coinvolti verso il messaggio che si è scelto di comunicare. Sono molti i contesti nei quali è possibile applicare quello che possiamo definire come il "metodo" Gamification: un sito, un servizio, una comunità, un contenuto o una campagna sono tutti contesti che possono essere "gamificati" in modo da spingere l'interesse, il coinvolgimento e la partecipazione degli utenti. Per raggiungere questi obiettivi, il processo di communication design deve necessariamente essere ripensato in modo da introdurre meccaniche e dinamiche di gioco, aggiungendo ai fattori tradizionali altre componenti trainanti che possano attirare l'interesse dell'utenza, spingendola a tornare su specifici contenuti proposti volontariamente e più volte nell'arco del tempo. Le meccaniche e le dinamiche di gioco sono i veri e propri ferri del mestiere nell'ambito della Gamification: l'introduzione di concetti come punti, livelli, missioni e sfide incoraggia gli utenti ad investire il proprio tempo, spingendoli alla partecipazione e aiutandoli anche a costruire relazioni all'interno del gioco che possono motivarli a raggiungere obiettivi predeterminati. Così facendo si va a stimolare una serie di istinti primari dell'essere umano come la competizione, il successo, i compensi, l'affermazione all'interno di un gruppo. Sollecitando nel modo giusto una persona, si possono ottenere ottimi risultati sia nel campo lavorativo che in quello personale. Pertanto, i concetti sfruttati dalla Gamification sono gli stessi che hanno da sempre accompagnato l'uomo nella sua storia: basti pensare alla nascita delle Olimpiadi, un luogo e un momento in cui poter competere per dimostrare chi sia il più forte in una determinata disciplina e, per fare ciò, ci si spingeva oltre i propri limiti per poter migliorare.

Oggi sono molti i siti web che cercano di creare community attraverso la Gamification: un esempio è quello del Sigaro Toscano, che utilizza tali principi per far progredire l'utente e ricercare nuovi gusti, curiosità o abbinamenti, concedendo ad esso punti da accumulare per migliorare il proprio "status" nella community. In questo modo si va ad accrescere il livello di soddisfazione finale dell'utente nell'utilizzare il sito e il prodotto stesso (Fig. 2.1).

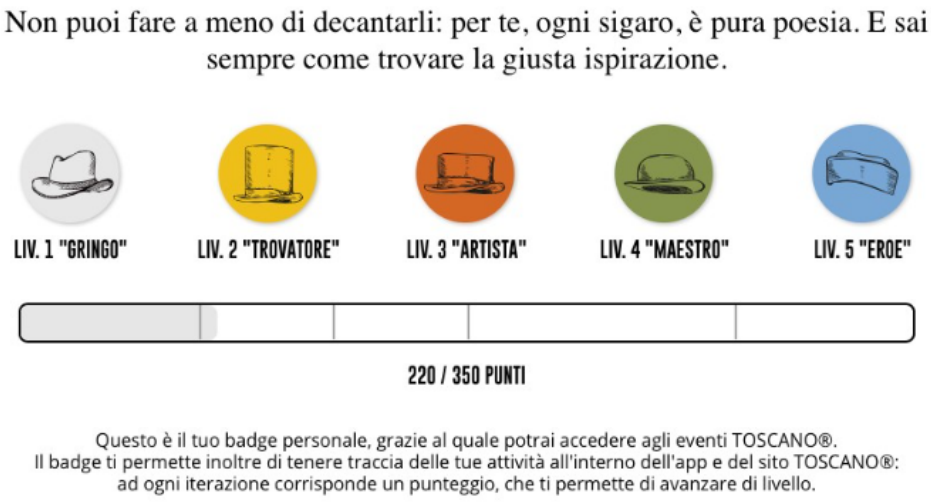


Figura 2.1: Il badge personale disponibile nella propria area utente del sigaro Toscano.

Per ridurre al minimo le possibilità di subire un attacco informatico, la formazione dei dipendenti regolare, continua e continuativa, deve passare da una visione di reazione a quella di prevenzione. Tecniche didattiche orientate solamente alla lezione frontale dei dipendenti si sono rivelate spesso inefficaci perché non sono abbastanza interessanti per la maggior parte dei partecipanti e non riescono a catturare l'attenzione dei dipendenti/discenti: pensare di istruire i dipendenti o comunque anche una persona al di fuori del contesto lavorativo può risultare utile e coinvolgente solo per una piccola parte dei partecipanti, ovvero coloro che, con molta probabilità, si applicherebbero a prescindere dal corso o dalla presenza di un formatore. In contesti similari interviene la Gamification, con lo scopo di coinvolgere le persone come se si stesse parlando di un gioco che, tuttavia, presenta un obiettivo finale diverso. L'errore umano, come già detto, è il

responsabile della maggior parte delle violazioni di sicurezza; molte società propongono una formazione attiva per i propri dipendenti, ad esempio tramite simulazioni sul phishing mirano a rendere più sicuri i mezzi di comunicazioni utilizzati. Alcuni di questi testi includono l'invio di e-mail di phishing per poter valutare la risposta dei dipendenti e la reazione dello staff di Cybersecurity per contenere l'attacco, sebbene sia solo una simulazione. Grazie alla Gamification, le aziende possono premiare in diversi modi (premio produzione, punti per avanzare nell'azienda, ricompense materiali) chi segue correttamente le procedure di sicurezza e chi aderisce correttamente alle sue linee guida, riuscendo a mantenere un buon comportamento aziendale. Questo sistema è utile anche nel caso in cui le cose non vadano bene, semplificando l'identificazione di coloro i quali mostrano un comportamento scorretto e portando i suddetti dipendenti a completare un'ulteriore fase di studio. Riconoscendo e gratificando i lavoratori che agiscono nella maniera corretta e correggendo coloro che hanno mostrato delle lacune si può creare un ambiente di lavoro più sicuro. La parte fondamentale in questio tipo di formazione è rendere consapevoli sull'importanza della sicurezza ed educare i dipendenti ad un senso condiviso di responsabilità per i dati con cui interagiscono ogni giorno: per creare una cultura della sicurezza ed innestarla all'interno dei processi aziendali occorre una profonda radicalizzazione di quest'ultima all'interno dell'educazione. Alcune possibili soluzioni implementative per avviare questo processo possono essere ad esempio:

L'abecedario base A-B-C-D (Ammaestra, Breve, Coinciso, Divertente): le lezioni che si tengono devono essere corte e divertenti, assicurandosi di seguire un approccio Top-Down. I dipendenti seguono il proprio leader: se egli stesso non incarna al meglio la cultura della sicurezza non lo faranno nemmeno loro. Bisogna educare i dipendenti alle "best practice" necessarie per continuare un percorso sicuro, cercando sempre di strappare un sorriso mentre si insegna;

Le tattiche intimidatorie non funzionano: l'obiettivo aziendale è quello della Cybersecurity awareness. Bisogna iniziare a pensare ad una strategia di marketing Gamification con lo scopo di persuadere e modificare il comportamento del dipendente;

I video attraggono maggiormente: per iniziare il processo, si può pensare di iniziare con dei piccoli video simpatici sulla sicurezza, in modo tale da far capire a tutti che è una responsabilità condivisa;

Rinforzo e follow-up: l'allenamento deve essere costante, in quanto gli attacchi sono in continua evoluzione e bisogna farsi trovare sempre pronti: si deve sempre prestare attenzione ai dipendenti che ancora non sono in grado di riconoscere una mail falsa e incoraggiarli nella comunicazione, richiamando i dipartimenti che sono ancora in ritardo sulla preparazione. Una sana rivalità all'interno dell'azienda risulta essere molto produttiva.

Lo studio condotto da I. Rieff [11] ha provato che la Gamification aiuta e non poco a migliorare i Security Awareness Training, andando anche ad elencare quelli che sono gli elementi migliori su cui basarli facendo riferimento alle loro ricerche. Alcune di queste meccaniche presentate nella seguente tabella potrebbero essere inserite anche in altre categorie, ma in linea di massima esse rappresentano la guida migliore per far approcciare il mondo della Cybersecurity a quello della Gamification per creare una forte dicotomia e migliorare la consapevolezza dell'importanza della sicurezza nella vita di tutti i giorni (Fig. 2.2).

Anche all'interno dello studio di L. A. Thompson, N. Melendez, J. Hempson-Jones e F. Salvi [12] viene riportato quanto sia importante l'utilizzo di elementi ludici all'interno di tecnologie educative e ambienti di apprendimento digitali. Le loro ricerche hanno portato alla creazione di un nuovo Framework, il RAD-SIM, da utilizzare come spunto quando si vanno a definire attività di tipo "Game-Based Learning" (Fig. 2.3). Il suo scopo è quello di andare in aiuto ai designers GBL, basandosi su principi comportamentali e suddividendolo in diverse sottosezioni che vanno anche a dare il nome al framework. Il solco, quindi, risulta già tracciato e ben definito, pertanto non resta che seguirlo e rimarcarlo lì dove è necessario.

Categories	Gamification Mechanics
Cooperation / Competition	Leaderboards Social Guilds Roles Avatars Virtual Goods
Prices	Badges / Medals Trophies Achievements Awards, Trading & Gifting / Rewards
Adventures	Challenges Actions Quest / Goal / Mission Boss Battles
Progression	Progress Bar / Status Points / XP Levels Feedback / Reports
Surprises	Unlockable Content Easter Eggs Lottery / Game of Chance Notifications

Figura 2.2: Le categorie delle meccaniche di Gamification come illustrate all'interno dello studio di I. Rieff [11].

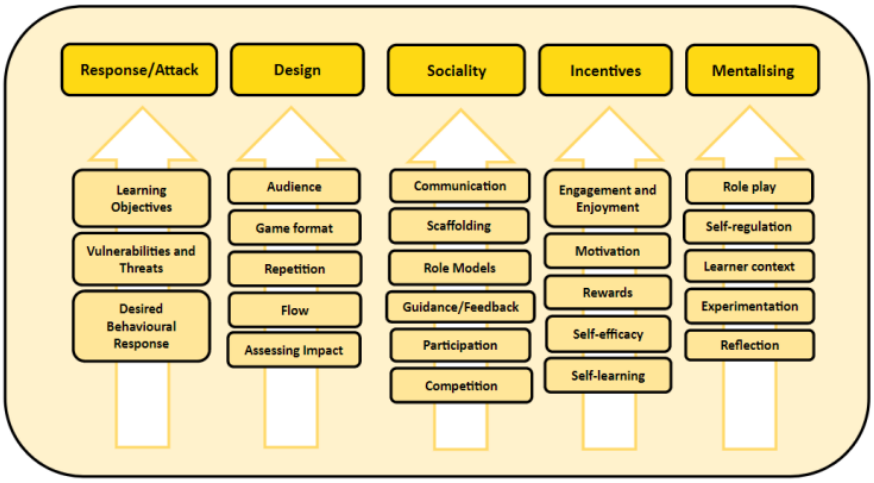


Figura 2.3: Il grafico che illustra i vari aspetti del framework RAD-SIM [12].

2.2 I tipi di giochi più utilizzati nell'ambito Cybersecurity

Esistono al giorno d'oggi moltissimi esempi di utilizzo di tecniche di Gamification per creare dei veri e propri giochi il cui scopo è quello di far avvicinare le persone alle buone pratiche di security awareness. All'interno della ricerca portata avanti da M. Coenraad, A, Pellicone, D. J. Ketelhut, M. Cukier, J. Plane e D. Weintrop [13] infatti, sono stati presi in considerazione ben 181 videogiochi diversi con riferimenti alla sicurezza informatica, suddivisi tra i vari store digitali (Google Play Store, Apple Store, Steam). I dati più rilevanti di questa ricerca sono principalmente due: come viene presentata la Cybersecurity e il metodo scelto per condividerla e utilizzarla all'interno dei videogiochi presi in considerazione.

Come è possibile notare dal grafico riportato in Fig. 2.4, sono tre principalmente le tipologie di presentazioni scelte:

- Deep Engagement: richiede un'immersione profonda dell'utente all'interno del gioco, ad

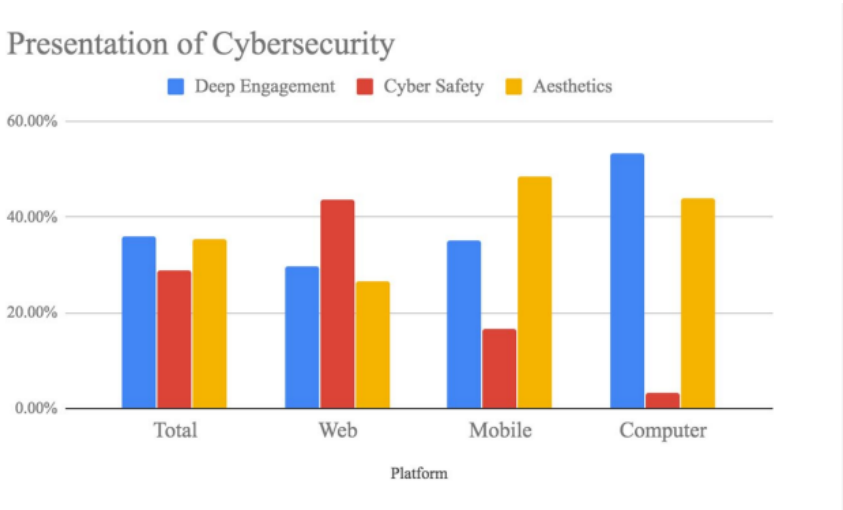


Figura 2.4: Le modalità con cui nei giochi viene presentata la Cybersecurity, come illustrato nello studio dei giochi digitali sulla sicurezza informatica [13].

esempio nei panni di un hacker che deve inserire del codice da linea di comando per rubare o cancellare delle informazioni;

- Cyber Safety: si riferisce alle persone che devono reagire agli attacchi ricevuti e quindi contrastare gli attaccanti. Il focus principale dei giochi di questo tipo è quello di fornire una certa formazione per le buone abitudini nella sicurezza informatica, ad esempio su come creare delle password molto resistenti o sul mantenere il database dell'antivirus aggiornato;

- Aesthetics: in questi videogiochi i termini relativi alla Cybersecurity vengono utilizzati in modo diverso, utilizzando quelli che sono gli assets grafici.

Solitamente si viene solo a conoscenza quindi dei nomi legati al mondo della sicurezza informatica, senza però avere una chiara definizione di essi. Il secondo dato rilevante è, invece, quello relativo al metodo utilizzato per integrare la Cybersecurity all'interno dei videogiochi. Dallo studio [13] è risultato il quiz gamificato come il metodo più utilizzato, seguito dai worksheets, gli arcade games ed infine i puzzle games (Fig. 2.5).

Integration Method	Total	By Platform	By Developer
Gamified Quiz	43 (23.8%)	Web - 38 (40.4%) Mobile - 7 (11.7%) Computer - 0 (0.0%)	For-Profit Company - 3 (27.3%) Game Company - 2 (3.8%) Government Agency - 13 (72.2%) Individual - 2 (7.7%) Non-Profit Company - 6 (18.2%) Academic Institution - 17 (43.6%)
Gamified Worksheet	19 (10.5%)	Web - 16 (17.0%) Mobile - 5 (8.3%) Computer - 0 (0.0%)	For-Profit Company - 1 (9.1%) Game Company - 1 (1.9%) Government Agency - 3 (16.7%) Individual - 2 (7.7%) Non-Profit Company - 3 (9.1%) Academic Institution - 9 (22.5%)
Arcade Games	26 (14.4%)	Web - 7 (7.5%) Mobile - 15 (25.0%) Computer 6 - (18.8%)	For-Profit Company - 3 (27.3%) Game Company - 10 (18.9%) Government Agency - 1 (5.6%) Individual - 8 (30.8%) Non-Profit Company - 0 (0.0%) Academic Institution - 4 (10.0%)
Puzzle Games	23 (12.7%)	Web - 12 (12.8%) Mobile - 9 (15.0%) Computer - 3 (9.4%)	For-Profit Company - 0 (0.0%) Game Company - 5 (9.4%) Government Agency - 1 (5.6%) Individual - 5 (19.2%) Non-Profit Company - 8 (24.2%) Academic Institution - 4 (10.0%)

Figura 2.5: Metodi di integrazione per la Cybersecurity nei videogiochi [13].

2.3 La paura mette le ali

Attraverso gli studi fatti all'interno dello studio di H. Qusa e J. Tarazi [14], si è cercata un'idea per far avvicinare anche i ragazzi delle scuole superiori a quello che è il mondo della Cybersecurity. Il mezzo che è stato utilizzato è lo sviluppo di un nuovo tipo di framework che fa uso di Gamification e utilizzare alcuni serious games per avere il responso dagli stessi ragazzi sull'effettiva correttezza del sistema. La scelta un po' particolare che è stata fatta, oltre all'utilizzo degli elementi ludici, è quella di usare le emozioni come perno del proprio sistema e in particolar modo due vengono ricercate: il divertimento e la paura. Due sentimenti completamente contrastanti ma che riescono a collaborare in un certo modo per poter arrivare all'obiettivo su cui si basa tutto ciò: insegnare nozioni di Cybersecurity, nel caso specifico di questa ricerca, a studenti delle superiori. Ma perché queste due? Il divertimento è sicuramente la cosa fondamentale che sprona una persona a giocare, insieme alla competizione che nasce e possibili achievement da raggiungere, mentre la paura viene considerata anche un sentimento migliore rispetto a tutti gli aspetti positivi. Questo perché essa riesce a stimolare meglio il giocatore a migliorarsi durante il periodo di training per evitare di avere delle conseguenze negative provenienti a loro volta da altrettanto negative scelte effettuate in precedenza. La cosa importante è che alla fine del gioco vengano mostrati i risultati, specialmente quelli negativi, in modo tale da spronare a migliorarsi proprio dove risulta esserci una carenza di conoscenze. Durante i test che sono stati effettuati si è rilevato un miglioramento del 5% in media nella scelta di una password sicura, passando da selezionare una password basata solo su numeri nel pre-test, ad una complessa formata da caratteri diversi nel post-test, avendo quindi un buon feedback. Ciò significa che l'utilizzo corretto dei sentimenti delle persone risulta avere un effetto positivo anche sulla loro produttività, oltre che sul loro indice di apprendimento. La paura effettivamente è un'arma molto potente, infatti si è sempre detto che "metta le ali", ma deve essere utilizzata in maniera corretta e somministrata in piccole dosi per evitare di avere una persona completamente paralizzata da essa e quindi avere il risultato completamente opposto rispetto a quello che si stava ricercando.

2.4 Winning the Game: come sconfiggere gli attaccanti con un gioco

L'impiego di dinamiche ludiche nel percorso di awareness non è certamente sinonimo di successo garantito, ma è certamente un passo nella direzione giusta, quella del "learn by doing" e del coinvolgimento attivo. Una testimonianza ci arriva dalla ricerca effettuata da McAfee intitolata "Winning The Game" [15] datata aprile 2018. Dati molto confortanti arrivano infatti dal punto tre di tale documento, dove viene riportato che il 96% delle aziende che hanno applicato la Gamification hanno riscontrato grossi benefici sulla Cybersecurity proprio in conseguenza dell'utilizzo di queste tecniche. Essa viene definita come un importante strumento per poter arrivare ad un'organizzazione della sicurezza più performante e che 4 organizzazioni su 10 organizzano degli esercizi di Gamification almeno una volta all'anno. Il più utilizzato risulta essere il "Capture the flag" seguito poi da "Red Team vs Blue Team".

Come riportato in Fig. 2.6, i benefici migliori ricevuti dall'applicazione di tecniche di Gamification sono per il 57% una maggiore attenzione e conoscenza all'interno dello staff IT di come possono avvenire le brecce, per il 49% come evitare di diventare una vittima di un tentativo di breccia, per il 46% come reagire a una breccia. Segnali confortanti arrivano anche dalla quarta voce che recita che per il 43% hanno rinforzato la cultura del lavoro di squadra, valore fondamentale per avere una sicurezza veloce ed efficace. Questo ci indica che la sana competizione che può arrivare dalla Gamification non va a minare i rapporti tra i colleghi in ufficio, ma anzi li ha rafforzati quasi in un caso su due. Questi benefici, si legge continuando nella ricerca, sono stati riconosciuti non solo da professionisti della sicurezza, ma anche da senior manager, i quali per il 77% afferma che la loro organizzazione di Cybersecurity sarebbe molto più sicura se applicassero queste tecniche. Prendendo in considerazione il gioco Capture the flag, il 54% dei partecipanti risulta soddisfatta del loro ruolo e affermano di utilizzare tecniche di Gamification uno o più volte all'anno, in confronto al 14% che invece ritiene di essere insoddisfatto. Questa però era solo la prospettiva dei dipendenti che utilizzano questi "giochi" durante l'anno, i dati si fanno ancora

Figura 2.6: La percentuale degli intervistati che credono che i concetti della Gamification rendono più forti le difese della Cybersecurity [15].

più interessanti quando si va a considerare quelli che non ne prendono parte. In questo caso abbiamo 7 persone su 10 che ritengono di non essere soddisfatte di lavorare in organizzazioni che non praticano la Gamification, mentre si arriva ad un significativo 80% di impiegati estremamente insoddisfatti e che desidererebbero mettere in pratica questi giochi. Particolarmente interessante risulta l'ultima sezione della ricerca, dove si ipotizza di trovare nella figura dei videogiocatori i cosiddetti "threat hunters", ovvero i cacciatori di minacce, della prossima generazione. Dati alla mano, il 45% degli addetti ai lavori nel mondo della Cybersecurity afferma di utilizzare anche con frequenza i videogiochi, mentre il 92% delle persone coinvolte in queste ricerche afferma che i videogiocatori possiedono le abilità necessarie per intraprendere una carriera nella Cybersecurity. I tre quarti dei senior manager interpellati ha inoltre aggiunto che considererebbe assumere un videogiocatore, anche se non possiede effettivamente esperienza o conoscenze in questo ambito, tutto ciò grazie alla loro capacità di imparare velocemente a cercare indizi, strumenti e armi nelle loro "quest" per arrivare al successo, portandoli poi a sviluppare anche persistenza, spirito di osservazione e logica. A dare forza a questa tesi, il 78% degli intervistati afferma che l'attuale generazione che sta entrando nel mondo del lavoro, cresciuta giocando ai videogiochi, possiede tutte le caratteristiche necessarie per poter far bene nella Cybersecurity, accompagnato poi anche dal nuovo punto di vista con cui si approcciano i problemi totalmente diverso rispetto alle generazioni precedenti (Fig. 2.7).

Questa ricerca si è quindi rivelata molto positiva per l'applicazione della Gamification per poter imparare i concetti fondamentali della Cybersecurity, portando ad accrescere lo spirito di squadra oltre alle conoscenze necessarie per poter affrontare correttamente i rischi di questo mondo.

2.5 Cyber Stability Games: è in gioco la sicurezza informatica

La multinazionale russa Kaspersky, specializzata nella produzione software per la sicurezza informatica, utilizza già da tempo la Gamification applicandola ai corsi di formazione aziendale per la security awareness. Parte di questo portfolio comprende la Kaspersky Interactive Protection Simulation (KIPS) [17], che offre diverse soluzioni per poter aumentare l'attenzione sulla Cybersecurity per il proprio staff, in modo da renderlo più partecipe all'interno della sicurezza

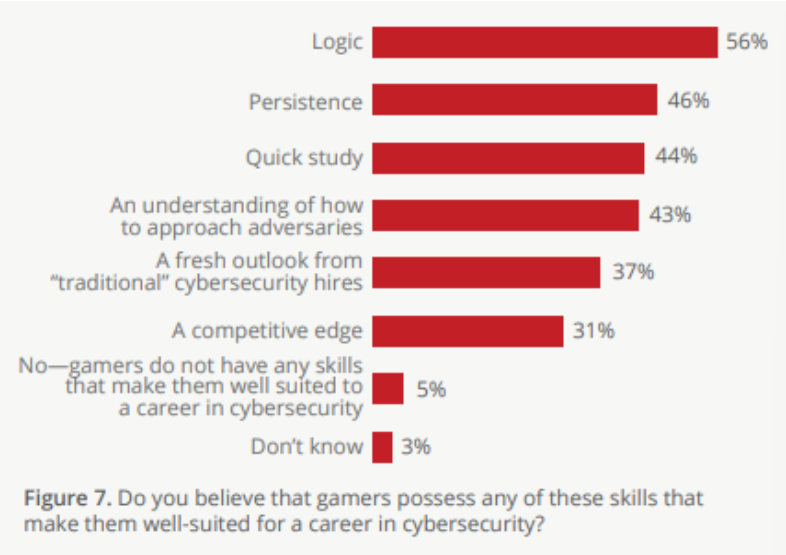


Figura 2.7: Le skill che secondo gli intervistati del report Winning the Game [15] possiedono i "gamers".

dell'azienda. KIPS presenta all'interno del suo programma una parte che fa uso della Gamification, arrivando anche a creare una simulazione di business strategico tramite un gioco a squadre, dimostrando la connessione tra l'efficacia degli affari e la Cybersecurity. Tra i vari "KIPS Games" è presente Cyber Stability Games [16], uno dei vari esempi di applicazione della Gamification che porta la sicurezza informatica all'attenzione di diplomatici, politici e figure professionali prive di background tecnico, facendo comprendere anche quanto sia effettivamente complicato gestire un cyber attacco. L'idea alla base è un'esperienza di "capacity building" che si sviluppa in cinque round e che simula un attacco informatico al Primo Comitato delle Nazioni Unite. Realizzato in collaborazione con DiploFoundation, il suo scopo è quello di far apprendere alle persone manchevoli del background tecnico necessario quali siano le complessità dell'attribuzione tecnica di un attacco informatico. I giocatori partecipano singolarmente alla simulazione e vestono i panni di alcuni diplomatici all'interno di un mondo fittizio, il cui compito sarà quello di affrontare un cyber attacco mirato e scoprire chi sia il colpevole scegliendo tra cinque possibili "threat actor": Black Octopus, Bob Hacktivist, Hacking-for-hire company, Red Snake e White Horse (Fig. 2.8).

Figura 2.8: I possibili colpevoli dell'attacco all'interno di Cyber Stability Games.

Il gioco si svolge in un totale di cinque round, i partecipanti possiedono un budget di spesa, delle risorse relative al tempo e varie schede che possono essere utilizzate per reagire alle singole

azioni. Ad esempio, nel caso di attacco ransomware che crittografa i dati e mette fuori gioco gli account di posta elettronica, viene chiesto al giocatore di scegliere tra: rivolgersi ad un'entità privata o governativa per ricevere supporto, pagare il riscatto richiesto dal criminale e sperare che sblocchi tutto oppure creare dei nuovi account gratuiti di posta elettronica. Alla fine del singolo round viene assegnato un punteggio che sarà ovviamente più alto per chi ha risposto correttamente all'azione richiesta e inoltre sarà anche presente un report, il quale spiegherà gli effetti delle carte giocate durante il turno per affrontare l'attacco e come si svilupperà poi di conseguenza lo scenario successivo. L'interfaccia e la dinamica di gioco sono strutturate per rendere Cyber Stability Games accessibile anche a chi non è un giocatore abituale di videogiochi in quanto non viene richiesta alcuna dote fisica o reattività. Il gioco è statico, basato solo sulla scelta delle carte, le quali risultano essere chiare da interpretare con una breve descrizione che permette di capire velocemente quale sia la funzione di ciascuna. Le cose più importanti, ovvero il costo dell'azione e il tempo impiegato, sono bene in evidenza rispetto alla descrizione ed è quindi difficile perdere di vista l'investimento che si sta facendo e la somma che rimane nelle proprie casse (Fig. 2.9).

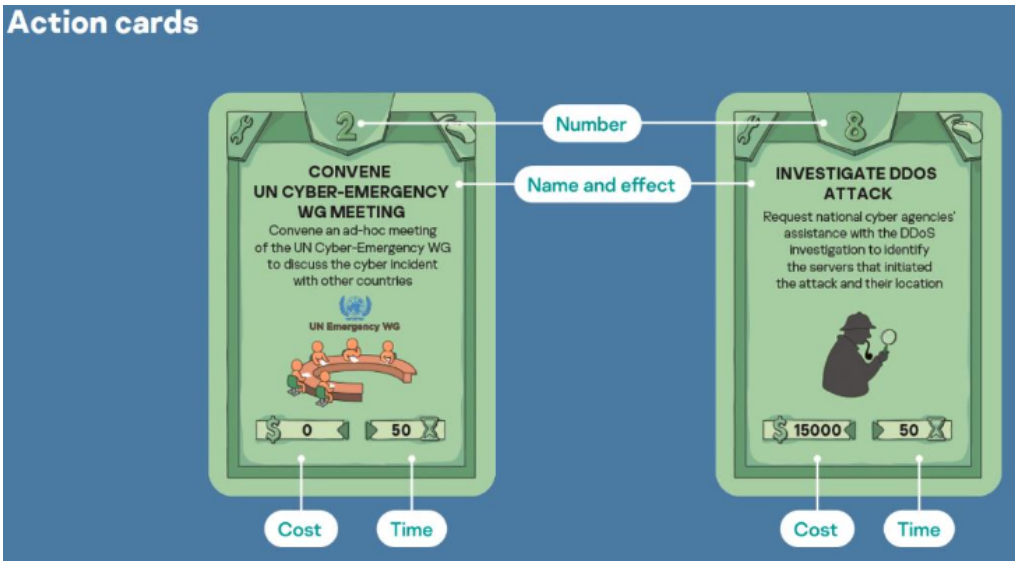


Figura 2.9: Le carte giocabili durante il proprio turno, con la descrizione degli effetti e dei costi in denaro e di tempo.

Ogni round si articola in poche e semplici fasi:

1. Un primo messaggio di esordio che presenta il problema come l'avvenuto attacco oppure l'arrivo di una notizia su di esso. Questa è l'unica fase del gioco in cui vengono presentati i pochi termini tecnici e le sigle che sono stati spiegati prima di iniziare il gioco;
2. Scelta delle carte per reagire all'attacco con il tempo per poter cambiare idea;
3. Reporting conclusivo e assegnazione del punteggio.

Cyber Stability Games ha portato all'attenzione alcune tematiche molto importanti e profonde con un gioco molto semplice e divertente, ad esempio la questione del budget, tema da sempre critico per quanto riguarda la sicurezza informatica poiché essa è da sempre vista come una "spesa" e non come un investimento, andando quindi a considerarla come se fosse una tassa annuale da pagare e non come l'inizio di un importante processo. Molto spesso poi le Nazioni che investono nella Cybersecurity arrivano a spendere cifre irrisorie per gli esperti del settore, ma che da un punto di vista esterno sembra essere una quantità anche generosa. Il budget per la creazione di questo gioco però è stato volutamente molto basso se lo si paragona ai prezzi riportati sulle carte da gioco e questo porta con sé un bel messaggio: l'investimento nella Cybersecurity dev'essere adeguato all'obiettivo che si vuole raggiungere. Contemporaneamente ne porta con sé anche un altro: giocare le carte più "pesanti", ovvero quelle che richiedono un budget elevato, non porta sempre

alla vittoria. Effettivamente questo è un problema segnalato anche da molti esperti di sicurezza, ci sono degli investimenti alti a fronte di risultati mediocri e questo ci insegna ancora una volta la differenza tra sapere e non sapere spendere bene il proprio budget: la sicurezza informatica deve essere un processo continuo e giornaliero, non si otterrà mai comprando e installando tutti i prodotti migliori sul mercato. Certo questi possono aiutare, ma bisogna tenere a mente sempre qual è il punto debole anche della macchina di ultima generazione appena uscita sul mercato: l'uomo che la manovra. Le soluzioni adottate dalle aziende dovrebbero essere mirate per le reali necessità di quest'ultima, dopo aver effettuato un'attenta analisi del rischio. Inoltre, è importante capire bene le tempistiche per difendersi da un attacco: non fare niente oppure rispondere troppo tardi non ripagano. Altro aspetto importante proposto da Kaspersky è la strategia: alcuni messaggi all'interno del gioco sono ingannatori e sibillini, fatti ad hoc per indurre il giocatore a sbagliare. Alcuni potrebbero lamentarsi affermando che questo non sia un comportamento corretto, ma d'altro canto non lo è nemmeno quello dei cyber criminali che promettono di sbloccare il dispositivo una volta ottenuto il pagamento richiesto per poi intascarsi la somma e sparire senza riparare il danno. La scelta di Kaspersky vuole insegnare che scendere a patti con i criminali informatici non è mai una buona idea e che durante una trattativa non ci sono garanzie o promesse infrangibili.

2.6 Conosci il tuo nemico

Si è visto come all'interno degli studi proposti sui possibili utilizzi della Gamification sia presente un grande elemento in comune tra loro: il punto di vista. Infatti, esso risulterà fisso sulla parte lesa, su chi si difende, senza andare ad enfatizzare troppo su "come è riuscito l'attaccante a superare le difese". Quello proposto all'interno dello studio di M. Adams e M. Makramalla [18] è esattamente questo: cambiare il punto di vista, sempre sfruttando elementi di Gamification. Il motivo è molto semplice, infatti tutto questo si rifà ad una celebre frase del generale militare, stratega e filosofo Sun Tzu ne "l'Arte della Guerra": "Se conosci il nemico e te stesso, la tua vittoria è sicura". È proprio quello che si vuole trovare, una vittoria assicurata, proprio per questo motivo il lavoro fatto da M. Adams e M. Makramalla [18] risulta molto utile alla causa. Infatti, grazie allo scenario di Training gamificato che hanno proposto, l'utente, da sempre considerato come l'anello debole nella difesa, si è ritrovato catapultato tutto ad un tratto nel lato delle persone da temere. Se quindi negli altri casi si tentava di trovare una risposta ad un possibile attacco o ad uno già in corso, adesso si passa a crearne uno da zero.

Avatars (Attacker Roles)	**Avatar Characteristics (Attacker Types)**
Bricolage: "The rookie"	• Script kiddies • Cyber-punks • Petty thieves
Effectuation: "The adroit"	• Insiders
Causation: "The architect"	• Nation states • Professional criminals
Emancipation: "The liberator"	• Insiders • Hacktivists
Hubris: "The optimist"	• Grey hats
Social: "The advocate"	• Hactivists

Figura 2.10: I possibili attaccanti interpretabili nello scenario pianificato da M. Adams e M. Makramalla [18].

L'utente viene posto per prima cosa davanti ad alcune domande per capire il livello di conoscenza sull'argomento Cybersecurity; fatto ciò, si passa a scegliere uno degli avatar interpretabili, descritti in Fig. 2.10, ma senza dare molte informazioni se non i punti deboli e forti e quali sono le risorse necessarie per poter avanzare all'interno del gioco. Nell'esempio proposto l'impiegato

riesce, dopo qualche fallimento, ad impiantare con successo un malware all'interno del sistema, tutto questo per insegnare concetti fondamentali come la prevenzione, l'anticipazione, la reazione e la risposta ai possibili attacchi. È sicuramente un punto di vista interessante, con molti punti di forza e alcuni concetti da rivedere probabilmente, specialmente per quanto riguarda i tipi di attacchi da implementare. In ogni caso, esso si può rivelare molto utile proprio perché così facendo si è in grado di capire meglio quali sono i possibili movimenti degli attaccanti, quali possono essere i punti deboli ed esposti e quali sono le azioni che, nel mio piccolo, posso fare per poter mantenere il tutto sicuro dal punto di vista informatico.

2.7 L'utente al centro di tutto

Lo studio condotto da E. G. B. Gjertsen, E. A. Gjære, M. Bartnes e W. R. Flores del Dipartimento di Telematica all'Università di Scienze e Tecnologia di Trondheim, Norvegia [19], si è concentrato sull'applicazione della Gamification all'interno dei programmi di "Security Awareness and Training" (SAT), i quali sono comunemente utilizzati all'interno del mondo del lavoro per mitigare il rischio di comportamenti insicuri tra gli impiegati. L'idea di utilizzare la Gamification a braccetto con il SAT non è di certo una novità, già dal 2014 si hanno degli esempi di giochi "tower defense" per insegnare la forza di una password utilizzata [49]. Viene inoltre riportato uno studio del 2015 [48] dove viene utilizzata una storia inventata su un possibile breach della sicurezza che ha compromesso i dati dell'utente di una banca, il cui scopo è valutare l'efficacia della soluzione in due diversi casi: con formazione basata su Gamification, per valutare le sue qualità nell'insegnare i concetti di sicurezza, e non basata su di essa. I risultati hanno riportato come avere un insegnamento con la Gamification sia meno efficace rispetto a una formazione tradizionale, ma allo stesso tempo è risultato più godibile, più divertente e meno noioso rispetto all'alternativa classica. Questo studio del 2015 [48] però risulta essere condizionato dal breve tempo in cui è stato compiuto e principalmente dalla mancanza di alcuni elementi fondamentali della soluzione gamificata come una classifica per alimentare la competizione, badges per sottolineare i traguardi raggiunti o valute virtuali. Tornando allo studio norvegese invece, si è optato per effettuare una ricerca qualitativa di design, tentando di mettere in pratica la loro idea con un prototipo interattivo. Si è quindi deciso di intervistare dieci impiegati di due grandi compagnie Scandinave, con domande sulla "quality assurance" relativa all'idea di utilizzare la Gamification insieme al SAT dal punto di vista di una compagnia. I quesiti vertevano sulla loro esperienza personale con i programmi SAT, sulle sfide in generale con la sicurezza e sulla Gamification. Venne inoltre chiesto loro di selezionare cinque fattori motivazionali che dal loro punto di vista sono i più importanti in una soluzione SAT gamificata. Partendo da questi risultati si è quindi arrivati alla costruzione del prototipo interattivo del loro gioco (Fig. 2.11), creato con lo scopo di essere testato per prelevare le impressioni dei partecipanti sul come un'applicazione basata sulla Gamification e con il fine di insegnare i concetti della sicurezza informatica dovesse apparire. Le risposte a questa esperienza da parte delle persone interpellate per il testing sono state raccolte per essere il nuovo punto di partenza da cui partire per migliorare il prototipo e trasformarlo lentamente in un'applicazione vera e propria.

Come riportato in Fig. 2.11, il prototipo contiene al suo interno esercizi e materiale relativi ad accrescere la consapevolezza dell'utente verso la sicurezza, il tutto racchiuso all'interno di un'esperienza gamificata con l'utilizzo di elementi quali punti, barre di progresso, badge e classifiche. Ancora una volta la competizione positiva porta a degli ottimi risultati. L'utilizzo del prototipo è stato anche schematizzato come segue:

- L'utente controlla dove e quando allenarsi accedendo all'applicazione apposita per l'apprendimento attraverso un browser web oppure un'applicazione mobile;
- L'applicazione presenterà una vasta selezione di tasks ed esercizi divisi nelle rispettive categorie. Saranno presenti poi contenuti multimediali come video, quiz e collegamenti per risorse esterne, regolarmente aggiornato ed esteso;
- Gli esercizi saranno coincisi e compatti, ogni task od esercizio dovrebbe durare un massimo di cinque minuti;

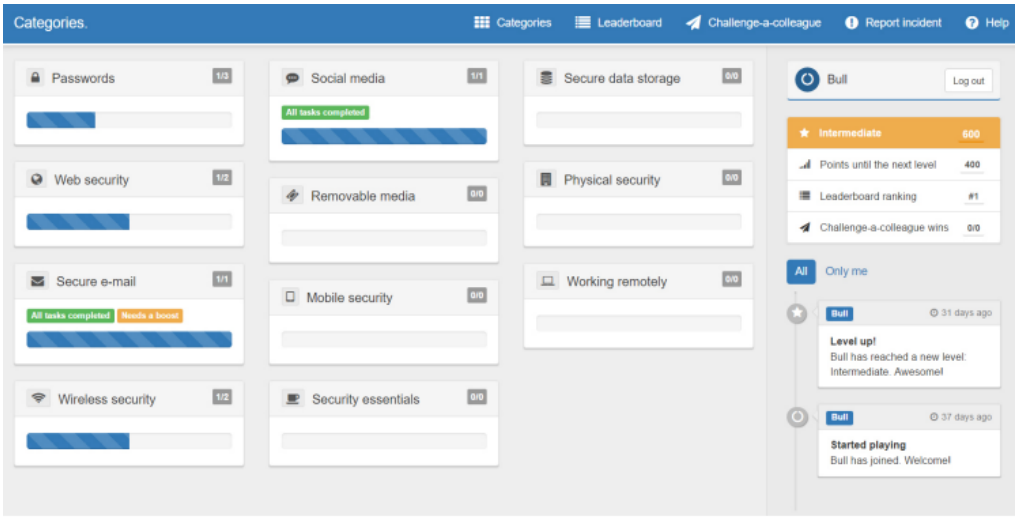


Figura 2.11: La pagina principale del prototipo che cerca di gamificare i concetti del SAT .

- L'utente è libero di completare qualunque esercizio in qualsiasi ordine, dando così al "giocatore" una completa autonomia e insegnare anche a non seguire sempre un certo tipo di percorso. Alcune restrizioni saranno presenti per fare in modo che l'utente riceva il tipo e la quantità di allenamento richiesto.

Al momento nel prototipo sono presenti una piccola selezione di elementi di Gamification, ma sono presenti in diversi esercizi di diverse categorie. Ogni utente avrà una propria progressione legata alle singole categorie insieme ad un punteggio ottenuto, completando esercizi si otterranno dei punti che andranno a sommarsi a quelli già presenti nel proprio "skill level". È presente anche una linea temporale in cui si tiene traccia delle attività dell'utente all'interno dell'applicazione e di una classifica dove si tiene traccia dei propri progressi e di quelli degli altri utenti. L'intenzione è quella poi di aggiungere un'altra voce al menù in alto chiamata "Sfida un collega", in cui sarà possibile fare una sfida tra colleghi su particolari argomenti. La conclusione a cui poi sono arrivati è stata la seguente: molti dei problemi dovuti all'approccio tradizionale dei SAT dipendono dal fatto di non valorizzare e non mettere al centro dell'attenzione l'utente finale, cosa che la Gamification fa "by design".

2.8 I pericoli della Gamification

Gli studi che sono stati condotti sulla Gamification hanno riportato segnali positivi e ne hanno descritto appieno ogni vantaggio che si avrebbe nell'utilizzarla per insegnare i concetti della Cybersecurity. Ovviamente, come ogni cosa d'altronde, esistono lati positivi e negativi. In primis bisogna scegliere con attenzione gli elementi ludici da riportare nel prodotto da proporre, non tutti infatti possono risultare utili per lo scopo che si è preposto. Inoltre, una volta selezionati, si deve fare particolare attenzione a quegli elementi che potrebbero non rispettare la privacy dell'utente, ad esempio utilizzando features come avatar, sfide o comunicazioni tra i vari utenti. Tutto ciò porterebbe ad avere una fuoriuscita di dati non necessaria, andando ad aumentare i rischi inutilmente, gli stessi che sono stati analizzati da Bruce Schneier nel suo blog: "siamo tutti sempre più portati a cedere i nostri dati online a multinazionali come Google, Facebook, Apple per le promesse di sicurezza che ci vengono fatte da esse. Questo sistema, sempre più grande ormai, è una ripresa dell'antico feudalesimo, dove noi siamo i vassalli dei grandi feudatari rappresentati dalle grandi compagnie. Tutti noi utenti cerchiamo la protezione delle grandi multinazionali, così come si faceva nel Medioevo", sebbene ora si parli di un altro tipo di sicurezza e tutta la visione sia molto romanzata [20]. "Ogni cosa nella vita ha un lato luminoso e uno oscuro; la Gamification non è di certo un'eccezione". Questa frase è l'incipit dello studio effettuato dalle università di Sao Paulo e Ishikawa [23] su quelli che sono appunto i lati positivi e quelli negativi dell'applicazione

della Gamification all'interno di ambienti educativi. Quando le persone trovano una cosa buona, tendono a focalizzarsi solamente sul suo lato più luminoso, ma dovrebbero sempre avere un rispettoso timore verso quello meno luminoso in modo tale da poterlo utilizzare correttamente. Kapp definisce la Gamification come "l'utilizzo di meccaniche di gioco, estetica e ragionamenti tipici dei giochi per motivare le persone ad agire, promuovere l'apprendimento e risolvere problemi". La sua definizione [21] può variare tra autore e autore, ma il nucleo resta intatto in tutte quante: "spronare le persone ad ingaggiare attività utilizzando elementi ludici che portano a divertirle". Anche gli strumenti utilizzati sono quasi sempre gli stessi: classifiche, badges, obiettivi da raggiungere e ricompense. Esiste però la possibilità che tutto questo porti a dei fattori negativi, solitamente tre, i quali anche essi vengono riportati da vari studi fatti sull'argomento: comportamenti inaspettati che vanno a sviare le persone dal vero obiettivo, una competizione indesiderata, ad esempio, tra quelli con delle performance più basse che sono costretti a competere con altre persone risultando in una perdita di interesse e infine una possibile dipendenza dal gioco. Ci deve quindi essere un focus sugli aspetti negativi al pari di quelli positivi, altrimenti si rischia di perdere un'ottima opportunità per far crescere nelle persone un sentimento comune di attenzione verso la sicurezza informatica. Inoltre, uno dei problemi più grandi è la perdita dell'individualità del lavoratore, andando a fondere la dimensione lavorativa e quella ludica, perdendo così lentamente autonomia e autodeterminazione. Le soggettività del dipendente e del datore di lavoro rischiano quindi di unirsi, poiché il primo è portato a "sentire" i fini dell'azienda come i suoi. Quindi gli elementi di game design lavorano sulla capacità di autodeterminazione del dipendente portandolo a modificare le motivazioni che lo spingono ad agire, passando da eseguire i compiti da "perché deve" a "perché è piacevole". Tramite il gioco il lavoratore viene portato a spingere al massimo le proprie performance lavorative, traendo così piacere da mansioni che normalmente sarebbero noiose. Il paradigma vitruviano dell'uomo autonomo, in controllo di sé e al centro del proprio universo, viene dunque sostituito da un meno appetibile "uomo-criceto" [22], il quale corre e si diverte all'interno della ruota della produzione. Attraverso gli elementi di game design quindi, il lavoratore viene spinto ad ottenere il massimo da sé stesso in contesti noiosi e stressanti in cui in altri casi sarebbe stato difficile fare di più e mantenere la propria performance migliorata per un periodo di tempo continuo come viene richiesto dal datore di lavoro.

2.8.1 Il lato oscuro della Gamification

All'interno dello studio [23] dell'università di Sao Paulo, Brasile, si è andato ad esaminare nel dettaglio quali sono gli effetti negativi dell'utilizzo della Gamification all'interno di contesti educativi. Il risultato ottenuta da questa ricerca ha riportato che sono quattro gli effetti negativi più ricorrenti:

Perdita di performance: il più ricorrente, trovata in ben 12 studi. Questo problema viene creato da alcuni tasks e situazioni nella quale la Gamification risulta dannoso o ostacola il processo di apprendimento degli studenti. La maggior parte degli studi analizzati però hanno riportato dei risultati sia negativi che positivi però nell'applicazione di elementi ludici ad un contesto educativo;

Comportamenti indesiderati: il secondo più ricorrente, presente in 9 studi. Si è manifestato poiché ha causato un differente effetto (positivo o negativo) nel contesto di apprendimento a cui è stato applicato a causa di una cattiva pianificazione oppure di una totale mancanza di essa;

Indifferenza: il terzo in ordine, presente in 6 studi. È stata registrata nei casi in cui l'applicazione della Gamification non ha influenzato gli studenti, né in senso negativo, né positivo;

Perdita di interesse: ultimo ma non meno importante, presente in 5 studi. È collegata alla graduale perdita di motivazioni da parte dello studente. Egli, infatti, comincerà l'attività motivato dagli elementi di Gamification presenti, probabilmente rimarrà in qualche modo deluso da essi e lentamente andrà scemando la sua volontà di continuare. Sebbene sia simile al primo effetto negativo nell'elenco, in realtà lo si può vedere come la causa che porterà poi successivamente alla perdita di performance.

L'approccio comune che ricorreva spesso nei casi presi in considerazione era il PBL, ovvero Point-Badge-Leaderboard (Punto-Badge-Classifica). Essi, infatti, risultano essere presenti in tutti e 4 gli aspetti negativi che sono stati riportati (Fig. 2.12), ciò però non significa che sia errato utilizzarli, bensì che farlo senza un design motivazionale ed istruttivo appropriato sia pericoloso.

Negative Effect	# of elements	Elements	Most impacting element
Indifference	8	Leaderboard, Badge, Level, Progression, Social Status, Point, Instant Feedback, Challenge	Leaderboard and Badge
Loss of performance	11	Leaderboard, Badge, Level, Social Status, Social Interaction, Point, Avatar, Progression, Instant Feedback, Challenge, Economy	Leaderboard, Badge and Point
Undesired behavior	11	Leaderboard, Badge, Point, Level, Instant Feedback, Progression, Social Status, Social Interaction, Avatar, Economy, Narrative	Badge and Leaderboard
Declining effects	4	Leaderboard, Badge, Point, Level	Leaderboard and Point

Figura 2.12: I possibili effetti negativi della Gamification presentati dallo studio dell'università di Sao Paulo, Brasile [23].

Lo scopo di questo studio era quello di analizzare e dimostrare che gli elementi della Gamification vanno utilizzati nel modo corretto, in modo da non incappare in un "malus" piuttosto che in un effetto benefico. L'intento è quello di poter proporre successivamente un approccio guidato all'uso di questi elementi, così da evitare di cadere negli stessi errori che sono stati riportati.

2.8.2 Come evitare i pericoli della Gamification

Si è visto come l'utilizzo errato della Gamification possa portare ad alcuni effetti indesiderati, totalmente anteposti a ciò che si ricerca quando la si vuole applicare. Inizialmente bisogna però capire una cosa fondamentale: predisporre un'iniziativa di Gamification, di qualunque tipo, non è affatto un gioco, come suggerirebbe anche la parola stessa. C'è molto di più oltre ai semplici elementi ludici, infatti attraverso di essi vengono esaminate le interazioni e la psicologia dei partecipanti [46]. Ovviamente, poichè esse hanno a che fare con il modo in cui le singole persone percepiscono le cose intorno a loro, possono facilmente essere fraintese se non ci sta un attento studio dietro di esso. Per prima cosa bisogna evitare che si presenti già in progettazione un certo senso di manipolazione all'interno dell'ambiente gamificato: in questi casi l'approccio "win-win" su cui si basano le ricompense, ad esempio, è destinato a fallire se le persone non si sentono magari appagate dai premi messi in palio e mostrano una certa indifferenza verso gli argomenti a cui sono sottoposti. Altro elemento da tenere sempre in considerazione è l'aspetto serio del prodotto che si propone, d'altronde è proprio la stessa differenza tra Gamification e videogiochi a consegnarci questo importante consiglio. L'apprendimento di uno o più concetti deve restare al centro dell'attenzione e quindi la creazione dell'ambiente "gamificato" deve risultare ben strutturata. Ultimo aspetto, ma non meno importante, è un qualcosa che va oltre gli aspetti psicologici e comportamentali: molti critici, infatti, considerano la Gamification come una moda del momento, visto il suo utilizzo in sempre più occasioni anche solo per rilanciare un brand e considerati i risultati immediati che riesce a procurare. Non deve essere posta sotto quest'ottica, ma bisogna rimanere ancorati al suo scopo principale: aiutare le persone ad imparare concetti, anche difficili, divertendosi. Se venisse integrata maggiormente nella vita quotidiana si potrebbe avere un miglioramento anche dei propri stili di vita. Prendiamo ad esempio gli studenti: al giorno d'oggi sono in molti a sentirsi inadeguati per gli studi che stanno portando avanti, pertanto, probabilmente, applicando alcuni elementi ludici al classico apprendimento, potrebbero portarli a vedere quelle materie particolarmente ostiche da superare come una montagna meno difficile da scalare. D'altronde, per avere la conferma che questa non sarebbe poi un'idea così cattiva, basti pensare anche all'etimologia latina della parola "studio", che, tra i vari significati, riporta quello di "amore", un qualcosa che negli anni moderni si è andato ormai a perdere negli studenti: se portassimo la Gamification in questo tipo di ambiente forse si potrebbe ritrovare il vero significato perduto di questa parola che gli antichi volevano tramandarci, così come riportarla all'interno del

mondo della Cybersecurity risulta essere molto efficace per l'apprendimento e la diffusione dei suoi concetti cardine.

2.9 Analisi delle meccaniche di Gamification

All'interno dei diversi usi della Gamification che sono stati riportati, sono diversi gli elementi attribuibili ad un videogioco. Alcuni sono stati riportati in diversi casi, altri invece solo in alcuni particolari. Analizzando le diverse categorie di meccaniche della Gamification riportate dallo studio di P. Andrade e E. L. Law [24], si potrebbe pensare ad una possibile linea guida da tracciare per indicare in quali contesti sarebbe meglio utilizzare un elemento piuttosto che un altro.

Competizione/Cooperazione: questa categoria di meccaniche è possibile applicarla in ogni contesto, sia lavorativo che educativo in generale. Andare a forgiare lo spirito di squadra dovrebbe essere un "must" per ogni azienda, come potrebbe esserlo anche per uno studente. La competizione invece, dovrebbe essere gestita bene per evitare il problema della perdita di interesse o dell'indifferenza analizzate in [23];

Premi: essi devono andare a ricompensare le scelte corrette prese dall'utente, quindi sono consigliate in qualunque contesto. Poter vantarsi di un achievement raro sbloccato può essere utile anche per alimentare una sana competizione con un collega;

Avventura: l'impronta da gioco di ruolo non è determinante per lo scopo ultimo a cui si punta con la Gamification. Certo, esso risulta essere molto più immersivo rispetto ad un normale quiz game, ad esempio, però non è da escludere la possibilità che alcune persone che non amano particolarmente i videogiochi possano trovare noiosa questa feature. Da utilizzare solo in contesti in cui si è sicuri di avere una maggiore presa, magari con degli studenti interessati al genere;

Progresso: questa categoria è da dividere in due parti: la prima comprende gli elementi che possono essere utilizzati praticamente sempre, come ad esempio i Report e i Feedback, molto importanti per capire dove si sta sbagliando e dove invece si è riusciti ad imboccare la strada giusta; la seconda, invece, comprende meccaniche da RPG (gioco di ruolo) come i livelli, l'esperienza da accumulare;

Sorprese: questa categoria è facoltativa, quindi non è strettamente necessaria. Questi elementi potrebbero allontanarci dal nostro scopo e rendere il nostro sistema come un normale videogioco: può essere qualcosa di simpatico pensare di inserire un Easter Egg o qualche elemento sbloccabile, ma meglio rimanere fermi su ciò che realmente serve.

Un'analisi su quelle che sono le possibili categorie di Gamification applicabili e sulle meccaniche principali utilizzate, viene fatta dallo studio [47]. In esso, infatti, è presente un'analisi di alcuni giochi riguardanti il Phishing nello specifico e che ha portato a creare una divisione della Gamification in due categorie: strutturale, che lascia il contenuto alterato ma rendendo tutto il contorno e quindi la struttura più simile ad un gioco, e riguardo al contenuto, dove avviene il duale. Per quanto riguarda le meccaniche che vanno a formare il nucleo della Gamification, risultano essere i punti, i badges e le classifiche (definita "la triade" all'interno dello studio di F. Tchakounté, L. Kanmogne Wabo e M. Atemkeng [47]), a cui è possibile anche associare i livelli, le sfide o le quest. Uno degli elementi su cui bisognerebbe porre l'attenzione è la distinzione che viene fatta dai normali giochi alla Gamification. Quest'ultima, infatti, risulta essere in contrasto con i primi e le ricompense che si possono ottenere in essi. Ma perché? Semplice: non esiste il fattore dell'intrattenimento, ma solo il divertimento. La vera differenza tra un videogioco qualunque e la Gamification è proprio questo: utilizzare un momento di svago per poter motivare le persone e farle portare a termine dei task che proposte magari con i metodi tradizionali possono risultare alquanto noiose. Ancora una volta, l'uomo e le sue emozioni sono messi al centro dell'attenzione, d'altronde fare leva su di esse sembra essere un metodo molto producente. È importante anche

la classificazione dei design per la Gamification, tra i quali ne risultano quattro a fronte delle ricerche e studi da cui sono stati analizzati: User-Centered Design, MDA framework, il framework di Schell e quello di Werbach e Hunter. Sarà proprio sul primo caso di design analizzato qui che verrà poi focalizzata l'attenzione più avanti.

2.10 Yin e Yang: è giusto usare la Gamification?

Dopo aver analizzato gli aspetti positivi e negativi dell'utilizzo della Gamification, la domanda che ci si pone è la seguente: è un bene fare affidamento sugli elementi ludici per insegnare concetti importanti, come la Cybersecurity, oppure il gioco non vale la candela ed i rischi sono troppo grandi rispetto ai possibili "guadagni"? La risposta è sì, è uno strumento molto utile e non utilizzarlo sarebbe uno spreco. In tutte le cose ci sono bonus e malus, per rimanere in tema videoludico, ed è lo stesso concetto che accompagna lo yin e lo yang. La cosa importante è saper utilizzare gli strumenti che la Gamification ci mette a disposizione, poiché ignorarne l'utilità sarebbe un male. Bisogna saper trovare un equilibrio nelle cose, senza arrivare al punto di mettere in pericolo la privacy delle persone o avere l'effetto inverso da quello sperato e arrivare ad avere un impiegato svogliato e indifferente. È una cosa sicuramente fattibile, basta solo fare attenzione a come vengono poste le cose e ricordarsi sempre che il punto al centro di tutto lo schema è trasformare l'uomo da punto debole nella catena della sicurezza a punto forte, concetto ripreso bene dagli studi di Human Computer Interaction, dove appunto l'utente finale del sistema rimane al centro durante tutta la catena di produzione.

Capitolo 3

La Human Computer Interaction

La scelta di mettere l'utente al centro di tutto, come specificato all'interno dello studio [19], è una scelta comune all'interno del processo di creazione di un applicativo basato sul processo di "User-centered design", uno dei fondamenti alla base degli studi di Human Computer Interaction (HCI). Il suo scopo è quello di limitare i fallimenti del progetto prendendo quelle che sono le necessità e le richieste di coloro che, orientativamente, potrebbero rappresentare il bacino di utenza del sistema che si andrà a sviluppare. Il risultato ottenuto dopo gli studi effettuati è più semplice da capire, con performance migliori e meno errori umani nell'utilizzare l'applicazione, incoraggiando anche l'utente a scoprire le caratteristiche più avanzate ed evitando di creare dei sistemi costruiti male già dall'inizio.

3.1 Human Computer Interaction: un connubio di discipline al servizio dell'utente

La Human Computer Interaction si occupa dei problemi connessi alla progettazione di interfacce uomo-macchina, cercando di offrire utili strategie e suggerimenti nel tentativo di rendere possibile un'efficace interazione fra l'utente ed il computer. Essa costituisce un ambito interdisciplinare di ricerca nato nel momento in cui i ricercatori si sono resti conto che i problemi relativi all'organizzazione e alla gestione del lavoro, insieme alla salute e ai fattori neuro fisiologici e ambientali, possono influenzare l'interazione tra uomo e computer. Ad occuparsi di questi problemi sono discipline quali l'ergonomia cognitiva, la psicologia, le scienze cognitive, l'informatica, l'industrial design e molte altre che collaborano al fine di completare in ogni suo aspetto il processo di HCI [25]. All'inizio il nome che si utilizzava per riferirsi a questi studi era man-machine-interaction (MMI), successivamente trasformatosi in Human Computer Interaction per il particolare interesse mostrato verso i computer e i loro utilizzatori. Si può pensare che abbia ripreso lo scopo della nascita dell'ingegneria industriale nel XIX secolo, creata per progettare strumenti e soluzioni che andassero a ridurre la fatica dei lavoratori e a migliorare la qualità della vita all'interno dei luoghi di lavoro. La HCI si è quindi evoluta partendo da discipline appartenenti a vari settori, ad esempio la computer graphics ha contribuito nella creazione di nuove tecniche di interazione tra uomo e computer, sviluppando dei sistemi come il CAD o il CAM (Computer Aided Design e Computer Aided Manifacturing) che permettono di "manipolare" oggetti virtuali come se realmente presenti nelle mani dell'utente. Altra disciplina da cui ha appreso molto e preso i principi è la psicologia cognitiva, la quale ha orientato i suoi studi verso l'uomo, inteso come elaboratore di informazioni ed esecutore di compiti, e si è concentrata sulla sua capacità di apprendere l'uso di sistemi, sulla rappresentazione mentale di essi e sulle prestazioni nelle interazioni uomo-macchina. Anche la linguistica ha dato il suo contributo, per esempio nello studio delle interfacce che utilizzano il linguaggio naturale; pertanto, risulta essere fondamentale comprendere la struttura sintattica e semantica della conversazione umana. Ma il campo della HCI è così ampio da coinvolgere anche la usability e l'ergonomia: quest'ultima ha apportato il suo contributo determinando le costrizioni del design dei sistemi e suggerendo specifiche linee guida e standard da osservare in fase di progettazione; la prima, invece, esprime quanto bene un utente riesce ad utilizzare tutte le funzionalità

di un sistema, comprendendo diverse "dimensioni" su cui andare a calcolare tale valore: l'utilità, l'apprendibilità, la facilità nel ricordare le varie funzionalità una volta apprese, l'efficacia, l'efficienza, la visibilità dello stato del sistema, la possibilità di avere degli errori recuperabili ed infine la godibilità del sistema.

I computer non sono utilizzati soltanto da esperti, ma da una vasta gamma di utenti per scopi lavorativi, ludici e educativi. Questo ha portato i progettisti dei sistemi computerizzati a cercare delle soluzioni che si adattino ai diversi tipi di bisogni che un utente possa avere, senza però arrivare a creare una soluzione personalizzata per ogni singola persona, ma venendo incontro ai bisogni e alle capacità di classi di fruitori. Gli obiettivi della HCI sono quelli di costruire dei sistemi utili, sicuri, usabili e funzionali, coinvolgendo nel processo di creazione quattro elementi: l'uomo, la macchina, l'attività da svolgere ed infine l'usabilità. Se un sistema forza l'utente e lo mette in difficoltà nello svolgere il suo compito, ciò significa che non ha un buon grado di usabilità. Uno degli elementi che ne fa da padrone al suo interno è sicuramente la UX, ovvero la User Experience, la quale studia in maniera dettagliata l'intera esperienza con il prodotto da parte dell'utente: essa focalizza la sua attenzione su problemi relativi all'usabilità, al carico cognitivo e più in generale all'esperienza che viene proposta. A questi si è aggiunto negli ultimi anni anche un altro fattore, la motivazione che spinge l'utente ad utilizzare un determinato prodotto o sistema. Anche per questo motivo la HCI si è avvicinata alla Gamification [26], in modo da trovare un metodo per poter motivare l'utente ad utilizzare il prodotto con voglia. Lo studio della Gamification nella Human Computer Interaction ha preso posto in una sottocategoria denominata "Player Computer Interaction", in breve PCI, la quale si occupa di studiare a sua volta la PX, la Player Experience. Come rivelato però all'interno di [27], sebbene la Gamification abbia comunque un intento positivo con le sue ricerche, riceve continuamente critiche da parte dei ricercatori di giochi non-HCI: esse si concentrano principalmente nel descriverla come "espediente di marketing", andando perciò anche ad influenzare la reputazione in senso negativo. Queste critiche che arrivano da fuori non devono però scoraggiare, semmai possono solo spronare a fare meglio, basti pensare che gli studi di PCI coprono oltre il 40% delle ricerche sui giochi all'interno della CHI. Si è comunque visto come esistano gli elementi negativi della Gamification, tutti rischi a cui si potrebbe arrivare nel caso la si utilizzi nella maniera sbagliata, come anche risulta tale una scelta errata di design all'interno della HCI, in quanto può portare a molteplici errori dell'utente. Bisogna prendere però i lati positivi di questi elementi e limitare quelli negativi: la critica, se costruttiva, va accettata e può portare anche ad un notevole miglioramento. Al giorno d'oggi la Gamification è ampiamente adottata per quanto riguarda il design, visto che il suo aiuto nel risolvere problemi presenti nella User Experience è davvero utile. Il suo corretto utilizzo e le eventuali meccaniche di gioco selezionate possono diventare un'arma potente per gli UX designers, questo perché viene introdotto il concetto di divertimento all'interno dell'applicazione o del sito web in considerazione. Ancora una volta i sentimenti degli utenti vengono considerati il fattore determinante: provando un certo piacere nell'utilizzare il sistema grazie proprio a questi elementi ludici, gli utenti sono portati ad utilizzarlo nuovamente per poter guadagnare altri premi magari o per competere con i propri amici e colleghi per superarli nella classifica generale. Ad oggi la Gamification è uno degli approcci più utilizzati tra i designers, i quali ne hanno colto le qualità migliori e portato la sua popolarità alle stelle, candidandola ad essere quindi uno dei pilastri portanti per un buon design.

3.2 L'interazione tra macchina e uomo

Lo studio principale su cui si focalizza la HCI è sicuramente l'interazione dell'uomo con il sistema computerizzato, andando a sviscerare nel dettaglio ogni elemento ad esso collegato. Ad esempio, all'interno del modello di interazione di Norman si può notare la creazione di un ciclo di comunicazioni tra l'utente ed il sistema, con la seguente creazione di due grandi "golfi": il primo relativo all'esecuzione dell'azione da parte dell'utente interagendo con il sistema, con attenzione particolare su quale sia il suo obiettivo finale, come è intenzionato ad eseguire le azioni che porteranno alla destinazione da lui ricercata, quale sequenza di azioni andare ad eseguire ed infine l'azione vera e propria; il secondo relativo alla valutazione, dove in output al sistema avremo lo stato di esso, la sua interpretazione e la valutazione che è stata definita portando avanti l'esecuzione dell'utente (Fig. 3.1) [28].

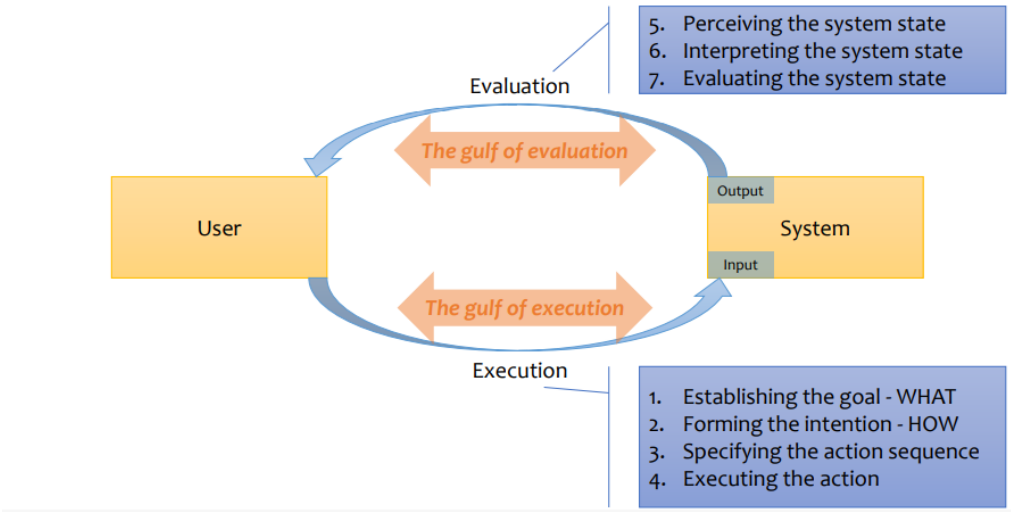


Figura 3.1: Il modello di interazione "Uomo-Macchina" teorizzato da Normann.

Senza alcun dubbio non si possono escludere degli errori possibili in entrambe le fasi: infatti, si parla di "Slip" nel caso in cui avvenga durante l'interazione dell'utente con il sistema e quindi la generazione del suo input, mentre si parla di "Mistake" quando avviene durante la creazione dell'output del dispositivo da far visualizzare alla persona che attualmente lo sta utilizzando. Il primo caso si ottiene nel caso in cui si effettui l'azione corretta ma si fallisce nell'eseguirla, ad esempio cliccando l'icona adiacente a quella corretta, niente a cui un'interfaccia migliore non possa porvi rimedio; il secondo fa riferimento all'idea sbagliata che l'utente si è fatto del sistema: un esempio è quello che avviene quando un utente clicca sull'icona di una lente d'ingrandimento pensando che serva per lo zoom, mentre in realtà abilita la funzione di ricerca. La soluzione a questo problema è un redesign dell'applicativo radicale. In entrambi i casi l'errore non è mai da attribuire alla persona che utilizza il prodotto che gli viene proposto, ma, come lo stesso Norman afferma, "rappresenta di solito il risultato di un design errato". Dopotutto l'essere umano tende ad essere impreciso, distratto, non onnisciente, deve essere il sistema ad anticiparlo ed evitare che cada in errore, minimizzando durante la valutazione azioni inappropriate e massimizzando durante l'esecuzione la possibilità di scoprire e riparare un'azione inappropriata.

3.3 Il processo di design "Human-centered"

Il focus della HCI è quindi quello di creare un sistema di interazione con una particolare attenzione sull'usabilità di esso. Per arrivare a questo obiettivo si segue un particolare processo definito "Human-centered" che, come suggerisce anche il nome stesso, pone al centro di tutto l'uomo e quindi l'utente (Fig. 3.2) [28].

Come è possibile osservare anche dall'immagine, il processo si articola in cinque passi:

Requisiti: è la fase in cui si effettua una ricerca su cosa sia necessario per l'utente ed eventualmente come viene raggiunto l'obiettivo. Per scoprirlo si effettuano alcune interviste o semplicemente un'osservazione delle interazioni;

Analisi: avviene la formalizzazione e la strutturazione dei requisiti. Viene quindi paragonata la situazione attuale con quella che ci si aspetta;

Design: vengono prese le decisioni principali per andare a strutturare la forma del sistema attraverso regole, linee guida e principi di design. Vengono modellate e descritte le possibili interazioni, considerando tutti i diversi tipi di utente;

Interazione e prototipazione: fase di supporto, la quale provvede ad una verifica intermedia del sistema grazie ad alcune metriche di valutazione e soprattutto all'utilizzo di prototipi.

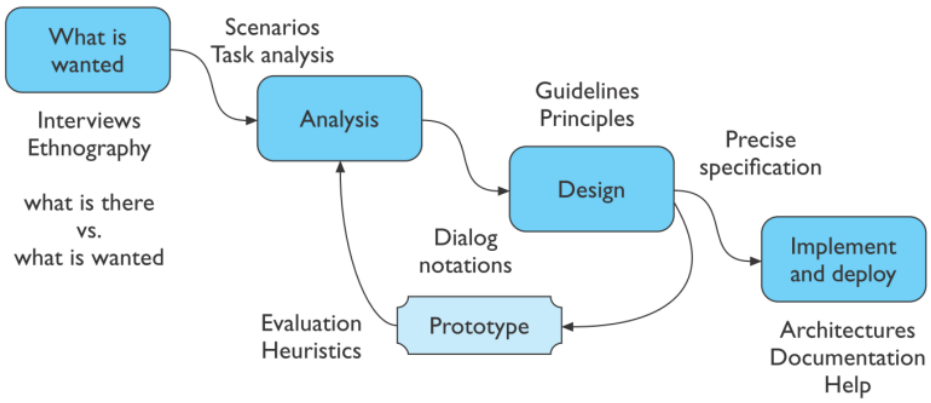


Figura 3.2: Il processo "Human-centered" proposto dagli studi di Human Computer Interaction.

Vengono coinvolti nel processo anche gli utenti e, nel caso in cui vengano sottolineate alcune problematiche, si ricomincia dalla fase di analisi;

Implementazione e sviluppo: ultima fase accessibile alla fine di tutti i test. Vengono implementati l'hardware e il software, insieme alla documentazione.

3.4 La ricerca del design giusto

Per avere un sistema che faccia riferimento allo User Centered Design bisogna attraversare diverse fasi. Si parte da quella forse più importante, considerando l'idea di fondo di lasciare al centro di ogni cosa l'utente: la ricerca dei bisogni, detto anche "Needfinding". In queste prime battute del progetto lo scopo è ricercare, attraverso interviste o osservazioni, quelli che sono attualmente i bisogni dei possibili utenti: quest'ultima parte è da tenere sempre in considerazione, in quanto non si costruirà un sistema diverso per tutte le persone che andranno ad utilizzarlo, bensì si avrà la copertura di diverse categorie di utenti denominate "personas". Esse non sono altro che delle descrizioni dettagliate di utenti fittizi ma verosimili che riflettono i diversi tipi di persone che potrebbero usare l'applicativo.

Una volta definite le necessità da ricoprire con il sistema da sviluppare, si passa all'analisi del task, ovvero il processo di apprendimento sugli utenti ordinari osservati in azione per scoprire nel dettaglio come eseguono le loro task e come ottengono i loro obiettivi. Questa fase aiuta a capire quali sono le attività che dovrebbero essere presenti nell'applicazione, a raccoglierne i requisiti e a formulare le prime teorie per un prototipo sul quale sarà possibile, in un secondo momento, andare a performare i test di usabilità. Quest'ultima parte rappresenta anche la fase successiva, nella quale si mette in pratica tutto ciò che è venuto fuori dalla fase di analisi e si arriva alla creazione di una versione "alpha" del sistema. Basandosi sui principi di design, esso permetterà di correggere gli errori di progettazione che sono stati fatti, creando quindi un'applicazione finale migliore. Esistono diversi tipi di prototipo, ognuno con una fedeltà più o meno alto al prodotto finale [28]:

Prototipo di carta: il più semplice ed efficace, consente di iniziare ad utilizzare l'applicazione mesi prima della sua effettiva implementazione. Permette di avere un'interazione naturale (puntare un'icona, ad esempio, con il dito equivale a cliccare con il mouse), è veloce da costruire, facile da cambiare anche in corso d'opera e soprattutto anche chi non si intende di programmazione può aiutare. Da esso si possono evincere il modello concettuale, la funzionalità, la navigazione e i contenuti da presentare sullo schermo, d'altro canto non si riesce ad avere un riscontro sull'aspetto dell'applicazione, il tempo di risposta ed eventuali problemi di efficienza;

Prototipo a video: consiste nel riprendere l'utilizzo di un prototipo di carta. Con esso ci si può concentrare nel messaggio che si vuole dare piuttosto che sulla qualità della produzione. Può anche essere un video senza alcun suono ma con dei fogli che descrivono le azioni che si vanno a riprodurre, in modo da evitare problematiche relative all'audio;

Wireframe: rappresentazione di una o più schermate connesse. Si passa a mettere mano al computer per questo tipo di prototipo, sebbene si abbiano ancora dei disegni simili a quelli fatti a mano per dare l'impressione che il design sia ancora preliminare e l'intera struttura non presenti ancora i colori. La cosa più importante è la possibilità di rappresentare il dispositivo con il quale l'utente finale interagirà per usufruire del sistema;

Prototipi ad alta fedeltà: creazione di applicazioni vere e proprie che presentano il layout finale, colori e grafiche. La scelta più costosa tra tutte, sia per il denaro da investire che per il tempo di preparazione.

La scelta di utilizzare un tipo di prototipo a discapito di un altro è da attestare ad un'attenta analisi sul budget a disposizione e soprattutto sui test da eseguire su di esso. Questa è probabilmente la fase più lunga poiché richiede molti tentativi per arrivare ad una fase finale di sviluppo e documentazione. In tutto il processo, comunque, si nota come il punto in comune tra tutte le fasi sia sempre lo stesso: l'utente. La scelta di posizionarlo al centro del progetto è stata già menzionata dagli studi sulla Gamification riportati in precedenza, come nello studio dell'università norvegese [19] dove la fase di creazione del prototipo è stata preceduta da una serie di interviste preliminarie. Il prototipo che è stato creato come risultato degli studi è solo una prima versione e l'esperienza che ne è scaturita dall'utilizzo è stata registrata attraverso un questionario post utilizzo, in modo da avere il responso degli utenti su quelli che sono stati i punti di forza e soprattutto quelli deboli, così da migliorare ove necessario. Il percorso per arrivare al sistema finale ancora è lungo probabilmente e non privo di errori, ma, alla fine, produrrà un sistema dall'alta usabilità e che potrà esprimere al meglio le sue funzionalità.

3.5 Come l'HCI viene incontro all'anello debole

Si è già detto che, all'interno di tutta la catena protettiva che viene creata per la prevenzione dagli attacchi informatici, l'uomo è di sicuro il punto debole, come affermato anche da Poulsen: "il lato umano della sicurezza informatica è facilmente sfruttato e costantemente trascurato. Le compagnie spendono milioni di dollari per firewall, crittografia e accessi sicuri ai dispositivi, tutto denaro sprecato poiché nessuna di queste misure è indirizzata all'anello debole nella catena della sicurezza". È stato anche visto in precedenza come sia facile entrare nella mente dell'uomo tramite la sua innata empatia e fiducia verso il prossimo. Come possiamo dunque definire un sistema sicuro, se lasciamo sempre in bella vista il punto debole al nemico? Schneier [29] afferma che "la sicurezza è da considerare buona quanto il suo collegamento più debole", riferendosi anch'egli alle persone come target predefinito degli attacchi. Tutto ciò però deve essere analizzato attentamente e in questo la Human Computer Interaction può dare un sostanziale aiuto. Infatti, come presente anche nello studio di M. A. Sasse, S. Brostoff e D. Weirich [29], indicare l'uomo come "weakest link" porta quindi a puntare il dito contro di lui per ogni problematica, cosa che è assolutamente negata dalla HCI. Quando si presenta un errore qualunque bisogna risalire fino alla fonte che lo ha provocato, come se volessimo seguire un fiume per scoprire da dove sgorga la sua acqua. In questo modo si arriva al design dei sistemi utilizzati, i quali non riescono a far intendere bene all'utente come interagirci, specialmente per quanto riguarda i punti più critici per la sicurezza, cosa che è andata avanti fino alla fine degli anni Ottanta. Come analizzato anche da Adams e Sasse, la sicurezza ha largamente ignorato i problemi di usabilità, facendo in modo che i suoi utenti affrontassero richieste irraggiungibili o contrastanti senza ricevere alcun supporto o addestramento, lacuna che può essere colmata grazie alla Human Computer Interaction, il cui approccio alla creazione del design si basa sul voler aiutare l'utente a completare la propria "task". Sempre Adams e Sasse hanno investigato su come vengano percepiti i meccanismi delle password ed è stato rivelato che la conoscenza di molti utenti sull'argomento è incredibilmente inadeguata, portando quindi a creare un proprio modello inaccurato sulle possibili minacce alla sicurezza e sull'importanza di quest'ultima. Uno dei punti più importanti espressi all'interno dello studio [29],

è sicuramente la visione della sicurezza dalla prospettiva del task: non è altro che un passaggio abilitante da completare per poter passare al compito principale da svolgere: un esempio ne è l'autenticazione, percepita come il passaggio intermedio per poter accedere a risorse personali. Questa visione è in realtà condivisa da molti utenti, i quali vedono la sicurezza come qualcosa che si pone in mezzo tra loro e il lavoro che devono portare a termine. Perciò, come riportato anche dallo studio [29], la persona deve essere motivata a fare questo "sforzo aggiuntivo" per poter utilizzare nella maniera corretta i meccanismi di sicurezza. Come rivelato anche all'interno dello studio di M. M. Eloff e J. H. P. Eloff [31], sono due principalmente i problemi che riguardano il rapporto tra l'utente e la sicurezza: la complessità di quest'ultima e la difficile realizzazione della creazione di un'interazione sicura con il sistema su cui si sta lavorando. Infatti, se si pensa all'utilizzo delle password, molte volte per evitare di dimenticarle le si scrive su un foglio, lasciandolo a volte anche in bella vista. La complessità della sicurezza poi è da sempre il suo nemico più grande, portando le persone ad evitarla proprio a causa sua. Le sue caratteristiche da utilizzare devono essere affidabili in primis, ma soprattutto semplici da utilizzare. Come dice anche Schneier [30], la sicurezza delle informazioni è più facile da implementare quando è visibile all'utente, in modo da poter prendere le sue decisioni basandosi su di essa. Bisogna comunque tenere in considerazione che non tutte le persone hanno interesse nel vedere come un file viene criptato: se il sistema è affidabile il grosso del lavoro può essere anche fatto in background, senza che l'utente venga a conoscenza di cose che non sono nel suo interesse. Dunque, in che modo è possibile far accrescere la motivazione di una persona, portandola ad essere soddisfatta anche di quello che sta facendo, e riducendo quel divario tra utente e sicurezza imposto dalla complessità di quest'ultima? Una ricompensa per il lavoro svolto, ad esempio, oppure la soddisfazione personale di aver battuto un proprio collega. Competizione, intrattenimento, ricompense, sono tutti elementi che fanno parte del mondo della Gamification, andando quindi a rimarcare come la convivenza di essa con la HCI sia possibile e, anzi, sia necessaria per poter avere il miglior risultato possibile.

3.6 Siamo forse troppo pigri?

Gli studi di Human Computer Interaction si fondano su quelli che sono i bisogni degli utenti e sulla ricerca del design ottimale per rendergli la vita più semplice. Ma questa ricerca della perfezione per quale motivo è così importante? È molto semplice: la motivazione la si può trovare considerando l'indole innata dell'essere umano di ricercare sempre la via più breve, quella che porta più facilmente al proprio obiettivo senza doversi sforzare eccessivamente. Tenendo questa cosa in considerazione, può sembrare normale quindi avere una cosa come la Cybersecurity al secondo posto, non perché sia meno importante, ma perché richiede molto tempo, è un processo molto lungo e deve anche diventare un elemento della vita quotidiana di ognuno di noi. D'altronde, se siamo così pigri nel mondo vero, cosa ci fa pensare che non lo siamo anche in quello virtuale [32]? La colpa di queste cose non deve essere mai data all'utente, bensì ad una scarsa attenzione sul design creato per lui. Riprendendo le cosiddette "regole d'oro per il design di un'interfaccia", si può notare come alcune di esse vengano quasi ignorate nel mondo della sicurezza informatica. L'esempio più comune è la password: essa dovrebbe essere, secondo i buoni principi della Cybersecurity, solo all'interno della testa dell'utente, ma molte volte questa cosa non accade e viene magari scritta su un foglio di carta. In questo caso si fa troppo affidamento sulla memoria delle persone, credendo che esse siano tutte in grado di ricordare ogni cosa. Un altro esempio comune è l'autenticazione a due fattori: questa richiede l'accesso a due dispositivi di solito nello stesso momento (ad esempio il computer e il telefono cellulare), rendendo la cosa molto tediosa. Tutto questo per confermare la tesi di partenza: la Cybersecurity è noiosa. Ma non l'argomento in sé, bensì i modi con i quali viene applicata risultano tediosi. Probabilmente è questo il motivo che ha spinto ad utilizzare la Gamification, cercare un modo per rendere più piacevole l'argomento, cercando di venire incontro a quei bisogni primordiali di tutti noi: trovare la strada più facile e meno dispendiosa di energie. Applicando quindi le conoscenze della HCI e la Gamification alla Cybersecurity, si potrebbe creare un sistema che soddisfa le necessità dell'utente, non lo annoia e soprattutto è utile per poter diffondere l'importanza della sicurezza informatica.

3.7 Le emozioni ci rendono quelli che siamo

All'interno dei vari studi che sono stati proposti, sembra essere ricorrente l'utilizzo della gestione delle emozioni dell'utente. Perché tutta questa attenzione rivolta su di esse? Se ci si pensa, sono esse a renderci veramente "umani": paura, gioia, tristezza, felicità, sono tutte caratteristiche che vanno a definire l'individuo e lo differenzia dall'altro per come le esterna e le prova. Questo focus, quindi, è più che giusto da parte della HCI: tra le varie componenti che la compongono sono anche presenti psicologia e scienze cognitive, il cui scopo è quello di scavare all'interno dell'uomo e capire quali sono i suoi pensieri. Le emozioni, insieme anche alla parte razionale che ci caratterizza, definiscono anche le azioni che tutti noi eseguiamo ogni giorno e, se si porta l'esempio nel campo della sicurezza informatica, risulta essere anche la chiave di volta negli attacchi basati su social engineering e phishing. Lo studio delle emozioni provate dalle persone è quindi fondamentale anche per la possibile strutturazione di un applicativo o un sistema da utilizzare. Molte volte la noia o la difficoltà possono portare l'utente a smettere di utilizzarli, stessa sorte che purtroppo tocca anche alla Cybersecurity. All'interno dello studio di I. Cristescu [33] viene posta la giusta domanda: qual è la connessione tra emozioni e design? L'emozione è una delle più grandi differenze nelle esperienze degli utenti, in quanto attiva quel meccanismo nel nostro subconscio che ne influenza la percezione durante l'utilizzo del sistema e può cambiare anche il tipo di coinvolgimento in un uso futuro. Tutto ciò porta, quindi, ad un redesign indirizzato a sfruttare le emozioni del possibile utente, in modo tale da spingerlo ad utilizzare l'applicativo che si vuole sviluppare, portando alla nascita del "design emotivo". Un esempio di sfruttamento delle emozioni all'interno della Gamification lo si può trovare in [34], dove viene proposta una storia gamificata, incentrata completamente sulla speranza, ad una classe scolastica. La tematica scelta, infatti, non rappresenta solamente un'emozione positiva, ma risulta essere anche uno schema motivazionale che sprona gli utenti a raggiungere gli obiettivi preposti. Da qui possiamo capire bene come siano potenti le emozioni umane: se soltanto l'idea della speranza in qualcosa porta l'uomo a superare i suoi limiti, pensare a quello che si potrebbe raggiungere coinvolgendo anche le altre potrebbe non avere alcun limite nel potenziale. Pensando alla Gamification, il suo scopo è quello di divertire, proponendo quindi un nuovo punto di vista all'utente diverso dalla solita monotonia grigia. Si potrebbe pensare al sistema che vogliamo sviluppare come una grande tela: la HCI ci permette di disegnare i lineamenti del quadro, definendo la base dell'opera. Se si esponesse così, potremmo già capire a cosa si riferisce l'opera, riuscendo magari a distinguere il contorno relativo ad una montagna rispetto a quello degli alberi, un po' come se stessimo leggendo un fumetto in bianco e nero. Ma aggiungendo il colore, nel nostro caso la Gamification, rendiamo il tutto più chiaro grazie anche alle sue diverse tonalità utilizzate (punti, badges, classifiche). Adesso che vediamo il quadro al completo, ci si potrebbe domandare quale sentimento ci faccia provare oppure quale messaggio volesse trasmettere l'autore, ed è proprio qui che entrano in gioco le emozioni. Ognuno proverà una sensazione diversa osservando il cielo dipinto, alcuni possono provare serenità, altri tristezza o altri ancora rabbia. Avvicinarsi ad esse e accoglierle potrebbe rivelarsi un'analisi importante, cercando di capire quali siano le emozioni prevalenti e magari anche il motivo che le provoca.

3.8 Testare i propri sistemi per certificare quanto siano sicuri

Come già visto nei capitoli precedenti, applicare la tattica militare del "conosci il tuo nemico" sia un metodo efficace per poter migliorare la propria attenzione sulla sicurezza (§ 2.6), capendo in anticipo i possibili movimenti degli attaccanti. Con l'aiuto della Human Computer Interaction è possibile raffinare ulteriormente questa tecnica, arrivando al punto di entrare nella mente degli attaccanti. Questo è possibile grazie alle molteplici discipline che lavorano al suo interno, le quali portano ad avere per ovvi motivi il focus sulle interazioni fisiologiche delle persone con le macchine. Basti pensare al design di tipo User centered: mette al centro l'utente, i suoi bisogni e le tasks che deve effettuare per poter sviluppare la migliore interfaccia possibile in termini di interazioni e soddisfazione visiva: si potrebbe paragonare questo genere di rapporto con quello che Tony Stark ha con la sua armatura, come citato in [35]. La possibilità di mettersi nei panni degli attaccanti è stata utilizzata anche da persone che non hanno a che fare con il mondo della

Cybersecurity, ma che hanno voluto provare per vedere quanto effettivamente siano al sicuro i propri dati e le proprie password. Un esempio lo ha portato l'eccentrico e mai banale Mark Cuban, proprietario dei Dallas Mavericks, squada che milita nella NBA. Come riportato anche da [36], ha provato un penetration test per tentare di accedere al suo Cloud di Apple e i suoi risultati hanno confermato quello che molte compagnie prima di lui avevano già attestato: per quanto le tecniche di sicurezza utilizzate siano all'avanguardia ed avanzate, possono essere sempre aggirate anche solo tramite una ricerca di Google. Grazie a questa sua ricerca fatta solo per pura curiosità, è stato spinto a incitare i suoi amici a provare questo test per i loro account e, cosa più importante, a cambiare le domande di sicurezza, le quali potrebbero essere scoperte semplicemente cercando sulla rete, e anche le sue attuali password, rendendole più difficili da scoprire. Il fattore psicologico ha influenzato molto le decisioni di Mark Cuban: la paura di perdere i propri dati e di vedersi sottratte le sue informazioni private hanno apportato un cambiamento in lui. Anche questo ci dimostra come, sotto una giusta quantità stress, nel suo caso auto-procurata dalla sua curiosità, temendo per la nostra sicurezza, si possano cambiare le proprie abitudini, andando ad adeguarle con le buone norme di Cybersecurity. Un passo questo che è possibile rendere più abbordabile grazie alle pratiche di HCI, le quali dei bisogni, delle emozioni e delle interazioni ne fanno il loro pane quotidiano.

3.9 Implementare la sicurezza nella HCI

Come è stato anche illustrato nel paragrafo precedente (§ 3.8), non sempre i sistemi che prendiamo in considerazione sono totalmente esenti da elementi di sicurezza, in quanto potrebbero essere semplicemente implementati male oppure presentare problemi di design. L'usabilità deve comunque rimanere al centro di tutte le applicazioni di HCI, a maggior ragione quando si toccano tematiche così importanti come la sicurezza informatica. Da qui la nascita di "un nuovo ramo": HCI-S, ovvero Human Computer Interaction-Secure. La definizione è la seguente: "parte dell'interfaccia utente responsabile di stabilire un luogo comune sia all'utente, sia ai features di sicurezza di un sistema. È quindi l'applicazione dei concetti di HCI all'area relativa alla sicurezza". Questa definizione, ripresa dallo studio di D. Katsabas, S. M. Furnell e A. D. Phippen [37], definisce una cosa di vitale importanza: il punto d'incontro tra utente e sicurezza: se non esistesse ci sarebbero problemi per l'utente, il quale non sarebbe in grado di relazionarsi con le opzioni che sono messe a sua disposizione. Lo scopo ultimo della HCI-S è quindi quello di rendere un sistema computerizzato più robusto, affidabile e sicuro attraverso miglioramenti dell'interfaccia dell'applicazione. La ricerca effettuata all'interno di [37] ha portato a riscrivere le 10 euristiche dell'usabilità teorizzate da Nielsen, aggiungendo in esse l'elemento sicurezza:

Funzioni di sicurezza e stato del sistema visibili: non ci si deve aspettare che l'utente effettui una ricerca per trovare gli strumenti della sicurezza o eventuali features nascoste, deve essere sempre informato sullo stato del sistema;

La sicurezza deve essere facile da utilizzare: il design dell'interfaccia deve essere tale da richiedere uno sforzo minimo per poter utilizzare le features sulla sicurezza implementate, raccogliendole tutte in un unico posto;

Semplice da usare per novizi ed esperti: il sistema deve poter essere facile e accessibile sia per utenti alle prime armi, che per quelli già navigati;

Evitare l'utilizzo di un vocabolario tecnico: un utente alle prime armi può trovare difficili le features di sicurezza se sono presenti solamente parole che esprimono dei tecnicismi e un vocabolario differente dal suo;

Gestire gli errori correttamente: non è possibile eliminare ogni errore da un sistema, ma si può rendere semplice il recupero da esso e minimizzare il loro numero. Gli eventuali messaggi di errore devono essere significativi e reattivi al problema che è sorto;

Permettere la personalizzazione senza essere "intrappolati": nel caso in cui venga scelta una funzionalità per sbaglio, il percorso da seguire per tornare al punto di partenza deve essere ben chiaro all'utente, in modo che non entri nel panico e abbia paura di aver fatto un errore irreparabile;

Semplicità nell'impostare le impostazioni di sicurezza: in questo modo l'utente si sentirà più confidente a configurare l'applicazione in base alle sue necessità;

Documentazione e aiuto per la sicurezza sempre a disposizione;

Trasmettere sicurezza all'utente: chiunque usi l'applicazione deve sentirsi protetto mentre la utilizza, sia dal punto di vista della sicurezza, mettendo a disposizione le ultime caratteristiche relative ad essa, sia nel caso in cui sbagli un'operazione e debba tornare sui suoi passi;

La sicurezza non deve ridurre le prestazioni: progettando l'applicazione con attenzione ed utilizzando algoritmi efficienti, dovrebbe essere possibile poter utilizzare le caratteristiche della sicurezza con un impatto minimo sull'efficienza dell'applicazione.

Di tutte le euristiche rivisitate, l'ultima è quella decisamente più importante. Il problema più grande che la Cybersecurity si porta dietro da sempre è il suo rapporto particolare con le performance. Essi, infatti, sono da sempre visti come due elementi inversamente proporzionali, senza trovare un equilibrio che possa essere ritenuto soddisfacente da entrambe le parti. Se grazie all'inserimento della HCI è possibile anche sconfiggere questo difetto, allora potremmo fare un gran bel passo in avanti verso un modello da seguire più sicuro, senza dover pagare la "tassa" relativa alle prestazioni: bisogna sempre tenere in considerazione che anche per la parte della HCI improntata alla sicurezza, l'utente rimane ancora una volta al centro dell'attenzione, garantendogli la creazione di un sistema usabile e sicuro. All'interno dello studio di R. Kainda, I. Flechais e A. W. Roscoe [38], viene proposto un nuovo modello relativo alle minacce alla sicurezza, il quale va a differenziarsi da quelli standard per il proprio focus: si passa dagli attaccanti malevoli ai possibili errori commessi dagli utenti legittimi che potrebbero compromettere il sistema.

Usability		**Security**	
Factor	**Measurable metrics**	**Factor**	**Measurable metrics**
Effectiveness	task success	Attention	Attention - failures
Satisfaction	Satisfaction	Vigilance	Vigilance - failures
Accuracy	Success rates	Conditioning	Conditioning - failures
Efficiency	Completion times, number of clicks/ buttons pressed	Motivation	Perceived, benefits, susceptibility, barriers, severity
Memorability	Recall	Memorability	Recall
Knowledge/ skill	Task success, errors, mental smodels	Knowledge /skill	Task success, mental models
		Social context	Social behaviour

Figura 3.3: I fattori e le metriche utilizzate per valutare Usabilità e Sicurezza [38].

L'obiettivo, quindi, risulta essere sempre lo stesso: ridurre i possibili errori degli utenti al minimo. In questo caso, l'errore umano potrebbe portare ad un attacco con successo con conseguenze non piacevoli, pertanto è utile soffermarsi su queste metriche di misura relative alla sicurezza, oltre che sull'usabilità, per il sistema che andiamo a prendere in considerazione. Proprio su quest'ultimo punto bisogna fare particolare attenzione, poiché si riferisce anche ad uno dei punti chiave del lavoro della HCI: tenendo conto dei fattori di usabilità riportati dalla tabella precedentemente presentata e dai punti illustrati da [39] riguardanti ai suoi componenti qualitativi, si può arrivare alla creazione di un sistema con un alto livello di usabilità, il quale porta anche l'utente a non inciampare in errori banali durante l'utilizzo. L'importanza di un sistema intuitivo, efficiente, programmabile, a prova di errori e con un alto livello di soddisfazione per l'utente durante l'utilizzo sono i punti chiave analizzati sempre da [39], o meglio i pilastri su cui costruire delle soluzioni

ideali per la Cybersecurity per piccole e medie imprese. Specialmente per la prima categoria, molte volte si deve affrontare come problematica l'assenza di vero e proprio personale specializzato in sicurezza informatica, lasciando quindi i dipendenti in prima linea a combattere nemici di cui non conoscono praticamente niente. Da qui la necessità di piazzare sia la Cybersecurity, sia l'utente, al centro delle strategie di difesa; dopotutto solo dei generali senza coscienza manderebbero in battaglia persone impreparate e senza equipaggiamento, con possibilità di vittoria praticamente inesistenti.

3.10 Usabilità vs Sicurezza: uno scambio non sempre accettabile

Si è visto come all'interno della Human Computer Interaction l'usabilità dei prodotti sia una dei bisogni primari da trattare. Allo stesso modo, pensando alla Cybersecurity, essa non è affatto un elemento positivo: nella maggior parte dei casi in cui si è posta una certa attenzione sull'aumentare il livello di usabilità del sistema, nello stesso momento ne ha risentito anche la sicurezza, essendo essi due valori inversamente proporzionali. O almeno così si è sempre pensato. Non mancano anche i commenti ironici sulla questione, come ad esempio quello che, come suggerimento per rendere il computer più sicuro, consiglia di rimetterlo nella scatola e sotterrarlo, ma in essi si cela sempre un fondo di verità dopotutto. La più grande difficoltà delle aziende, approcciandosi alla sicurezza, risiede nella perdita di performance da tenere in conto, sebbene esso sia un approccio sbagliato alla questione. Il concetto di sicurezza come passaggio intermedio torna spesso in voga, non riuscendo a scostarsi di dosso questa etichetta che gli è stata affibbiata da tempo ormai. Ma forse ci stiamo ponendo la domanda sbagliata: invece di chiedere "cosa scegliere tra l'usabilità e la sicurezza" non prendiamo entrambi senza porci il problema [40]? Dopotutto ci sono già adesso degli esempi di sistemi facili da usare e allo stesso tempo sicuri: un esempio sono i nuovi sistemi per le ordinazioni online utilizzati da piccoli ristoranti durante il periodo pandemico per adattarsi alle restrizioni. Come citato in [41], in questi casi non serve effettuare il login con un account, ma viene associato l'ordine con un'e-mail o un numero di telefono e i cookies del browser, proteggendo le transazioni grazie all'HTTPS. Nessuna password o numero di carta di credito viene memorizzato, lo scambio di informazioni è sicuro e non presenta di certo problemi di usabilità. Coordinando quindi gli esperti di sicurezza e di User Interface/User Experience, si può arrivare quindi ad evitare questo "tradeoff". Questo concetto è stato riportato anche all'interno di [42], dove i concetti di usabilità e sicurezza sono stati sviscerati per poterli capire meglio. Il risultato, anche in questo caso, ha decretato che nessuno dei due è superiore all'altro per importanza, a dimostrazione del fatto che gli studi di HCI si stiano muovendo effettivamente molto di più verso la HCISec. In questo modo si possono mantenere alte le prestazioni del sistema, aggiungendo anche il fattore di sicurezza, ormai fondamentale. All'interno di [40] invece, si può trovare un'interessante riflessione: l'usabilità è così centrale nella costruzione della sicurezza che funziona anche nel mondo reale e nessuna organizzazione può più permettersi di ignorare. L'unica sicurezza buona è quella che applica l'usabilità ad essa. Le persone quando scelgono la sicurezza senza alcuna istigazione a farlo? Quando essa appare come la soluzione veloce e che arriva dritta al punto per poter completare le operazioni che devono eseguire. Se però la via più sicura non ha un buon livello di usabilità, gli utenti cercheranno una soluzione diversa, magari anche creata sul momento da loro ed è in questi casi che portano ad essere l'anello debole. Non è di certo ciò che cerchiamo, bensì vogliamo che diventino una sorta di "eroi" di tutti i giorni. Supportando il loro lavoro con alcuni elementi della Gamification (ricompense, badges), pensando alla sicurezza come un'impostazione di default e rivedendo alcuni dettagli sull'applicazione delle misure di sicurezza si può effettivamente arrivare ad avere come risultato la presenza sia dell'usabilità che della sicurezza, da sempre vista come un orizzonte inarrivabile.

3.11 Lo stress come possibile fonte di prestazioni

Una cosa che è capitata a tutti sicuramente è trovarsi di fronte ad una schermata di errore, cosa abbastanza comune invece nella vita di tutti i giorni di un programmatore. Quando la si vede,

sono due i pensieri che passano per la testa: rabbia in primis poiché le cose non vanno come vorremmo e voglia di risolverlo il prima possibile per poter sistemare il problema e tornare a quello che si stava facendo in precedenza. Ciò che avviene durante il secondo pensiero è dettato principalmente dallo stress, il quale ci guida durante tutto il procedimento di risoluzione di quella schermata d'errore tanto fastidiosa. Da qui però possiamo trarre uno spunto interessante: lo stress è un'altra di quelle "emozioni" che ci permette di performare meglio, spingendoci a capire il motivo di quella schermata d'errore e a sistemarlo. Ad esempio, all'interno dello studio di J. Grant e C. Boonthum-Denecke [43] è possibile notare come una delle implementazioni della HCI nel mondo della Cybersecurity avvenga proprio stimolando nel modo giusto il livello di stress degli utenti: esiste una curva che descrive il rapporto tra esso e il livello di performance raggiunto, la quale raggiunge il punto più alto con un livello di stress nella media. Ovviamente un eccessivo stress porta la persona ad andare più spesso nel pallone, deconcentrandolo e portandolo a rinunciare al suo obiettivo, mentre uno troppo basso non aiuta molto nel migliorare le prestazioni. Per quanto riguarda i metodi per stimolare il livello di stress, possono essere ad esempio l'utilizzo di un colore rosso più luminoso per i messaggi di errore, oppure di simboli di pericolo o simili agli stop stradali, per arrivare anche all'uso di punti esclamativi. Bisogna quindi fare una particolare attenzione anche a come segnalare gli errori all'utente, tenendo il livello di stress entro certi limiti per evitare reazioni negative e avere dei buoni riscontri sulle reazioni che porta alla loro vista. Le scelte di design sono ancora una volta messe in primo piano per la riuscita di un'applicazione o di un sistema. In pratica, quindi, può essere una buona idea andare a mettere sotto stress l'utente, ovviamente senza esagerare e controllando che su un tale soggetto non sia troppo controproducente, per poter avere una reazione positiva al problema, ricordandosi però che lo scopo di ciò è quello di rendere l'utente sempre vigile.

3.12 Gli insegnamenti della Human Computer Interaction

Gli studi di Human Computer Interaction mostrano come, ponendo al centro dello sviluppo l'utente finale, si possano effettivamente raggiungere gli obiettivi preposti per il sistema da creare. È un processo, quello che si va a iniziare, lungo e non privo di problemi e di molteplici interazioni: basti pensare alla fase di testing del prototipo, la quale può portare via molto più tempo di quello previsto. Il numero di errori possibili nell'utilizzo dell'applicativo o dei problemi di usabilità è però molto basso alla fine del lavoro, portando quindi ad avere un buon sistema che soddisfi l'utente nelle funzionalità che propone. L'applicazione poi degli elementi ludici porta il sistema a possedere anche un fattore di divertimento che in altri può mancare, arrivando a definire un'esperienza ancora più completa. Per l'utilizzo nel campo della Cybersecurity, avere un sistema in grado di insegnare i suoi elementi fondamentali, riuscendo anche a divertire l'utente senza farlo cadere in banali errori nell'utilizzo e con un alto grado di usabilità, risulta essere una potente arma per portare avanti la consapevolezza nelle persone di quanto siano importanti nella catena di difesa informatica.

Capitolo 4

La Prototipazione

In questo capitolo verrà introdotto il processo di Human Computer Interaction che verrà messo in pratica al fine di ottenere un prototipo per il sistema testabile: verranno seguiti i passaggi descritti anche nel capitolo precedente per poter arrivare ad assecondare i bisogni principali delle "personas" prese in considerazione all'interno di questo studio. Si inizierà quindi con la fase di "Needfinding" per capire le necessità e i bisogni dei possibili utenti del sistema che si andrà a creare, passando successivamente alla ricerca dei task da coprire (basandosi sempre sui risultati delle interviste fatte) ed infine si passerà ad un'ampia fase di testing, utilizzando un prototipo e avendo di conseguenza delle valutazioni euristiche su di esso, improntate a migliorare lì dove sarà necessario.

4.1 La scelta delle personas

Il primo passaggio da cui iniziare lo studio di HCI è quello della ricerca del bacino di utenza che si andrà a soddisfare con il sistema che si sviluppa. In una prima fase si pensava ad uno molto ampio, che comprendesse così esperti del settore, lavoratori e privati cittadini, in modo da poter sensibilizzare sull'importanza della Cybersecurity. Durante questa fase è stato fondamentale l'aiuto di Chiara, la quale ha messo a disposizione il suo lavoro precedentemente condotto sull'applicazione della Gamification per la diffusione dei principi della Cybersecurity [56]. Al suo interno erano stati presi in considerazione come possibili utenti sia esperti di Cybersecurity, sia lavoratori che però non avevano mai avuto a che fare con queste tematiche. Tenendo in considerazione che il suo lavoro [56] si è concentrato su un bacino di utenza molto vasto e che i possibili sistemi che si sarebbero andati a sviluppare erano già stati in qualche modo esplorati ampiamente nel corso degli anni, andando quindi a non evolvere la situazione di molto, si è optato per restringere il campo: partendo da una platea meno numerosa rispetto all'idea di partenza, si potrebbero avere un numero di risposte ovviamente più basso, ma ci si concentra sulle categorie di utenti più a stretto contatto con i pericoli dell'informatica, come fosse la prima linea di una guarnigione. Viene quindi introdotto uno strumento molto potente, il quale permette di identificare i possibili utenti dell'applicativo che si vuole sviluppare prima ancora di poterle incontrare dal vivo: le "personas". Questo concetto fu introdotto per la prima volta negli studi di HCI da A. Cooper [45] e fu illustrato come la descrizione precisa delle caratteristiche di un possibile utente e ciò a cui vuole adempiere. Il suo utilizzo non è obbligatorio ma fortemente consigliato poiché riesce ad aiutare molto i designers, potendosi focalizzare il più possibile sui diversi pattern di comportamento degli utenti rispetto al prodotto che si vuole creare. Grazie agli studi di Y. Chang, Y. Lim e E. Stolterman [44], si è potuto osservare come effettivamente l'utilizzo delle personas sia molto d'aiuto negli studi di Human Computer Interaction. L'esperimento che hanno proposto è molto semplice: hanno creato due team con lo scopo di risolvere un problema di design, ma uno dei due team ha utilizzato il concetto di personas, mentre all'altro è stato vietato. Alla fine del lavoro di entrambi i team, l'utilizzo di questo potente strumento è risultato molto impattante: infatti, il team a cui era stato vietato l'utilizzo è arrivato ad una conclusione meno specifica rispetto all'altro e individuando una possibile soluzione proprio nell'inclusione delle personas. Per questo

motivo è stata ponderata la scelta di creare ben tre diverse categorie di personas per questo caso specifico, le quali riescono a comprendere tutte quelle persone che combattono in prima linea per la sicurezza informatica:

Esperti di Cybersecurity: perché includere anche gli esperti in materia, sebbene siano senza alcun dubbio le persone più preparate ai pericoli informatici? È molto semplice: la ricerca che si è fatta era indirizzata a risolvere i bisogni delle personas che si prendevano in considerazione, chi meglio di loro poteva indirizzare la ricerca verso le problematiche più ricorrenti e longeve della sicurezza informatica? Il loro aiuto sarà dunque fondamentale;

Lavoratori non esperti di Cybersecurity: probabilmente la categoria più soggetta agli attacchi informatici e target principale dei cyber criminali. Le persone appartenenti a questa categoria sono molto utili alla ricerca poiché possono fornire dati interessanti sulla loro possibile formazione, seppure minima, nella Cybersecurity, cercando di capire anche quali potrebbero essere stati i problemi più ricorrenti;

Studenti universitari dell'orientamento Cybersecurity: con questa categoria si vanno ad includere i ragazzi che aspirano a diventare un giorno esperti in materia. La scelta di includerli è dovuta al voler cercare di inquadrare fin da subito quali sono i problemi che incontrano e che ritengono complessi da superare nei metodi di insegnamento della Cybersecurity. Poiché la Gamification viene applicata proprio per rendere più divertente e leggero l'apprendimento, si possono analizzare quali sono le problematiche maggiori nell'insegnamento per cercare di rimuoverle grazie ad essa.

Ognuna di queste categorie è fondamentale per un preciso motivo: per cercare di rendere il prodotto finale con un alto livello di usabilità, tenendo fissi però l'utente e i suoi bisogni al centro di ogni cosa.

4.2 Il questionario su Cybersecurity e Gamification

Una volta inquadrato il target, si passa al vero e proprio Needfinding. Si è quindi optato per effettuare la ricerca attraverso un questionario creato su Microsoft Forms principalmente per la facilità con cui è possibile diffondere il link (Appendice A); tuttavia, anche il classico approccio diretto, ovvero parlando faccia a faccia con l'utente, non è stato scartato. La ricerca è iniziata ufficialmente il 20 dicembre 2022 con l'obiettivo di raccogliere più dati possibili nell'arco di un mese a partire da questa data: il focus principale delle domande create si è concentrato prevalentemente su tre elementi:

- Le conoscenze della Cybersecurity ed eventuali esperienze con essa;
- L'importanza delle emozioni nel proprio lavoro o corso di studi seguito;
- Le preferenze verso gli elementi ludici che fanno parte della Gamification.

Anche in questo caso l'esperienza di Chiara è stata molto utile per evitare alcune problematiche. Inizialmente si era pensato di porre alcune domande personali all'utente tra cui il nome, ma è stata bocciata come idea quasi subito per evitare eventuali problemi di privacy che potevano essere sollevati dalle aziende; perciò è stata applicata una prima scrematura a questa categoria di quesiti, lasciando solamente due domande personali, ovvero il range d'età e l'eventuale occupazione, riuscendo nello stesso tempo a mantenere l'anonimato e a comprendere a quale categoria di personas facesse riferimento quella risposta. Sebbene siano state prese queste precauzioni, a volte sono risultate inutili e alcune aziende hanno deciso di non prendere comunque parte al questionario. Per rispettare i principi di HCI, è stato esplicitato come le domande non avessero una risposta giusta o sbagliata, cercando di trasmettere tranquillità all'intervistato: ogni risposta è stata importante in un modo o nell'altro. Sono state inserite anche alcune domande che andavano a verificare se l'utente si mantenesse coerente nelle risposte o meno, ad esempio le domande relative a cosa fare per controllare se il sito in cui si naviga sia sicuro e quella in cui si domanda se si controlla da dove

si sta scaricando un file. Le domande sulla Cybersecurity riguardavano principalmente quanto venisse ritenuta importante (su una scala da 1 a 5), sulla descrizione di eventuali attacchi subiti e soprattutto quale problema relativo alla sicurezza informatica far sparire. Quelle attribuite alle emozioni invece, si basavano sul cercare di capire se riuscissero sempre ad influenzare come approcciarsi alle situazioni relative al mondo del lavoro o dello studio. Infine, la parte relativa alla Gamification serve per individuare quali elementi ludici inserire nel sistema da progettare, così, per non sbagliare, si è lasciato scegliere agli utenti quali eventualmente inserire e quali evitare preferibilmente. Di questa categoria, la domanda più importante è di sicuro quella relativa alla scelta tra cooperazione e competizione, due elementi totalmente agli antipodi ma che, se sfruttati bene, sono strumenti molto potenti. Nelle domande che erano state pensate a risposta multipla, all'inizio era stata esclusa la risposta "Altro" per evitare di ricevere delle risposte fuori contesto. In un secondo momento, invece, dopo aver analizzato il questionario preparato da Chiara per il suo lavoro [56] e aver discusso dell'argomento con lei, si è arrivati alla conclusione che potesse risultare utile avere delle risposte diverse da quelle preparate, in modo da raccogliere ulteriori dati che possano ampliare gli orizzonti imposti inizialmente.

4.3 Analisi risultati questionario

Il questionario preparato per raccogliere dati sulla conoscenza di base della Cybersecurity e sugli elementi ludici preferiti ha raggiunto un totale di 59 persone, un buon numero considerando il bacino di utenza ristretto che ci si era imposto all'inizio, riuscendo ad ottenere risposte significative da tutte e tre le categorie di personas che erano state prefissate all'inizio. Per cercare di ottenere il maggior numero di risposte possibili, è stata creata anche una versione inglese per includere anche studenti o lavoratori stranieri. Nel primo sondaggio sono presenti anche delle risposte in inglese, motivo in più che ha portato a questa decisione, sebbene abbia raccolto solo due responsi.

Figura 4.1: Il range d'età dei partecipanti al questionario "Cybersecurity e Gamification".

La prima cosa da analizzare è il range d'età delle persone che hanno risposto al questionario: come si può vedere dal grafico in Fig. 4.1, la maggior parte di esse viene da un'utenza molto giovane che fanno, o faranno parte nel futuro prossimo, della prima linea di difesa contro gli attaccanti. Poter contare su una buona base di conoscenza e di consapevolezza della sicurezza informatica fa sicuramente ben sperare per il futuro della Cybersecurity. Sono state raccolte 27 risposte da parte di studenti universitari dell'orientamento di Cybersecurity, 14 da parte di lavoratori non esperti di sicurezza informatica e infine 18 da parte degli esperti. La media del livello di ansia raccolta è di 2.82: tutto sommato le persone che hanno risposto ne percepiscono una giusta dose; per quanto riguarda l'importanza data alla Cybersecurity fortunatamente nessuno ha risposto sotto il 4 (su una scala da 1 a 5).

Un argomento importante all'interno del questionario sono sicuramente le emozioni (Fig. 4.2), in quanto si è già parlato in precedenza anche dell'importanza del design emotivo (§ 3.7). In questo caso il focus è su quelle che si provano quando ci si approccia ad un argomento nuovo relativo alla Cybersecurity. Come si può notare, la maggior parte delle persone intervistate prova piacere a studiarli, forse perché si tratta comunque di individui quasi tutti all'interno del settore, ma pesano molto di più quelle risposte distribuite tra noia, rabbia, tristezza ed angoscia. I responsi relativi alla categoria "Altro" variano da interesse e stupore a repulsione e disperazione. Da ciò

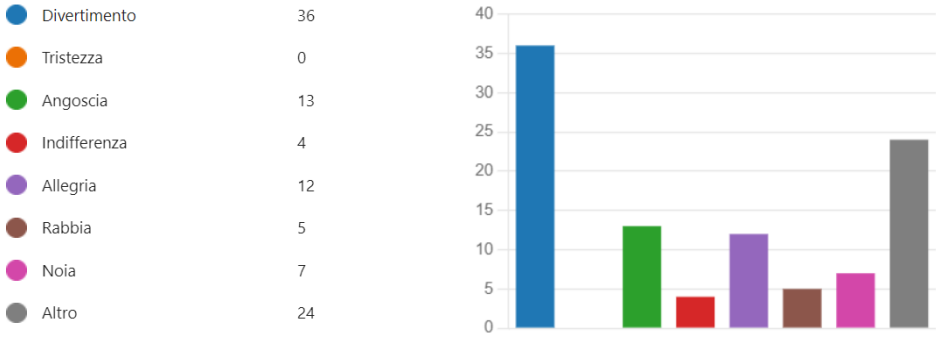


Figura 4.2: Le emozioni che i partecipanti al questionario "Cybersecurity e Gamification" provano quando si approcciano ad un nuovo argomento della Cybersecurity.

si potrebbe denotare che le persone sono spaventate dei nuovi pericoli che arrivano ogni giorno ma, allo stesso tempo, sono sempre alla ricerca della conoscenza necessaria per poter affrontarli.

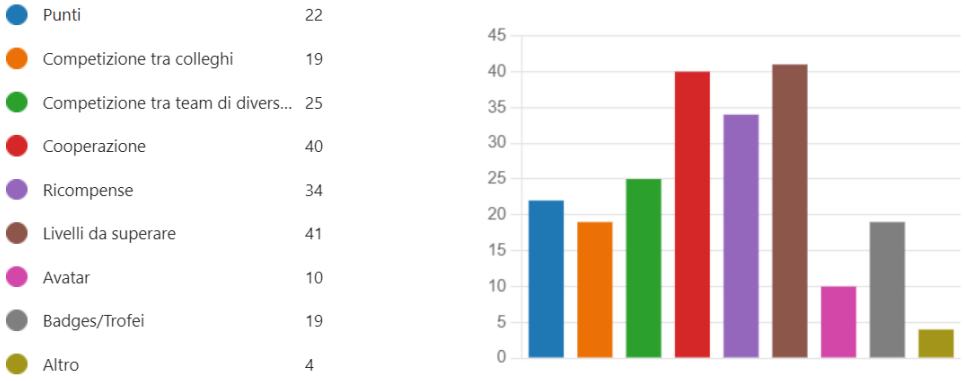


Figura 4.3: Gli elementi ludici scelti dai partecipanti al questionario "Cybersecurity e Gamification", spicca tra tutti la "Cooperazione".

Passando alle preferenze degli utenti verso gli elementi ludici, possiamo notare dalla Fig. 4.3 come i due grandi pilastri contrapposti tra loro, ovvero la competizione e la cooperazione, spiccano al di sopra degli altri, così come ci si aspettava: sebbene sembri che la prima sia al di sotto degli altri, bisogna tenere in considerazione che sono presenti due preferenze per il lato competitivo tra cui scegliere e, insieme, raggiungono un bel numero di adesioni. La cooperazione è di sicuro il metodo più scelto, anche questo risultato come da previsioni; insieme ad esso si trovano ricompense e livelli da superare. Da quel che si evince, l'utenza raggiunta è abbastanza affezionata al mondo dei videogiochi, ma d'altronde a chi non piace essere ricompensati dopo aver faticato per superare un ostacolo piuttosto ostico? Passando alle problematiche della Cybersecurity più sentite da parte dei partecipanti, ne sono uscite tre in particolare: Phishing, social engineering e debolezza delle password. Su quest'ultima, alcuni esperti erano addirittura esasperati dal loro utilizzo e sperano di non doverne più usufruire in futuro. Queste sono le stesse problematiche analizzate nel primo capitolo relativamente agli attacchi più comuni, andando a confermare la loro reale minaccia nella vita di tutti i giorni. Un punto però importante che viene trapelato è la sensibilizzazione all'importanza della sicurezza, la quale porterebbe ad avere un numero decisamente inferiore di attacchi a buon fine e sarà anche presa in considerazione nella parte successiva. Alle domande su un possibile attacco phishing e navigazione su un sito non del tutto sicuro si sono mostrati tutti molto attenti e preparati sull'argomento, ma non bisogna abbassare mai la guardia e, infatti, una delle risposte riportava di porre attenzione ai siti in cui navigava solo nell'ambito lavorativo. Non è stata assolutamente considerata una risposta sbagliata per la domanda posta, ma è stata molto importante poiché fa capire che l'attenzione sull'argomento deve rimanere sempre alta, anche al di fuori dell'ambito lavorativo. La domanda su cui si è puntato molto per la ricerca delle difficoltà e

dei bisogni delle persone sulla Cybersecurity era quella che proponeva l'utilizzo di una bacchetta magica per risolvere uno solo dei problemi relativi alla sicurezza. Una particolare risposta ha colpito molto sia per il parallelismo proposto, che per l'idea alla base, un po' fuori dalle righe per così dire:

> "La domanda è divertente! Se facessimo un parallelismo con la medicina avremmo una visione più chiara della situazione. In particolare, basta equiparare i vari problemi della Cybersecurity (es. controllo degli accessi, confidenzialità e integrità delle informazioni, etc.) con i sintomi di una determinata malattia noteremmo che le soluzioni proposte (IAM, cifratura e firma digitale) servono unicamente a mitigare i sintomi. Se avessi la bacchetta magica andrei a rimuovere tutte quelle cause che rendono necessaria l'esistenza stessa della Cybersecurity".

Altra risposta interessante, invece, proviene dalla domanda relativa alla scelta tra la cooperazione e la competizione:

> "Preferisco la cooperazione, come branca è troppo vasta per sapere tutto da soli".

Quest'ultima risposta ha un grande valore, perché ancora una volta dimostra come l'argomento Cybersecurity sia effettivamente complicato da affrontare da soli: riprendendo un pò il paragone proposto dalla risposta precedente, non esiste nemmeno in medicina un unico medico che sappia curare ogni male esistente. Non è semplice riassumere in poco tutto ciò che si è riusciti a raccogliere grazie a questa piccola ricerca, bisogna tuttavia partire però da quello che era il focus principale di tutto il questionario: quali sono i bisogni principali degli utenti riguardo alle problematiche relative alla Cybersecurity? Si potrebbe dire in generale la poca sensibilizzazione all'importanza dell'argomento e alcuni attacchi molto noiosi e persistenti come il phishing.

Le emozioni che sono state elencate nell'approccio a queste tematiche fanno ben sperare: curiosità, divertimento, ma anche angoscia e timore mostrano come, almeno per quanto riguarda le categorie di persone analizzate, l'importanza di questi argomenti porti ad avere l'asticella dell'attenzione sempre alta, senza tralasciare anche l'aspetto divertente dell'apprendimento di concetti nuovi. A questo punto si può iniziare a pensare al prossimo step, ovvero la preparazione di un prototipo che porti all'applicazione dei concetti necessari per soddisfare i bisogni degli utenti e cercare di sensibilizzare il più possibile sull'importanza della Cybersecurity.

4.4 La scelta del prototipo

Dopo la prima fase di raccolta del Needfinding e aver inquadrato gli aspetti su cui concentrarsi, si passa alla fase successiva, ovvero quella della scelta e dell'implementazione del prototipo. Quando si è messi di fronte ad un bivio non è mai semplice decidere se percorrere una strada piuttosto che un'altra, ma, in questo caso, ci si può affidare ai diversi pro e contro di ogni possibilità. Esse sono state già ampiamente analizzate all'interno del capitolo 2.16, ma alla fine la scelta è ricaduta sul prototipo di carta per diversi motivi: per prima cosa è il più semplice e veloce da creare; inoltre risulta essere facilmente modificabile e, in questo caso, è probabilmente la ragione fondamentale che ha portato alla scelta di questa tipologia, viste le previsioni che portavano a molte modifiche sulla prima versione del prototipo. Ultima cosa, ma non meno importante, sono i costi praticamente nulli che lo caratterizzano, portando avanti lo stesso messaggio che anche Cyber Stability Games con le sue carte porta avanti [16]: non sempre una spesa maggiore porta ad un risultato migliore. Anche nell'eventualità di fare un buco nell'acqua, con l'idea portata avanti inizialmente, i danni risultano contenuti.

4.4.1 Le tematiche del prototipo e gli elementi di Gamification

Una volta terminata la problematica della scelta del prototipo, si passa alle tematiche da affrontare durante il testing. A fronte dei risultati del questionario, si è optato per due argomenti da proporre:

la sensibilizzazione verso le tematiche della Cybersecurity e alcune simulazioni di attacchi, le cui tipologie sono state scelte sempre dalle problematiche evidenziate dal questionario. Il nome pensato per l'applicativo è "Payload Please", che ricorda molto il nome di un noto videogioco in cui si interpretava un ispettore che lavorava alla frontiera e si dovevano analizzare bene i documenti di ogni singolo cittadino prima di poterlo far entrare nel paese. In un certo senso si è quindi cercato di portare lo stesso spirito di questo gioco nell'interpretazione del prototipo sulla sicurezza informatica, quindi, così come nel videogioco si doveva prendere la decisione di lasciar passare o meno la persona, così bisogna porre una certa attenzione per capire bene se quello che viene presentato è un tentativo di attacco o di sensibilizzazione.

Si va dunque ad elencare quali sono i tentativi di attacco che sono stati teorizzati per i test della prima versione del prototipo:

- Mail falsa di Amazon che chiede la conferma di alcuni dati personali tramite un link fornito nel corpo del messaggio per consentire nuovamente l'accesso al proprio account, con rischio di blocco del profilo in caso contrario (Fig. 4.4);
- Mail falsa di Google Rewards che, in cambio di alcune risposte personali, promette una ricompensa monetaria molto più alta del normale. In questo modo si va a simulare una possibile raccolta dati per la creazione di un dizionario per effettuare un attacco di brute force sulle proprie password;
- Mail falsa da parte di "Lidl" che annuncia alla vittima di essere vincitore di un premio, ma allo stesso tempo proponendo di poter annullare l'iscrizione al programma a premi cliccando su un link proposto nel corpo del messaggio. In entrambi i casi, però. l'utente viene trasportato su un sito falso;
- Mail falsa di convocazione della Polizia, molto simile a quella presentata nel primo capitolo;
- Mail falsa da parte di PayPal che informa l'utente che una sua transazione non è andata a buon fine ed è richiesto l'accesso al suo profilo tramite il link proposto nel corpo del messaggio.

Per quanto riguarda la parte relativa alla sensibilizzazione si è pensato, invece, ai seguenti casi:

- Richiesta di passaggio dalla vecchia password all'autenticazione biometrica in aggiunta all'uso di OTP (One Time Password) da parte dell'azienda in cui si lavora. In questo caso viene specificato che non è una cosa obbligatoria per analizzare i diversi approcci a questa raccomandazione;
- Mail da parte di un superiore che richiede dei documenti importanti ma non tramite canali ufficiali aziendali ma direttamente nella sua casella di posta personale;
- Richiesta da parte del portale del Politecnico di Torino di aggiornare la propria password dell'account, cercando di spronare l'utente ad inserirne una molto più sicura dando anche delle linee guida.

Una volta selezionati sia gli attacchi che i tentativi di sensibilizzazione, non resta che implementarli anche in base agli elementi ludici scelti sempre dagli intervistati nel questionario (Fig. 4.3). Per descrivere più semplicemente l'utilizzo del prototipo è stato preparato anche un piccolo sketch che illustra il possibile funzionamento, come si può notare in Fig. 4.5. Quello descritto nell'immagine è uno dei casi d'uso pensato per poter testare il sistema: durante una classica mattinata in ufficio arriva una mail un pò strana e l'utente confuso chiede aiuto ad un suo collega per un consiglio, da questo possiamo notare subito la possibile cooperazione nella simulazione di attacco. Successivamente anche il capo conferma che quello che ha affrontato non era altro che una prova per tutti quanti i dipendenti, mostrando alla fine una classifica che illustra le scelte positive e negative di ognuno, mettendo solo alla fine i punti guadagnati in questo "turno". Così facendo, si vuole porre in secondo piano la questione più ludica e si cerca di mettere in mostra la sensibilizzazione alla sicurezza informatica e specialmente alle cose negative che sono successe. Ovviamente tutto

questo non è per evidenziare gli errori, ma per poter migliorare sempre. L'ultima scena illustra una possibile competizione relativa al secondo utilizzo dell'applicativo, magari mettendo in palio qualche ricompensa per spronare a partecipare. La cosa importante è non renderla tossica, deve essere sana e portare le persone a dare il massimo per poter migliorare se stessi.

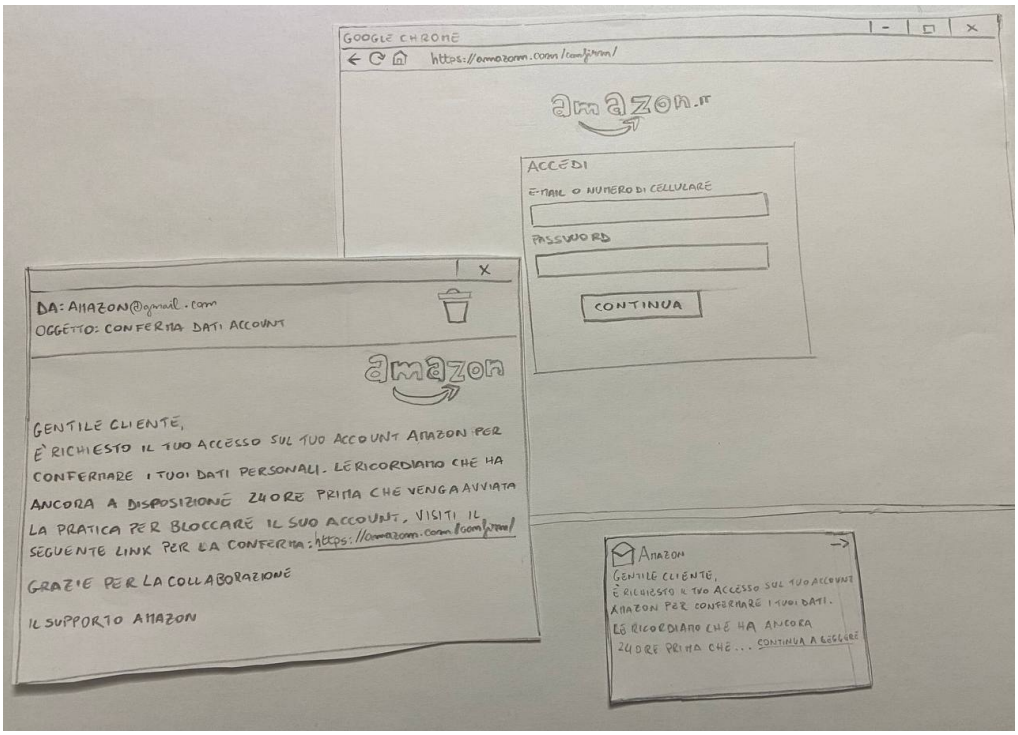


Figura 4.4: La simulazione della mail falsa di Amazon presente nella prima versione del prototipo di "Payload Please".

4.5 La fase di testing e i metodi di valutazione

Una volta delineati quelli che saranno i possibili ostacoli a cui verranno sottoposti i partecipanti alla fase di testing del prototipo, bisogna specificare in che modo poter valutare l'efficacia del sistema e soprattutto il livello di usabilità dello stesso. Su quest'ultimo aspetto si andrà ad utilizzare il questionario "SUS", ovvero il "System Usability Scale", il quale verrà proposto alla fine dell'intera sessione all'utente che ha provato la prima versione del sistema (Appendice B). Esso fu ideato da J. Brooke [50] ed è uno dei questionari post test validi per poter analizzare il livello di usabilità del sistema o dell'applicazione che si vuole sviluppare. Altra scelta possibile era il "NASA-TLX" (Task Load indeX), nato anch'esso negli anni 80' come il SUS grazie agli sforzi fatti dalla NASA per misurare il carico di lavoro percepito e che veniva richiesto ai membri delle squadre spaziali a cui venivano affidate delle tasks molto tecniche [28]. Il primo motivo che ha portato all'esclusione di tale questionario è dato dal suo obiettivo: studiare prodotti molto complessi in ambienti ad alti rischi (medicina, militare, aerospaziale...). Il secondo è dato dai pro che porta il SUS rispetto al NASA-TLX [51]: è molto semplice da somministrare ai partecipanti, risulta essere molto scalabile, può essere utilizzato anche con dei campioni piccoli con risultati affidabili e riesce a differenziare efficacemente un sistema con un alto livello di usabilità da uno basso. Per quanto riguarda il suo funzionamento, risulta essere anch'esso semplice: vengono elencate 10 domande all'utente subito dopo aver finito il test e a cui si può rispondere con un valore che va da 1 a 5, il quale esprime quanto sia d'accordo o meno con il relativo quesito proposto. Una volta raccolte tutte le risposte si andrà a calcolare il valore nel seguente modo: per le domande con numero dispari si prende il punteggio assegnato dall'utente e si andrà a sottrarre 1, mentre per le domande con numero pari il valore assegnato dall'utente verrà sottratto da 5. Una volta fatto ciò, si andranno a sommare tutti i singoli valori da ogni domanda e si moltiplicherà il totale per 2.5.

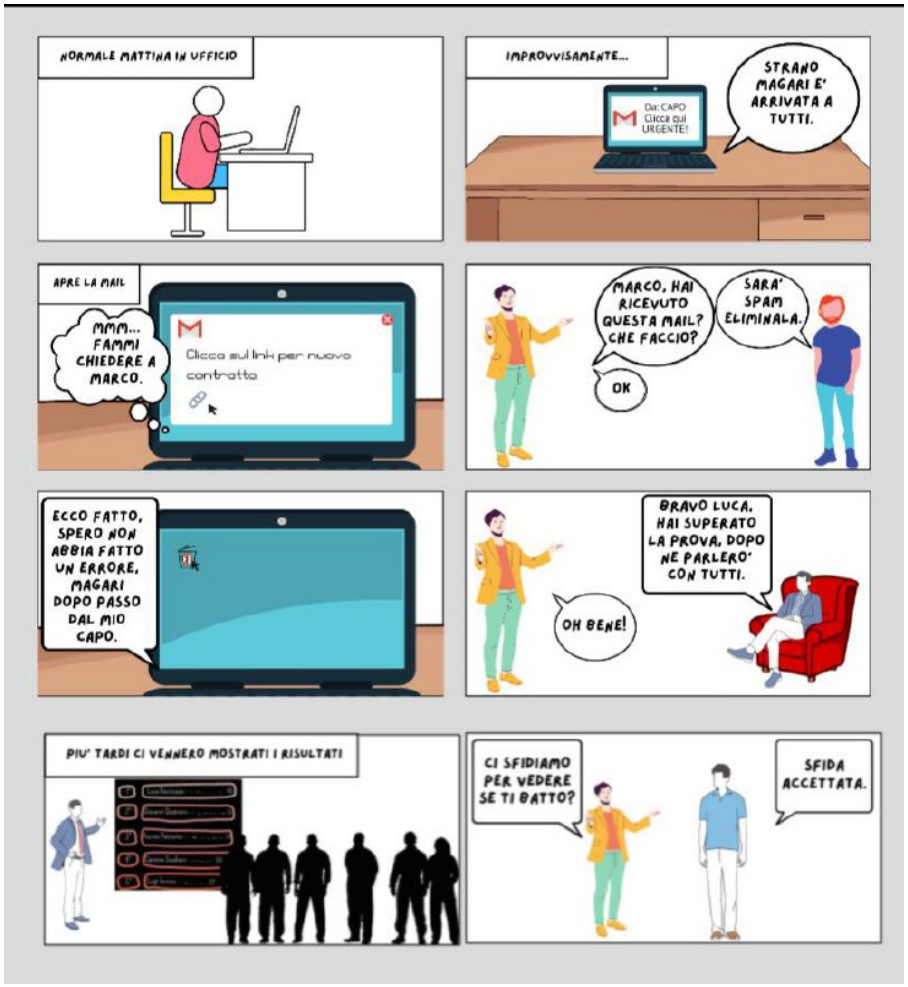


Figura 4.5: Lo sketch di presentazione per il prototipo di “Payload Please”.

Il valore finale oscilla nell'intervallo 0-100, nel caso in cui risulti essere maggiore di 68, il sistema si può considerare con un livello di usabilità al di sopra della media.

Passando al test vero e proprio, è stato pensato di somministrare ad ogni singolo utente sia attacchi che tentativi di sensibilizzazione per un totale di tre test a simulazione, con un livello di difficoltà crescente in alcuni casi per cercare di far abbassare la guardia e colpire quando meno se lo aspettano. Può essere considerata effettivamente una mossa meschina, ma dopotutto agli attaccanti non puoi chiedere certamente di avvertire quando vogliono prendere i tuoi dati. Si cercherà anche di trasmettere il messaggio di mantenere l'asticella dell'attenzione sempre alta per evitare spiacevoli inconvenienti. Andando avanti con i test verrà stilata anche la “classifica” con tutte le persone che ne hanno preso parte e i relativi bonus e malus che hanno guadagnato con le loro azioni: così facendo verrà poi anche messo in gioco la variabile “competizione”. Ovviamente qualunque altro tipo di commento o critica sul test e sul prototipo viene presa in considerazione, anche al di fuori delle domande del SUS, in modo tale da mantenere un contatto stretto con l'utenza. Le possibili simulazioni pensate sono le seguenti:

- Per i lavoratori e gli esperti due attacchi tra le finte mail di Amazon e PayPal, la richiesta di documenti da parte di un superiore in maniera insolita e per quella relativa alla sensibilizzazione invece, la richiesta di passaggio all'autenticazione a due fattori con parametri biometrici;
- Per gli studenti invece, la finta mail di Google Rewards e la falsa convocazione della polizia o una delle due mail false di Amazon e PayPal, finendo con la parte di sensibilizzazione relativa al cambiamento della propria password per l'accesso al profilo universitario.

Prima di iniziare verrà contestualizzata la situazione in cui si trova ogni partecipante, ad esempio nel caso di un lavoratore si introduce con un possibile "sei in una qualunque mattina in ufficio e stai lavorando ad un importante progetto, quando all'improvviso..."; stessa cosa ma con soggetti diversi si può proporre per gli studenti. Durante i test, essendo che il prototipo non è automatizzato e richiede la presenza umana, sarò io stesso a simulare ogni comportamento possibile del sistema, tirando i fili da dietro le quinte come un burattinaio e, in quanto "macchina", non potrò essere d'aiuto per i partecipanti se non per la parte introduttiva e l'incipit per i tentativi di attacco o sensibilizzazione: lo scopo è quello di rendere la simulazione la più veritiera possibile, in modo da poter analizzare come nel quotidiano le persone affrontano i problemi, spronando anche l'utente a descrivere a parole quelli che sono i suoi pensieri e le azioni che vuole mettere in pratica (Fig. 4.6). Viene posta una particolare attenzione sul metodo di valutazione dei partecipanti durante i singoli test: ogni casistica proposta avrà un punteggio massimo ottenibile, il quale sarà condizionato dalle singole azioni degli utenti e dai bonus e malus che si andranno ad ottenere. Per cercare di automatizzare questo sistema è stato pensato ad un algoritmo di valutazione da seguire con riserva, il quale prevede la perdita o il guadagno di punti a seconda del tipo di scelta presa dall'utente, dividendo in quattro le possibili opzioni: errori molto gravi e meno gravi e scelte buone e ottime. I punti persi o guadagnati saranno bilanciati in proporzione del massimo ottenibile per singola casistica: solitamente per gli errori gravi e le scelte ottime si ottengono rispettivamente un malus ed un bonus del 40% del totale, mentre per le altre due possibili azioni è il 20%. Ad esempio, nel caso dell'attacco di Phishing l'accedere al sito comporta un penalità meno grave, mentre inserire i dati all'interno del form presente ne comporterà una peggiore; stesso metodo si applica per le azioni duali, dove nel caso in cui l'utente legga semplicemente la mail senza fare altro otterrà un bonus minore, invece se provvederà a segnalare la mail come spam e a cancellarla otterrà un punteggio maggiore. Ovviamente il puro e semplice algoritmo appena descritto non sarà sempre valido a prescindere, ci saranno dei casi "borderline" dove l'intervento umano decreterà quanti punti assegnare o togliere in quel particolare caso. Ad esempio, nel caso in cui un utente apra il link per il sito di Phishing e mentre sta scrivendo i primi caratteri del suo username chiede un aiuto ad un suo collega, l'errore da potenzialmente grave subirà una riduzione della penalità poiché ha riconosciuto che stesse sbagliando in quel momento e ha voluto confrontarsi prima di andare oltre.

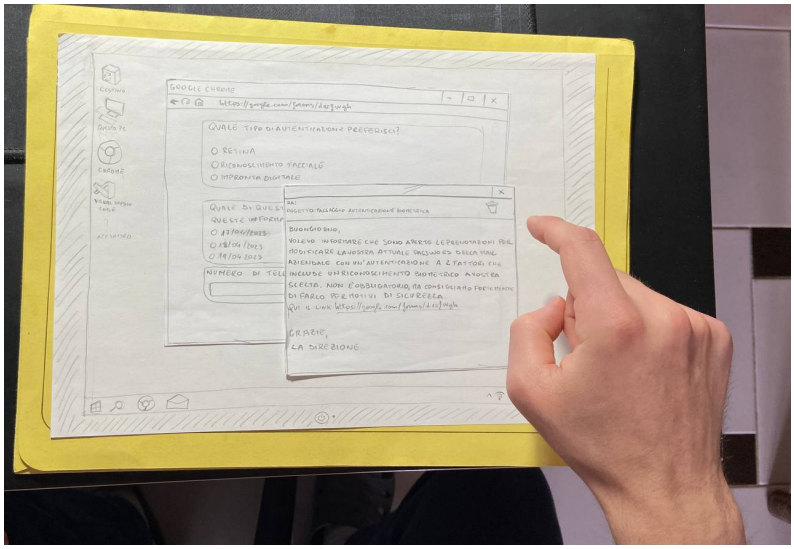


Figura 4.6: Una delle simulazioni proposte durante i test con il prototipo cartaceo di "Payload Please". L'utente simula il comportamento del dispositivo attraverso il "tocco" sui fogli.

4.6 I risultati dei test sul prototipo di carta

La parte relativa ai test ha riportato utili osservazioni da parte dei diversi partecipanti, grazie alle quali è possibile rendere migliore questa prima versione. Colgo nuovamente l'occasione per

ringraziare tutti coloro che hanno messo a mia disposizione una parte del loro tempo per testare il sistema. Sono 12 i partecipanti che si sono resi disponibili per affrontare la simulazione, distribuiti tra le tre categorie di personas già discusse in precedenza. Al fine di verificare l'esito in generale di questa prima fase di testing, ci si è basati su due fattori principalmente: il primo è il risultato del questionario SUS, il cui punteggio finale, dopo aver eseguito tutti i calcoli come anticipato nel paragrafo precedente (§ 4.5), arriva ad un totale di 84.5, andando quindi ben oltre il valore di 68 imposto per i sistemi nella media come livello di usabilità. Il secondo è rappresentato dalle critiche costruttive ricevute dall'utenza, la quale, sebbene abbia avuto modo di testare il prodotto nella sua fase embrionale, lo ha comunque ritenuto valido dal suo punto di vista. Quest'ultimo aspetto sarà fondamentale anche durante le fasi successive di testing, andando a rimarcare la centralità dell'utente e delle sue necessità, così come previsto dal design di tipo User-Centered presentato dalla Human Computer Interaction. Andiamo quindi a vedere nello specifico quali sono stati i commenti più significativi che portano ad una riflessione sui possibili cambiamenti per migliorare lo stato del sistema. La prima osservazione che è stata posta risulta essere sulle modalità in cui venivano somministrati gli attacchi e le sensibilizzazioni:

> "Non si potrebbe fare un tentativo anche con strumenti diversi dalle mail? Ad esempio con messaggi o chiamate false, visto che di recente ne sto ricevendo molte".

Il successivo commento invece, si riferisce all'elemento dei punti, i quali sono messi in secondo piano e senza aver definito un vero e proprio massimo punteggio raggiungibile:

> "Essendo un appassionato di videogiochi, dopo aver letto e analizzato le varie azioni positive e negative che ho fatto durante la simulazione, ero curioso di sapere quanti punti mancassero per arrivare al punteggio massimo. Visto che sono anche una persona che tende a completare ogni cosa al 100%, sarei veramente curioso di riprovare per poter ottenere questa volta tutti i punti disponibili".

Sulla parte relativa invece ai casi proposti ci sono stati un paio di commenti interessanti, i quali hanno anche portato alla creazione di nuovi tentativi di attacchi e possibili casi di sensibilizzazione all'importanza dell'argomento:

> "L'idea è molto divertente, ma forse ci sono pochi casi veramente borderline che mi potrebbero portare a pensare veramente a cosa sto andando incontro".

Per quanto riguarda l'utilizzo degli elementi ludici all'interno del prototipo, verranno elencate tutte le osservazioni fatte dai partecipanti alla fine del questionario:

- Sulla "classifica" proposta con i bonus e i malus guadagnati durante il test e i punti che ne sono scaturiti, quasi tutti hanno notato per prima cosa i propri errori, cercando di capire se è una cosa che succede spesso oppure solo un caso isolato dovuto alla distrazione. I punti invece, sono rimasti in secondo piano per tutti, tranne per qualcuno il cui senso della competizione spicca al di sopra della media;
- Sulla possibile ripartecipazione alla simulazione, quasi tutti gli utenti si sono mostrati interessati a riprovare, sia per migliorarsi nelle loro lacune, sia per un eventuale ricompensa interessante;
- Sulla presenza della cooperazione, tutti hanno avuto modo di utilizzarla, magari per chiedere ad un collega di lavoro o di università, nessuno ha disprezzato l'aiuto di chi ha più conoscenza sull'argomento. Sulla competizione invece, sono stati rilevati un paio di casi di utenti molto competitivi, i quali hanno mostrato il proprio interesse nel riprovare il test solo per essere il migliore. In generale però, la competizione non è stata vista come una possibile tematica negativa e che porta ad avere elementi tossici nella vita lavorativa o universitaria.

Un ringraziamento particolare va anche al Professore Atzeni, il quale si è sottoposto a quello che si potrebbe definire una versione 2.0 del prototipo iniziale. Infatti, oltre ai casi citati in precedenza, sono stati aggiunti dei tentativi di attacco ad hoc per lui e altri casi più "borderline", come richiesto anche durante un paio di test dagli utenti. La simulazione nuova è stata di gradimento del professore, il quale ha dato un grosso contributo al miglioramento del sistema con una particolare attenzione da porre sulle emozioni provate dai partecipanti:

> "Oltre ad analizzare nelle successive simulazioni tematiche differenti dal phishing e dalla autenticazione biometrica presenti attualmente nei casi proposti, ci sarebbero alcuni elementi da tenere in considerazione, come i livelli di ansia e tensione presenti dopo il test. La competizione che potrebbe scaturire da una seconda applicazione può sicuramente avere degli elementi positivi, ma se applicata in scenari lavorativi alquanto stressati, potrebbe portare solo a vedere questa simulazione come un'ulteriore fonte di stress. Sarebbe appropriato controllare dopo la prima simulazione i livelli di tensione ed ansia raggiunti dai singoli e paragonarli con quelli dell'ambiente in cui sono collocati, ad esempio con un piccolo questionario per raccogliere queste informazioni dai diretti interessati: nel caso in cui si rivela essere un ambiente non adatto, si potrebbe anche decidere di non eseguire ulterirori simulazioni."

4.7 Cosa rimane di questa prima fase e i possibili cambiamenti al prototipo

La cosa che più mi ha colpito, durante tutta la fase di testing, è stato il gran numero di recensioni positive per l'idea alla base del progetto: sia studenti che lavoratori hanno affermato di essersi divertiti durante la simulazione e hanno notato che i "malus" guadagnati alla fine sono effettivamente delle loro lacune, portandoli ad ammettere i propri sbagli e a porli in condizione di eliminarli una volta per tutte. L'alto valore raggiunto nel SUS è sicuramente un buon punto da cui ripartire, tuttavia alcune cose necessitano dei piccoli ritocchi in modo da poter migliorare ancora il sistema: un primo cambiamento è rendere visibile il punteggio massimo raggiungibile accanto a quello invece accumulato dall'utente, affinché ognuno possa tenere traccia di quanto manchi effettivamente per arrivare alla perfezione, almeno per quanto riguarda le tematiche presentate nella singola simulazione; altra modifica riguarda la descrizione dei bonus e dei malus guadagnati, in quanto alcuni partecipanti avrebbero voluto sapere quali dei vari test a cui si sono sottoposti hanno portato a guadagnarli. Per venire incontro a questa esigenza verrà aggiunta, subito dopo la descrizione del rispettivo bonus e malus, il caso specifico che l'ha scaturito, riuscendo così anche ad evidenziare e a tenere traccia al meglio le proprie azioni durante la simulazione. Infine, il cambiamento forse più importante è quello di inserire un breve questionario alla fine della simulazione e dopo aver visionato i risultati nella classifica finale, in modo da poter tenere traccia dei livelli di ansia e tensione provati dai singoli utenti e che, nel caso in cui risultassero al di sotto di una certa soglia, porterebbe ad una possibile riproposizione di Payload Please nell'ambiente preso in considerazione (Appendice C).

4.8 Il passaggio al sistema informatico

Alla fine dei vari test su carta e dopo aver formalizzato i cambiamenti da apportare all'intero sistema, ci si pone il seguente quesito: come è possibile portare tutto ciò nel mondo informatico, anche solo parzialmente, per poter rendere il tutto applicabile nel quotidiano? Per prima cosa ci si sposta sul sistema operativo Kali Linux, creato ad hoc per queste tipologie di test. Dopo alcune ricerche [57], è stato possibile trovare una combinazione di alcuni programmi per mettere in piedi il sistema Payload Please. Per prima cosa, bisognava individuare un programma che fosse in grado di creare un sito web falso, ma che potesse allo stesso tempo trarre in inganno l'utente che lo visitava. Sono due i programmi che effettuano questo specifico topic: HiddenEye [52] e Nexphisher [53]. Entrambi sono degli strumenti utilizzati per il phishing, presentano inoltre la possibilità di salvare i dati dell'utente che vengono inseriti all'interno dei siti falsi, con focus principalmente

sull'indirizzo IP, username e password. Se si volesse trovare una differenza sostanziale tra i due, HiddenEye risulta essere il più personalizzabile: infatti, è possibile inserire all'interno del sito anche un "keylogger", in grado di rilevare ogni singolo tasto premuto dalla vittima quando il focus è sulla schermata del sito web falso.

Figura 4.7: La pagina principale che viene mostrata all'utente all'avvio di HiddenEye.

Figura 4.8: La pagina principale che viene mostrata all'utente all'avvio di NexPhisher.

Come è possibile anche notare dalle immagini 4.7 e 4.8, i possibili siti da emulare sono più o meno gli stessi e il prodotto finale mantiene anche la stessa verosimiglianza con il sito originale, a meno di tonalità di colore o impostazioni della pagina non più in uso. Come detto in precedenza, la differenza sta nella capacità di HiddenEye di aggiungere al sito un keylogger, grazie al quale

risulta possibile vedere sin da subito all'interno del prompt dei comandi l'input della vittima. All'interno delle Fig. 4.9 e 4.10, si riesce a constatare come le informazioni raccolte siano visualizzate istantaneamente sul computer dell'attaccante, lasciando anche la possibilità di accedervi in un secondo momento all'interno dei file appositi creati in automatico dall'applicazione. A differenza di Nexphisher, HiddenEye fa un passo avanti in più: infatti, come si nota anche dall'immagine 4.9, viene mostrato anche quale sia l'user agent della vittima (in questo caso Mozilla) e anche il sistema operativo dal quale sta al momento accedendo la vittima (Linux x86_64). Sono stati analizzati un buon numero di programmi per la creazione di siti falsi per effettuare tentativi di phishing, ma sono stati scartati per diversi motivi. La maggior parte di loro, come ad esempio Blackeye, Socialphish o Socialfish, sono stati depennati dalla lista dei candidati poiché supportavano come modalità di propagazione solamente il tunnel attraverso i server Ngrok, ma, a causa delle politiche di privacy, esso prende seri provvedimenti contro qualunque account faccia uso dei suoi servizi per effettuare il phishing, anche se solo a scopo didattico. Questo aspetto ha portato infatti non pochi problemi per la ricerca degli strumenti. Un altro programma scartato, ma per motivi differenti, era LockPhish, il quale era in grado di ottenere informazioni, come IP e il dispositivo da cui si stava accedendo al link, ma rimanendo sempre all'interno del localhost e senza avere altre informazioni come username e password che invece sono raccolti da HiddenEye e Nexphisher.

Figura 4.9: Le informazioni raccolte tramite l'utilizzo del sito creato da HiddenEye.

Le due applicazioni selezionate danno la possibilità all'attaccante di scegliere come veicolare il link malevolo, ad esempio tramite il localhost o un tunnel già indirizzato verso un server Ngrok (che però presenta i problemi sopra elencati); esistono anche altre opzioni, ma al momento sono tutte quante indisponibili a causa di problemi ai vari server. A questo punto possiamo dire di avere pronte le nostre cartucce per compiere la simulazione, manca ancora però "l'arma" vera e propria. Certo, è sempre possibile l'invio manuale dei link tramite una mail creata ad hoc, ma ci vorrebbe molto tempo e alcune informazioni andrebbero probabilmente a perdersi. Per questo scopo, ci si affida ad un altro programma: King Phisher [54] (Fig. 4.11). Esso è uno strumento creato proprio per testare la consapevolezza dell'utente andando a simulare attacchi di Phishing, ma, a differenza dei due programmi precedenti, King Phisher mette a disposizione un'architettura molto flessibile che permette di avere il controllo totale sulle mail che vengono inviate. Grazie ad esso è possibile creare la mail ad hoc come quelle viste nel prototipo di carta proposto nella fase precedente, il tutto reso possibile dal file HTML che viene richiesto come input. All'interno di esso si definisce il corpo della mail (Fig. 4.12) ed è facilmente modificabile tramite l'editor messo a disposizione dallo stesso King Phisher. Sebbene il suo utilizzo sia indirizzato solo alle campagne di phishing, grazie alla possibilità di modificare tutto dal codice HTML, è possibile inserire un qualunque tipo di link al suo interno, ad esempio quello creato da HiddenEye se si volesse simulare

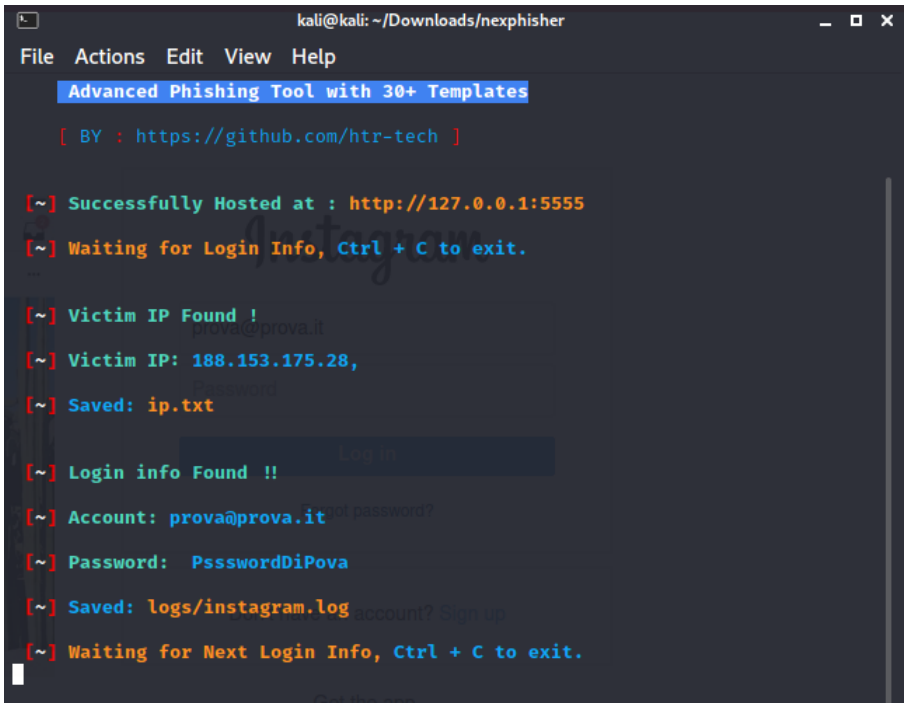


Figura 4.10: Le informazioni raccolte tramite l'utilizzo del sito creato da NexPhisher.

un attacco oppure un normale link di Google forms per la raccolta di partecipazioni al passaggio all'autenticazione biometrica se si volesse invece testare il livello di consapevolezza degli utenti. La prima cosa che viene richiesta all'avvio di King Phisher è la creazione della propria campagna di phishing, con la possibilità di analizzare alcuni suoi elementi come il numero di visite totali dei messaggi inviati, le credenziali che sono state ottenute da coloro che sono caduti nella trappola e altre informazioni interessanti. Sfruttando la possibilità di King Phisher di inserire un file HTML come mail, è possibile sfruttare un altro programma che riesce ad automatizzare anche questo aspetto: PhishMailer. Esso permette di scegliere uno dei vari siti messi a disposizione, allo stesso modo di HiddenEye o Nexphisher, ma alla fine del processo andrà a creare un file HTML. Aprendolo apparirà il sito falso come accadeva anche per gli altri programmi, ma la peculiarità di PhishMailer è la personalizzazione: sarà possibile durante la creazione inserire delle informazioni personali per rendere il tutto ancora più veritiero, ad esempio nel caso della pagina finta di Instagram sarà possibile inserire il nome della persona proprietaria dell'account e anche il nome stesso del profilo presente sul social network. Il link, che molte volte viene mostrato alla vittima come se fosse uno veritiero, nasconde al suo interno il link falso di un altro sito creato per la raccolta dati. Con tutte queste possibilità si può addirittura pensare all'utilizzo di tutti questi programmi per una simulazione il più soggettiva e veritiera possibile: HiddenEye o Nexphisher per la creazione dei siti falsi per la raccolta dati, PhishMailer per la creazione del file HTML contenente le informazioni personali che spingono la vittima a cliccare sul link ed infine King Phisher come mezzo per la diffusione. Durante i vari test non sono però mancati i problemi da affrontare, ma, tra tutti, quello più ostico è stato il trasporto del link falso creato da HiddenEye o Nexphisher al di fuori della macchina virtuale. Questi programmi permettono di scegliere varie opzioni per la creazione del sito, ma, tralasciando quelli segnalati già da essi come indisponibili, rimanevano solo due opzioni: localhost e Ngrok. La scelta più ovvia era la seconda: grazie al suo tunnel infatti è possibile caricare il sito web in localhost su uno dei server messi a disposizione, rendendolo così accessibile a chiunque acceda al link di Ngrok correlato. Per poter utilizzare questo servizio, era necessario la creazione di un account per aver accesso ad un token di autenticazione: una volta impostato sulla propria macchina virtuale, sarebbe stato possibile controllare lo stato dei server creati dal loro sito. Purtroppo, o per fortuna a seconda del caso, le politiche di Ngrok prevedono il ban automatico per chiunque tenti di accedere ai propri servizi per scopi di phishing e quindi, non appena si caricava la pagina con all'interno installato il programma malevolo, essa si trasformava in una di errore dove veniva segnalato che l'account in questione aveva violato i termini di privacy.

Dopo alcune ricerche sul web, è risultato inutile anche contattare il servizio clienti poiché non viene accettato l'utilizzo del phishing sui propri server neanche in caso di scopi puramente didattici o educativi. Successivamente, si è deciso dunque di passare ad un'altra soluzione attraverso un altro mezzo molto simile ad Ngrok: LocalXpose. Il funzionamento è lo stesso, la differenza sta nei tipi di tunnel che vengono creati e nessun ban automatico per creazione di contenuti di phishing. L'unico neo, se così lo si vuol chiamare, è la possibilità di aprire solamente un tunnel HTTP con l'account gratuito.

Se per questa problematica si è riusciti a trovare una soluzione attraverso l'utilizzo di un altro mezzo simile, storia diversa è quella che riguarda la seconda, ovvero i problemi di autenticazione con il server SMTP da parte di King Phisher. Ancora prima di iniziare ad utilizzarlo, così come descritto all'interno della pagina GitHub del creatore, bisogna modificare alcune impostazioni necessarie per il funzionamento e tra queste è presente il server SMTP a cui connettersi per l'invio delle mail. Sempre dalla loro pagina, sono presenti due server SMTP pubblici a cui è possibile connettersi, uno relativo agli indirizzi gmail con porta di rifermento 465 e l'altro invece per quelli di office365 con porta 587. Quest'ultimo risulta irraggiungibile, quindi l'unica opzione è collegarsi al server SMTP di Google, ma purtroppo il processo di autenticazione porta sempre ad un fallimento. Il problema sta nelle impostazioni di sicurezza della mail di Google, le quali bloccano i tentativi di accesso al servizio da programmi di terzi. Nel caso in cui si voglia disattivare questo blocco, non è più possibile farlo dal 30 maggio 2022. Come è si può notare in Fig. 4.13, questa misura è stata presa per evitare accessi indesiderati da parte di hacker sul proprio profilo. Ancora una volta la sfortuna nella fortuna. Considerato che al momento la via più facile risulta ostruita, si è dunque decisi di passare per quella un pò più lunga. Accedendo ad un account di posta elettronica Outlook, se si modifica il campo relativo al messaggio della mail come un HTML, è possibile inserire la mail finta creata da PhishMailer. In questo modo si va sicuramente incontro ad una possibile segnalazione per spam da parte del server che la riceve, ma almeno in questo modo è possibile testare la situazione durante la seconda simulazione, ovvero quella in cui si è consapevoli che la macchina di Payload Please è in funzione.

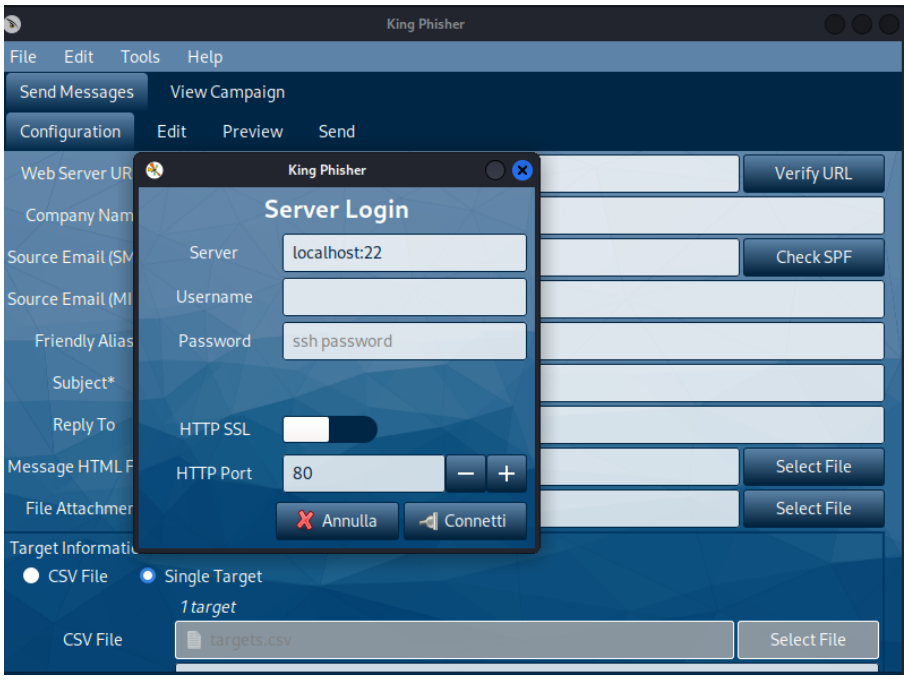


Figura 4.11: La pagina principale che viene mostrata all'utente all'avvio di King Phisher.

4.9 I preparativi per la fase di testing informatica

A causa dei problemi dovuti all'autenticazione sul server SMTP di Gmail, si è cercata una nuova strada che potesse in qualche modo essere imboccata per arrivare ad una simulazione che riuscisse

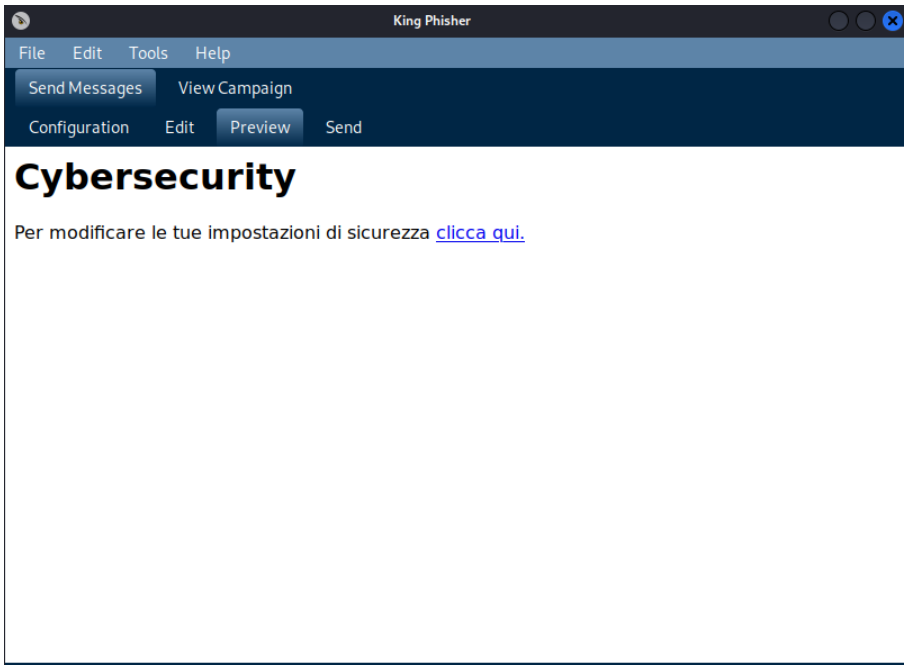


Figura 4.12: Un esempio di mail che verrà inviata alle vittime tramite l'utilizzo di King Phisher.

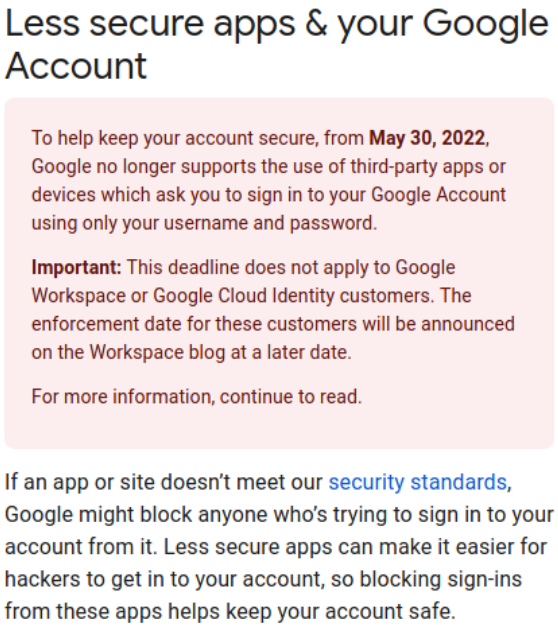


Figura 4.13: L'aggiornamento delle policy di sicurezza da parte di Google per l'accesso all'account da parte di applicazioni di terzi, datato 30 maggio 2022.

ad essere il più possibile vicina a quella proposta da King Phisher. La soluzione migliore è quella di inviare "manualmente" le mail tramite un indirizzo di posta elettronica creato proprio per questo scopo; l'unico ostacolo era il file HTML da utilizzare. Attraverso la possibilità di modificare la pagina web come un normale file HTML e il salvataggio del messaggio nelle bozze, è stato possibile attuare il tutto grazie ad un indirizzo di posta elettronica Outlook. Questa però non è stata la prima scelta, inizialmente infatti l'intento era quello di utilizzare un indirizzo di Gmail, ma purtroppo la modifica a livello di codice HTML rimaneva solamente a livello locale, senza riuscire a mantenersi oltre la creazione del template da inviare e risultando, quindi, a destinazione come una mail vuota. Una volta trovata la casella di posta da cui inviare le mail per la simulazione informatica di Payload Please, si è iniziato una fase di studio per quanto riguarda i pattern di

difesa dei vari domini di mail. I test sono stati fatti principalmente su una casella di posta Gmail, poiché molte persone in generale la scelgono per il proprio indirizzo mail privato. Dopo vari test condotti, si è arrivati a riconoscere il seguente pattern, se così è possibile descriverlo, per quanto riguarda la posta elettronica targata Google:

- Se viene ricevuta una mail contenente uno dei file HTML creato da PhishMailer e con all'interno un link che porta ad un tunnel localxpose per il sito malevolo, essa verrà inserita all'interno della casella di posta in arrivo, ma verrà segnalato all'utente come possibile tentativo di phishing;

- Se viene ricevuta una mail con un file HTML, ma con un link del tutto normale (nei test è stato utilizzato quello per la home di Google), verrà comunque inserita in posta in arrivo ma segnalandola sempre come possibile phishing;

- Se è presente solo il link malevolo inserito senza alcun HTML come se fosse un normale messaggio di posta elettronica, finirà all'interno della posta in arrivo senza alcuna segnalazione da parte del sistema.

Al di fuori di questi casi riportati, non si esclude la possibilità che il dominio di posta elettronica possa in ogni caso inserire la mail all'interno della categoria Spam. Una cosa interessante notata durante i test è la seguente: nel caso in cui il dispositivo che accede al link di LocalXpose abbia un antivirus attivo in quel momento, non appena si accederà alla pagina malevola esso bloccherà il caricamento della suddetta, segnalando all'utente che stava accedendo ad un sito pericoloso. Questa misura di prevenzione probabilmente entra in funzione poiché l'unico tipo di tunnel che è stato possibile creare tramite LocalXpose è uno di tipo HTTP, andando quindi ad apparire subito come un sito non sicuro e, con buona probabilità, la scelta dell'antivirus di bloccarlo si sarebbe applicata anche nel caso in cui esso fosse del tutto innocuo. L'aspetto da sottolineare è che anche nel caso in cui il sistema di difesa del dispositivo dell'utente non faccia accedere effettivamente alla pagina, il programma in ascolto riesce comunque a salvare l'IP pubblico della vittima, lasciando all'attaccante un'informazione non di poco conto. La conclusione a cui si è arrivati dopo i vari test e i pattern riconosciuti, è che per Gmail un file HTML all'interno dell'oggetto della mail viene riconosciuto come possibile minaccia, lasciando poi il compito all'utente di capire se lo sia o meno effettivamente. Per rendere le cose più complicate e imprevedibili è necessario far risultare qualunque mail almeno sospetta, così da stimolare l'utente a concentrarsi bene per capire se quello che ha davanti a lui è qualcosa di cui fidarsi o meno. Si è dunque pensato di inserire un file HTML in ogni oggetto della posta da inviare, ma, se fosse qualcosa che non ha alcuna relazione con il resto della mail, sarebbe facile intuire che quella aperta in quel momento è totalmente sicura e l'HTML presente sia stato inserito solamente per tentare di trarre in inganno l'utente. Per evitare ciò, attraverso una semplice proprietà del CSS, l'intero file HTML sarà invisibile all'utente: in questo modo la mail verrà comunque segnalata come sospetta ma, senza vedere qualcosa fuori luogo, si spera possa far ragionare l'utente sul da farsi e analizzare bene ogni elemento presente. Alcuni attacchi riproposti sono simili a quelli visti in precedenza con il prototipo di carta, altri invece nuovi si basano sulla disponibilità data da Nexphisher o PhishMailer, mentre per quanto riguarda la parte relativa alla sensibilizzazione si cerca di analizzare quanto le persone siano a conoscenza effettivamente di alcuni elementi della sicurezza informatica e di incitarli a passare a forme di difesa più sicure di quelle attualmente in uso. Alla fine dei test verrà riportata la classifica contenente i punti ottenuti e quelli massimi ottenibili per ogni casisitica proposta e, alla fine della sua presentazione, verrà illustrato un breve questionario per controllare quale sia il livello di stress presente nelle persone che hanno preso parte alla simulazione, così da poter valutare con dei dati alla mano una possibile ripresentazione di Payload Please. In questo caso non farò da semplice macchina come con il prototipo di carta, bensì farò le veci di uno dei colleghi della persona attualmente sotto test, così da poter simulare comunque un lato cooperativo o in alcuni casi anche competitivo: in questo modo sarà possibile testare i cambiamenti apportati al prototipo cartaceo originale e l'affidabilità e l'utilità del sistema nel caso in cui venga riproposto una seconda volta dopo aver svelato a tutti l'esistenza di Payload Please.

4.10 I test del prototipo informatico e i possibili miglioramenti

I test sul nuovo prototipo informatico hanno seguito esattamente lo stesso schema utilizzato per quello di carta: si introduce l'utente allo scenario e vengono proposti uno alla volta i casi da analizzare, l'unica differenza è il mezzo che viene utilizzato per effettuare la simulazione. Anche in questo caso si è seguito il metodo per la valutazione delle azioni dei partecipanti in base all'algoritmo descritto nel paragrafo precedente (§ 4.5). I buoni risultati ottenuti nella prima fase di testing cartacea sono stati confermati generalmente anche in questo nuovo tipo di test. In questo caso il numero di partecipanti è leggermente diminuito rispetto al prototipo di carta, assestandosi su 10 partecipanti distribuiti sempre tra le 3 categorie di personas, nello specifico: 2 esperti di Cybersecurity, 4 lavoratori e 4 studenti. I parametri seguiti per la valutazione sono due: il primo è un'intervista agli utenti riguardante la differenza percepita tra il prototipo cartaceo e quello informatico, le modifiche effettuate e il divertimento percepito; il secondo è l'interpretazione dei dati ricavati tramite il questionario post test, al fine di monitorare il livello di stress percepito dall'utente. Vengono, inoltre, inseriti commenti degli utenti ritenuti particolarmente interessanti e che servono da spunto per le fasi successive: ad esempio, il seguente è relativo al livello di divertimento provato durante la simulazione:

> "Rispetto al prototipo di carta avere il tutto su computer e con il rischio che uno sbaglio possa risultare effettivamente fatale rende il tutto molto più realistico e da un certo punto di vista anche divertente. L'aggiunta poi del punteggio massimo raggiungibile mi piace perché adesso posso sapere quanto ancora posso migliorare su un certo argomento rispetto ad un altro in cui magari sono andato meglio."

Il fattore del divertimento si è mantenuto sugli stessi livelli del prototipo cartaceo: dopo la simulazione, sulla domanda relativa ad esso, per l'80% dei partecipanti si è rilevato essere agli stessi livelli rispetto alla prima prototipazione, trovando nello storytelling uno strumento migliorato rispetto al caso precedente; grazie ad esso, infatti, è stato possibile immergersi maggiormente nelle casistiche. Il focus principale relativo alla sensibilizzazione è rimasto invariato e tutti gli utenti hanno avuto un commento positivo su questa tematica, in particolar modo dovuto al racconto dello scenario e alla presentazione dei diversi casi di colleghi che possono relazionarsi in qualunque momento con l'utente, in modo da rendere la simulazione molto più realistica. Oltre al collega amichevole e sempre pronto a dare una mano quando serve, serviva anche inserire un contrappeso negativo per poter rendere le cose anche più divertenti e dalla soluzione meno ovvia, arrivando quindi a creare una seconda figura da contrapporre al collega sincero. La sua nascita è avvenuta in un secondo momento, inizialmente infatti si era pensato di inserire una sorta di modalità "hardcore", la quale prevedeva alcuni punti extra sul totale guadagnato in cambio della disattivazione dell'antivirus, in modo da affidarsi totalmente ai propri mezzi. Successivamente, grazie all'intervento di Chiara, questa feature è stata rimossa perché è stata ritenuta poco educativa: il messaggio che poteva far trasparire era quello di aumentare la competitività togliendo però sistemi di sicurezza. Questo scambio poteva essere potenzialmente rovinoso, specialmente se la competizione che ne poteva nascere non era sana, perciò si è deciso di trasformare questa parte introducendo una sorta di "boss malvagio" dei videogiochi, il quale proverà a tentare l'utente in vari modi: può proporre di disattivare l'antivirus durante il periodo della simulazione di Payload Please per avere dei punti extra in cambio, oppure di consegnare le soluzioni dei prossimi test in cambio di alcune informazioni personali. Così facendo, si è cercato di simulare anche possibili attacchi di Social Engineering interni all'azienda stessa e i comportamenti degli attaccanti che iniettano un ransomware nel nostro sistema per poi chiedere un riscatto oneroso in cambio della liberazione dal malware. Ancora una volta, il professore Atzeni si è offerto di testare il prototipo informatico dopo aver già contribuito in precedenza con quello cartaceo, i cui commenti si sono rivelati puntuali e utili anche in questa situazione.

> "Le modifiche sembrano avere avuto un buon risultato in generale, ma ci sono ancora alcuni punti in cui si potrebbe aggiungere qualcosa in più per migliorare la simulazione. Ad esempio, nella classifica finale mostrata, l'idea di inserire a quale tentativo di

attacco o sensibilizzazione sia associato il punteggio ottenuto è una buona idea, ma se possibile sarebbe bene inserire le descrizioni di alcuni esempi di casi reali che illustrano uno scenario uguale o quantomeno simile, in modo da coinvolgere ancora di più l'utente. Bene la parte di storytelling, il quale riesce ad alternare elementi puramente informatici ad altri in cui è presente una forte interazione sociale, come ad esempio nel caso del collega che prova a far abbassare la guardia in cambio di punti facili. L'unica cosa che si potrebbe migliorare in questo aspetto è far partecipare persone che lavorano nell'ambiente, le quali potrebbero dire qualcosa che possa in qualche modo mettermi nella posizione di pensare bene a come comportarmi con loro: una persona del settore, ad esempio, che conosce tutti gli aspetti che si celano dietro alla sicurezza dell'università, può in qualche modo imporre la sua opinione anche solo con la mimica facciale o i gesti, elementi questi da non sottovalutare in un discorso faccia a faccia. L'ultimo aspetto che si potrebbe valutare è la possibilità di inserire altri argomenti su cui incentrare i test, così da poter creare due simulazioni diverse: la prima per esperti di sicurezza informatica e che contiene maggiori tecnicismi, la seconda per le persone meno esperte e che punta molto sui concetti base e la sensibilizzazione."

Terminata la fase di testing, si è quindi passati all'analisi delle considerazioni fatte da ogni partecipante e dei riscontri inseriti nel questionario post test da ognuno di loro: in questo modo è possibile valutare la possibilità di riproporre Payload Please negli ambienti di cui fanno parte gli utenti, concentrandosi in particolar modo sui livelli di stress rilevati che, in questo caso, si è riscontrato in quantità maggiori tra i lavoratori piuttosto che tra gli studenti. Infatti, il valore medio calcolato per questi ultimi si aggira su un valore pari a 3, mentre per l'altra categoria sul 3.2, definendo l'ambiente universitario come un ambiente meno stressante nel quale ripresentare Payload Please. Successivamente, sono stati definiti i possibili miglioramenti per quella che potrebbe rappresentare la versione definitiva:

- Inserimento di casi reali nella classifica finale, così da sensibilizzare ancora di più sull'importanza della sicurezza informatica in primis e in secondo luogo per mostrare come le simulazioni proposte da Payload Please possono aiutare per evitare di far accadere nuovamente gli stessi errori;
- Ampliamento delle tematiche da affrontare nelle varie simulazioni, così da avere la possibilità di proporre due simulazioni diverse. I possibili argomenti sono: il GDPR e la protezione dei dati personali, elementi di Computer Forensics, l'importanza di alcuni elementi come le TPM 2.0, il firewall o la VPN, possibili tentativi di Reverse Engineer;
- Con l'aumento del numero di argomenti proponibili agli utenti, si potrebbe anche distribuire il periodo di simulazione in più giorni, in modo da poter analizzare anche le reazioni su test ancora più specifici;
- Coinvolgimento da parte di personale tecnico all'interno delle simulazioni, in modo tale da poter avere persone pratiche del settore che possono aumentare il grado di sfida per gli utenti sotto simulazione.

Analisi particolare va fatta per le nuove tematiche da aggiungere alle possibili simulazioni. Esse, infatti, sono state pensate per cercare di venire incontro sia alle persone più esperte nell'ambito Cybersecurity, sia a quelle che vogliono entrare in questo mondo ma non hanno particolari competenze. Per quest'ultima categoria, infatti, sono indirizzate le simulazioni che si basano su concetti base e che vanno a ritoccare quelle che sono delle precauzioni che nella maggior parte dei casi già vengono prese. Ad esempio, nel test sulla VPN un sistemista nelle vesti di "boss malvagio" potrebbe fare delle proposte poco ortodosse, ad esempio dicendo di averla disabilitata poiché rendeva le comunicazioni più lente e c'era bisogno di maggiore banda; a quel punto chiederebbe all'utente quali applicazioni utilizzerebbe durante questo periodo in cui la VPN non è attiva per vedere la sua reazione. Per la simulazione sull'importanza del firewall si potrebbe proporre all'utente un nuovissimo tipo di firewall comprendente IDS e IPS, ma allo stesso tempo allungherebbe i tempi di accesso al computer e limiterebbe il numero di siti visitabili utilizzando una blacklist o una whitelist, affrontando in prima persona quello che è il dilemma della scelta tra la sicurezza e

le prestazioni. Per quanto riguarda la tematica della protezione dei dati personali, è una di quelle che può essere utilizzata per entrambe le tipologie di utenti che possono partecipare alle simulazioni di Payload Please; la differenza sta nel tipo di test che viene proposto. Ad esempio, per una persona esperta il test potrebbe riguardare la presenza di alcuni dati personali di clienti specifici all'interno dei database in un periodo oltre la data di scadenza concordata con essi, mentre per il personale meno esperto la simulazione potrebbe includere una richiesta delle informazioni di alcuni clienti da parte di un'azienda di terzi che non è mai stata nominata in precedenza con i diretti interessati. Altra tematica interessante è di sicuro la parte relativa alla Computer Forensics, la quale, in questi ultimi anni, ha guadagnato sempre più importanza anche per il suo impiego nel campo investigativo: l'esempio che verrebbe proposto al pubblico più tecnico ed esperto è la sensibilizzazione su uno dei problemi di maggiore interesse per le aziende, ovvero il data breach. La simulazione prevede la richiesta di un collega di una pennetta contenente del materiale importante riguardo progetti e clienti dell'azienda: la parte più importante di questo test riguarda le successive rassicurazioni che vengono fatte all'utente sotto test, affermando che verrà usata solo per spostare dei file da un computer all'altro e, nel caso non si fidi totalmente, può anche procedere a copiare i file presenti sulla chiavetta USB sulla propria macchina e cancellarli una volta finito. Altra possibile simulazione su questa tematica potrebbe vedere un utente sottoposto ad una sorta di "interrogatorio" da parte di un esperto forense, il quale sta indagando su una problematica che da li a qualche giorno si sta verificando in azienda, ad esempio l'introduzione di un malware nei sistemi. Per tentare di capire quale sia il problema, le domande che vengono poste sono relative a come l'utente abbia eseguito alcune azioni nei giorni precedenti, ad esempio se ha utilizzato alcuni dispositivi di alcune marche specifiche, se ha lavorato solo con il laptop aziendale, oppure se ha trovato in giro una certa pennetta, la quale potrebbe essere incriminata di aver trasportato malware. Nei giorni successivi, mentre il team di sicurezza si occupa del malware, l'esperto forense potrebbe ripresentarsi e proporre alcune soluzioni per limitare i danni, ad esempio proponendo di usare solo sistemi live e macchine virtuali per evitare di diffondere ulteriormente il software malevolo nel caso sia presente già nella memoria di alcuni computer. Altra tematica rilevante è l'importanza della TPM: per spiegarne il ruolo agli utenti meno esperti, si può proporre di effettuare un downgrade del proprio sistema operativo da Windows 11/10 a Windows 7/XP, usando come scusa la lentezza di computazione dei computer e spiegando che in questo modo si dovrebbe risolvere il problema. In realtà, questa simulazione vuole far capire all'utente come siano necessari i sistemi operativi di ultima generazione, specialmente per la parte di sicurezza, mentre quelli più vecchi sono ormai obsoleti da molti punti di vista e non più supportati dalla casa produttrice. Con queste nuove tematiche, che vanno ad aggiungersi a quelle già presentate nel prototipo cartaceo e in quello informatico, si cerca di includere il maggior numero di argomenti possibili all'interno delle simulazioni, senza togliere la possibilità di inserire ulteriori elementi in futuro che andrebbero ad espandere gli orizzonti raggiungibili da Payload Please. La grossa novità sta nel fatto che, sebbene la macro-tematica sia sempre la Cybersecurity, con queste nuove tipologie di simulazioni si vanno anche ad introdurre degli elementi molto importanti, come l'inadeguatezza dei sistemi operativi più vecchi o la scelta tra performance e sicurezza: in questo modo, si potrebbe rendere Payload Please un ottimo sistema di sensibilizzazione per più argomenti, i quali ruotano tutti intorno a quello più grande relativo alla sicurezza informatica.

L'ultimo aspetto da analizzare sono le risposte ricevute per il questionario post test sia da parte di studenti che di lavoratori. Dai risultati ottenuti si è notato come per i primi la simulazione potrebbe essere riproposta nuovamente anche in tempi brevi, dato che i relativi responsi riportano un livello di ansia e stress non troppo alto, mentre per l'altra categoria di utenti è apparso il risultato opposto. Le occupazioni dei lavoratori che sono stati presi sotto esame sono risultate quasi tutte abbastanza frenetiche, mentre l'ambiente di lavoro creato con i colleghi risulta in tutti i casi amichevole e ispirante. Basandosi solamente sui risultati del questionario, al momento si potrebbe riproporre un nuovo test per la categoria degli studenti senza troppi problemi, mentre per i lavoratori bisogna analizzare bene ogni situazione nello specifico e in alcuni casi si potrebbe pensare di ripetere il tentativo con una "difficoltà diminuita" per non superare il limite di stress sopportabile, sfociando così in un risultato negativo. Tralasciando questo aspetto, i test sono andati molto bene e i risultati sono positivi, con queste altre modifiche che sono venute fuori attraverso l'ultima simulazione si può rendere il prodotto ad un livello superiore.

4.11 Un possibile approccio "futuristico"

Il progetto di Payload Please ha utilizzato strumenti e tecnologie comuni, rimanendo sempre con un budget anche limitato per diffondere il messaggio della qualità che non sempre risulta essere il sinonimo di costoso. Durante il test del prototipo informatico con il professore Atzeni è venuto fuori un argomento interessante nella parte finale, qualcosa che porta con sé un sapore alquanto futuristico: si potrebbe valutare un approccio a Payload Please tramite le tecnologie della realtà aumentata e virtuale. Esse potrebbero rendere anche i test eseguiti da remoto molto più immersivi, basti pensare alle sensazioni che il visore della realtà virtuale ci regala, cose totalmente impensabili fino a qualche anno fa. Un esempio di applicazione di questo hardware futuristico ci viene dato dal lavoro della Texas A&M University [60], il quale ha scelto di utilizzare i visori della realtà virtuale per insegnare i concetti della Cybersecurity, dando vita al CiSE-ProS (Cyberinfrastructure Security Education for Professionals and Students). L'obiettivo posto era quello di trovare un metodo per far accedere ad un vero e proprio data center gli studenti che non potevano farlo fisicamente, in modo da imparare gli aspetti più fisici della sicurezza informatica. Infatti, all'interno della simulazione, l'utente si muoverà, grazie al visore e ai dispositivi ad esso collegati, all'interno di un centro dati e potrà "toccare con mano" componenti hardware e software che lo caratterizzano. Come si può notare, la grande utilità di queste nuove tecnologie è quella di trasportare le persone in posti che per loro sono al momento inaccessibili, arrivando anche ad attraversare migliaia di chilometri solo con l'accensione di un visore. Parlando però in termini più realistici, la realtà virtuale è ancora oggi una tecnologia a cui possono effettivamente accedervi pochi, visto che i prezzi per i dispositivi rimangono ancora molto alti: nell'esempio pocanzi proposto, il visore per la realtà virtuale utilizzato era un HTC Vive, il cui prezzo ancora oggi oscilla tra i 600 e gli 800 euro, limitando così la dimensione dell'audience raggiungibile.

Per quanto riguarda invece la realtà aumentata si potrebbe fare un discorso diverso: infatti sono sempre di più le applicazioni che abilitano questa feature, sfruttando le tecnologie degli attuali smartphone. Applicare la Gamification in un contesto simile non è assolutamente una cattiva idea, anzi può portare solo ad elementi favorevoli: se si pensa alle possibili combinazioni di elementi ludici utilizzabili, con la realtà aumentata potrebbero essere ancora di più e le simulazioni ancora più immersive e realistiche, sfruttando in questo modo veramente il nostro telefono "intelligente". L'applicazione della Gamification in generale con l'ausilio della realtà aumentata è stata analizzata già in parecchi contesti, ad esempio nello studio di R. Hammady, M. Ma e N. Temple [58] è stata utilizzata come strumento di comunicazione per un museo, mostrando come si potessero sfruttare le opere presenti nel museo come spunto per creare dei minigiochi che andassero a spiegare anche la storia che si cela dietro ad una particolare statua o dipinto. Da ciò si può dedurre come questa tecnologia possa essere una potente arma da utilizzare, in grado anche di dare vita agli oggetti e ad immergersi in un'esperienza del tutto nuova: un esempio che mostra come la realtà aumentata venga utilizzata per sensibilizzare alle problematiche della sicurezza informatica è sicuramente dato dallo studio dell'università di Deusto [61], all'interno del quale è stata fatta particolare attenzione ai ragazzi tra i 15 e i 18 anni, ovvero coloro i quali sono sempre collegati ai dispositivi mobili e diffondono le proprie informazioni personali su internet. Per tentare di far capire quanto questa pratica possa essere pericolosa, è stato preparato un serious game, grazie al quale è stato possibile dare "vita" agli intangibili concetti della Cybersecurity quali: furto d'identità, malware ed eccessiva condivisione di dati personali, ovviamente presentate con le rispettive contromisure da prendere. Da questo lavoro [61] si è potuto vedere quanta importanza venga posta per l'utilizzo di queste tecnologie in ambito educativo di ogni grado, cercando di sensibilizzare da subito a quelli che sono i rischi legati al mondo informatico.

Spostandosi, invece, verso un esempio di applicazione di realtà aumentata che applica i concetti della Gamification in ambito Cybersecurity, lo si può trovare nello studio di H. Alqahtani e M. Kavakli-Thorne [59], all'interno del quale ci si è focalizzati sulla creazione di un'applicazione che potesse diffondere maggiormente la Cybersecurity Awareness attraverso la realtà aumentata: CybAR. La base su cui si fonda è molto semplice: non solo insegna i concetti della sicurezza informatica, ma mostra le conseguenze di veri attacchi informatici accaduti e descritti tramite feedback. Quest'ultima parte è molto simile all'idea di inserire casi reali nella classifica di Payload Please per un maggiore coinvolgimento degli utenti, ma la realtà aumentata porterebbe ad un esito decisamente migliore e più immersivo. Non sono da sottovalutare però i rischi che possono venire da queste tecnologie: nel caso della realtà aumentata, essa non è altro che una possibile

applicazione dell'IoT (Internet of Things), ereditandone perciò anche i suoi stessi rischi. Come analizzato da V. D. Dissanayake [62], i dati diffusi si possono trovare in tre diversi stati: a riposo, in fase di processo e in trasmissione. Durante ognuno di essi si è soggetti a diverse vulnerabilità e soprattutto provenienti da due diverse prospettive, sia dall'architettura IoT e sia dal sistema di realtà aumentata. Grazie però ai nuovi modelli di policy da seguire, si possono mitigare questi rischi, rendendo sia i servizi che i dispositivi di questa tecnologia più sicuri.

La strada futuristica rimane quindi una possibilità significativa e, sebbene possa essere più costosa rispetto a quella seguita finora, potrebbe risultare un passo in avanti deciso verso la nuova frontiera della tecnologia e, allo stesso tempo, rappresentare una nuova soluzione per la sensibilizzazione alla Cybersecurity. Il viaggio che si è intrapreso in questo lavoro per eliminare l'etichetta di anello debole dall'uomo potrebbe aver trovato un nuovo mezzo da sfruttare per arrivare fino in fondo.

4.12 Una possibile implementazione "virtuale" per Payload Please

Nel paragrafo precedente (§ 4.11) si è visto come l'utilizzo della realtà virtuale e aumentata abbia avuto modo di allargare le prospettive per quello che riguarda la sensibilizzazione alla tematica della sicurezza informatica: si potrebbe pensare anche ad un possibile approccio di Payload Please verso queste nuove tecnologie, magari sfruttando i nuovi argomenti per le simulazioni che sono stati proposti, visto che molti di essi richiedono un contatto con altre persone e meno con il computer. Prendiamo in esempio il caso della simulazione sull'importanza del firewall: una possibile breccia in questo sistema di difesa è dato dal tentativo di IP Spoofing [63], grazie al quale è possibile, insieme ad altre precauzioni da prendere per evitare che l'attacco fallisca, accedere alla rete protetta come se si fosse in possesso di un indirizzo valido. Si potrebbe simulare, tramite realtà aumentata o virtuale, una breve scena in cui appare una finestra di dialogo contenente una domanda alquanto insolita di un collega che, per esempio, domanda quale sia l'indirizzo IP della macchina su cui sta lavorando: nel caso in cui accetti, si potrebbe mostrare all'utente come questo "collega" riesca ad effettuare un IP Spoofing basandosi sulla maschera dell'IP fornito e a superare i controlli del firewall da un computer totalmente estraneo alla rete aziendale. In questo modo è possibile avere un responso quasi immediato delle proprie azioni e, soprattutto, mettere in evidenza come la fuoriuscita di un'informazione così piccola possa risultare così dannosa. Altra tematica interessante su cui focalizzarsi è quella che riguarda l'importanza delle VPN, la loro utilità e il ruolo che rivestono all'interno del contesto "sicurezza": esse, infatti, non sono dei sistemi di protezione contro tutti i mali informatici, bensì servono per cifrare la propria cronologia e soprattutto proteggere il proprio indirizzo IP [64]; ad ogni modo, risulta necessario un antivirus nel caso in cui il sistema venga infettato da malware. La simulazione virtuale potrebbe fare leva proprio su questo aspetto, emulando l'arrivo di una mail sulla propria casella di posta elettronica, contenente un documento in allegato che, a detta del mittente, contiene delle informazioni importanti sulle nuove politiche di sicurezza dell'azienda. Nel caso in cui l'utente scelga di scaricare e visionare il file, dopo un pò si cominceranno ad intravedere alcuni errori per poi scoprire che il documento, in realtà, conteneva un malware che ha infettato l'intero dispositivo; si potrebbe inoltre illustrare come il malware vada a danneggiare il computer e i singoli file attraverso un breve video dimostrativo, andando così a descrivere con le immagini ciò che solitamente è sempre stato presentato solamente con le parole. Come dicevano i latini "Verba volant, scripta manent", anche se in questo caso più che di parole si parla di fotogrammi su un dispositivo.

Queste sono solamente alcune possibili idee di applicazione; se ne potrebbe proporre una per ciascuna delle simulazioni proposte in questa tesi. L'aspetto migliore di queste nuove tecnologie è quello di poter effettuare i test in ogni luogo, eliminando il limite fisico dell'ufficio e creando un senso di immersione maggiore: vedere attraverso lo smartphone o il visore ottico gli oggetti che prendono vita davanti a noi è un concetto affascinante, ben oltre le aspettative che si hanno con le pratiche classiche di Gamification o Serious games. Il connubio tra le esperienze passate di applicazione delle tecniche di Gamification, l'aiuto della HCI nello scoprire i bisogni e i problemi degli utenti e le nuove tecnologie futuristiche, potrebbero portare a dei risultati mai raggiunti prima, riuscendo a raggiungere anche quelle persone meno interessate alla sicurezza informatica

e perché no, magari far nascere in loro una passione per una tematica così vasta e in continua espansione.

4.13 La valutazione delle nuove casistiche

Per poter avere la certezza che le nuove tematiche proposte dopo il test informatico siano utili e ottimali, si è pensato di proporre un ultimo test indirizzato per valutare questi fattori. Innanzitutto sono state schematizzate le varie simulazioni, al fine di avere un buon numero di casistiche proposte al singolo utente che possano seguire un filo conduttore e ne aumentino il coinvolgimento delle persone. Inoltre, sono stati accorpati alcuni esempi insieme ad altri, così da non avere dei test più lunghi degli altri e, soprattutto, che possano fare da collante tra una casistica e l'altra. Ogni punto descritto per tematica viene considerato come se avvenisse in un giorno diverso da quello precedente e successivo. La prima tematica presentata è quella relativa al GDPR:

- Vengono richiesti all'utente dati personali e sensibili di alcuni clienti da inserire nel database che verranno poi cancellati dopo un paio di giorni, cercando di soffermarsi molto sui termini "personali" e "sensibili" (Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, punto 10 [65]) in modo da porre l'attenzione su questi termini;
- Viene presentato un contesto relativo alla creazione di un sito web commissionato che presenta cookie non strettamente necessari da accettare "forzatamente" per permettere il corretto funzionamento della pagina, spiegando che senza di essi alcune funzionalità del sistema potrebbero essere compromesse, arrivando ad avere un calo delle prestazioni. Si insinua così nella mente dell'utente la problematica della diffusione di dati non necessari;
- Durante una normale discussione tra colleghi spunta fuori la questione del sito web ed uno di essi propone una possibile soluzione diversa, affermando che si dovrebbero diminuire il numero di cookie da accettare e informazioni da diffondere. Viene così introdotto il "principio di minimizzazione" e la sua utilità attraverso un normale confronto con gli altri colleghi, come analizzato all'interno dell'Art. 5/1C del Regolamento UE 2016/679 [65];
- Viene fatta una richiesta particolare da parte di uno studente tirocinante in azienda, il quale chiede il permesso di utilizzare i dati personali e sensibili dei clienti per eseguire una ricerca relativa alla sua tesi, elemento questo discusso nei punti 33 e 50 del Regolamento UE 2016/679 [65]. Egli afferma che necessita di tutte le informazioni possibili di questo tipo e, a questo punto, dovrebbe iniziare una sorta di "contrattazione" per arrivare ad un numero ridotto di dati da diffondere;
- Alla scadenza dei giorni che erano stati previsti per la cancellazione dei dati sensibili e personali proposta nella prima casistica, l'utente scorge alcuni dati che sono effettivamente assenti sul database, mentre altri sono ancora presenti. Se viene fatta notare questa cosa al superiore che aveva richiesto questo lavoro, andrà a spiegare il motivo dietro questa scelta e la differenza che intercorre tra le informazioni scartate e quelle ancora disponibili.

La seconda prevede casi sull'importanza del Firewall, usando la casistica sul TPM come collante:

- Viene proposto da parte del sistemista l'installazione di un firewall di ultima generazione [67], cercando di capire da parte dell'utente quali servizi possono essere bloccati per questioni di sicurezza e quali, invece, sono necessari per i progetti su cui si sta lavorando al momento. Questo scambio di opinioni è necessario affinché la scelta dell'utente non si limiti al semplice "SI" o "NO", ponendolo davanti anche alla scelta tra performance e sicurezza;
- L'utente nota che da quando è avvenuto il dialogo con il sistemista il computer va effettivamente più lento come anticipato: una delle soluzioni proposte per questo problema è quella di effettuare un downgrade del sistema operativo attualmente in uso sul computer, passando da Windows 11/10 a Windows 7/XP. Viene spiegato che, così facendo, i computer

più vecchi possono usufruire di un sistema più "leggero" e che migliori quindi la loro velocità di calcolo. In realtà, questo caso vuole sottolineare come i sistemi operativi più vecchi siano ormai obsoleti e non più supportati dalla casa madre, mentre quelli nuovi presentano delle impostazioni di sicurezza aggiornate e migliorate. Può anche essere presentato all'utente come prova la richiesta di Microsoft della presenza del TPM 2.0 nel computer per poter installare il nuovo Windows 11 [66], proprio per la sicurezza aggiuntiva che questo dispositivo mette a disposizione;

- Uno dei colleghi particolarmente euforico afferma all'utente che la soluzione per la lentezza del computer può essere evitata se ci si collega alla connessione dati dello smartphone. Nel caso in cui l'utente non si fidi totalmente di questa proposta, lo stesso collega gli chiede l'indirizzo IP del computer che sta utilizzando, affermando che potrebbe trovare una soluzione alternativa: in questo caso l'utente corre il rischio di incappare in un possibile attacco di IP Spoofing [63] facilitato dalla sua collaborazione.

La terza tratta casi sull'importanza della VPN e che sfrutta una simulazione sulla Crittografia per un maggiore coinvolgimento:

- Viene chiesto da parte del sistemista in che fasce orarie avrebbe bisogno di essere collegato alla VPN per il progetto su cui l'utente è al momento impegnato, affermando che non è possibile al momento dare la disponibilità per l'intera durata della giornata lavorativa;
- L'utente riceve un messaggio da parte di un collega che contiene un documento in allegato: gli viene chiesto se può dare un'occhiata per controllare se ci sono errori o imprecisioni. Nel caso in cui l'utente si mostri restio nel farlo, il collega può cercare di tranquillizzarlo dicendo che quello che stanno usando è un canale protetto dalla VPN: lo scopo di questa casistica è quello di far capire all'utente che essa è un potente mezzo sicuramente, ma non protegge da tutti i mali informatici e, se dovesse scaricare un qualche tipo di malware, avrebbe bisogno di un antivirus per eliminarlo;
- Il sistemista dopo alcuni giorni spiega che non ha potuto consentire l'accesso alla VPN con costanza in questi giorni perché in azienda stanno valutando di modificare alcuni algoritmi di sicurezza propri della VPN. Viene spiegato che, a quanto gli è stato comunicato, essi dovrebbero essere molto più sicuri perché sono prodotti dall'azienda stessa e che il fatto che nessuno al di fuori di loro li conosca è una protezione in più. In realtà, sebbene le parole del sistemista sembrino essere convincenti, stanno descrivendo un caso di applicazione della "Security through obscurity" [68], un concetto sbagliato e che purtroppo si vede spesso in casi come quello appena descritto dove, nella maggior parte dei casi, si vanno solo a creare dei peggioramenti piuttosto che delle migliorie.

L'ultima, ma non per importanza, riguarda la tematica relativa alla Computer Forensics:

- L'utente viene approcciato da un analista forense [69], il quale chiede alcuni minuti del suo tempo per rispondere a qualche domanda. Egli afferma che in azienda è stato rilevato un malware e sta investigando per capire quale sia stato il mezzo di trasporto utilizzato per infettare i sistemi. Viene chiesto all'utente se ha utilizzato dispositivi di una certa marca, oppure se abbia usato dispositivi al di fuori del computer aziendale: alla fine, dopo aver annotato le sue risposte, consiglia all'utente di adottare momentaneamente soluzioni alternative per il suo lavoro, ad esempio l'utilizzo di macchine virtuali, in modo tale da non diffondere ulteriormente il malware e danneggiare altre risorse;
- Un collega chiede in prestito una pennetta all'utente, la quale contiene dati personali e sensibili di alcuni clienti dell'azienda e viene affermato che lo scopo è un semplice passaggio di dati da un computer all'altro. Se l'utente si mostrasse restio a prestarla, il collega potrebbe cercare di convincerlo affermando che può scaricare tutti i dati sul suo computer e poi cancellarli prima di consegnargliela: nel caso in cui faccia effettivamente così, dopo poche ore gli verrà riconsegnata senza alcun problema. La seguente casistica vuole concentrarsi su una possibile problematica, il data breach: attraverso una veloce analisi, si possono ricavare i dati precedentemente memorizzati nella pennetta e, sebbene non siano visualizzati dal PC, sono ancora presenti e accedibili;

- L'analista forense ritorna, spiegando che sono riusciti a individuare e ad eliminare il problema del malware, chiedendo inoltre se in questo periodo abbia seguito i suoi consigli. Se l'utente ha prestato la pennetta nel giorno precedente, gli viene fatto notare come alcuni dati siano stati inseriti su un database particolare in azienda e che normalmente non dovrebbero esserci: viene spiegato l'errore fatto dall'utente nel giorno prima e come è stato effettivamente possibile fare una cosa simile. Nel caso in cui non abbia mai accettato l'offerta del collega, si limiterà semplicemente a spiegare come si sono liberati del malware.

In questa ultima fase di valutazione sono state testate tutte le tematiche pocanzi descritte con 4 utenti diversi e appartenenti alle categorie degli studenti e degli esperti, in modo tale da poter avere una valutazione su ognuna di esse e ricevere eventuali critiche costruttive sulle nuove casistiche. Con essi il numero di partecipanti alla sessione di testing arriva ad un totale di 26, sul cui valore è stata calcolata la media dei partecipanti ad ognuna delle 3 sessioni di test, assestata sul valore di 8.66, e anche la varianza statistica dei partecipanti, arrivata ad un valore di 1.33. Anche per quest'ultimo test si è seguito l'algoritmo di valutazione dell'operato degli utenti durante i test, come presentato precedentemente (§ 4.5). Gli esiti in questa fase sono stati positivi e tra i vari aspetti valutati durante le simulazioni risultano anche alcuni che sono stati pensati in ottica di sviluppi futuri: ad esempio, è stato chiesto agli utenti un parere sulla possibilità di inserire maggiore varietà di tematiche all'interno della singola simulazione settimanale e che seguono sempre un filo conduttore, avendo la maggior parte dei pareri positivi su questo punto di vista, specialmente perché così facendo è possibile avere una visione d'insieme più ampia e degli scenari di storytelling più coinvolgenti. Altro quesito posto agli utenti è quello riferito alla trasposizione della simulazione di Payload Please nel corso di più giorni, come simulato anche durante questi stessi test, ricevendo ottimi responsi anche da questo punto di vista: le motivazione principali relative a questa eventualità vengono dalla possibilità di avere un momento di "divertimento" durante la giornata lavorativa ma che non intralcia comunque la produttività e, soprattutto, risulta più facile immagazzinare le informazioni ricevute durante i test. Il fattore divertimento, inoltre, è rimasto invariato rispetto al primo prototipo informatico proposto, mentre il lato storytelling è migliorato ed è stato un punto forte di quest'ultima simulazione. Sono inoltre disponibile all'interno dell'Appendice D dei possibili casi d'uso per le tematiche presentate in questo paragrafo. Tirando le somme di quelli che sono stati i vari test messi in atto in questi mesi, a livello statistico sui 26 partecipanti totali si ha avuto un feedback positivo da 20 persone (circa l'80% dell'utenza), limitandosi a solo un 20% quelli negativi, i quali però racchiudevano in essi critiche costruttive e opinioni volte a migliorare il prodotto finale. Grazie ad esse, si è arrivati ad una buona versione di Payload Please, andando così anche a levigare quelli che erano dei punti critici in precedenza.

4.13.1 Possibili casi d'uso in realtà aumentata delle nuove casistiche

Se si guardasse in ottica futuristica, con questo nuovo livello di storytelling raggiunto si potrebbe avere un approccio molto positivo anche con la realtà aumentata o virtuale, sfruttando così appieno anche i momenti in cui non è possibile un'interazione diretta con colleghi universitari o di lavoro. Esistono diversi strumenti in realtà aumentata e virtuale che possono aiutare ad elevare il realismo e lo storytelling delle simulazioni: in particolar modo, l'applicazione Metaverse [71] è un ottimo strumento che permette di creare interazioni e, tramite queste, una narrativa scorrevole e accattivante. Ci si potrebbe ispirare anche al pattern adottato da Wonderscope [70] il quale ha come target un pubblico dell'età dell'infanzia e che trasforma il mondo intorno a loro in storie in tempo reale: il suo punto cardine, da questo punto di vista, è l'interazione che l'utente ha con il racconto che scorre all'interno del suo dispositivo, parlando con i personaggi e ascoltando le loro risposte come se fossero proprio davanti a loro. Se si riuscissero a coniugare in un'unica soluzione la possibilità di creazione di storie di Metaverse e le interazioni di Wonderscope, si potrebbero creare delle casistiche molto realistiche e coinvolgenti, in grado di toccare i punti d'interesse dei singoli utenti con simulazioni ad hoc per loro. Ad esempio, nei casi proposti per la tematica della Computer Forensics, poter vedere i risultati delle proprie azioni in diretta, magari con una piccola dimostrazione di come sia possibile ricavare i dati presenti in precedenza all'interno della chiavetta USB, può essere un metodo migliore per spiegare l'importanza di questi concetti. Altro aspetto importante che si potrebbe analizzare, con le tecnologie sopra discusse, è l'interazione con

l'analista forense, il quale reagirebbe in maniera realistica alle risposte ed alle azioni dell'utente. Anche con il tema relativo al GDPR si potrebbero pensare diverse soluzioni, per esempio simulando la conversazione con il cliente che richiede il sito con i cookie da accettare forzatamente: in questo modo si potrebbe avere una relazione "diretta" e lo scambio di opinioni potrebbe portare a far cambiare idea sul progetto da sviluppare e ritornare, così, nella giusta direzione. Oppure, si potrebbe descrivere l'approccio del superiore che, tramite un'applicazione dello smartphone, analizza i dati nel database, i quali risultano violare alcune normative del GDPR, spiegando nel dettaglio quali eventualmente. Per quanto riguarda il firewall, si potrebbe illustrare in maniera più realistica l'interazione con il collega ed, eventualmente, cosa accadrebbe se si scegliesse di consegnargli il proprio IP e vedendo, attraverso il proprio smartphone, il tentativo di IP spoofing e le azioni che vengono eseguite spacciandosi per l'utente. Con tutte le infinite possibilità proposte da queste tecnologie, è proprio il caso di dire che "l'unico limite è il cielo", sebbene negli anni si è riusciti a superare anche quello.

4.14 L'insegnamento di Payload Please

Durante i vari mesi di preparazione dei prototipi e di testing, è stato possibile interagire con molte persone diverse tra loro, ognuna di esse con problematiche specifiche e con un livello di preparazione sulla sicurezza informatica diverso, ma grazie a loro è stato possibile migliorare sia Payload Please sia il suo approccio gamificato. Esplorare questo mondo ha aiutato a capire ancora meglio quali siano le difficoltà che le persone incontrano quando si parla di Cybersecurity e immedesimarsi in loro, per poi arrivare a proporre una soluzione prima cartacea e in un secondo momento informatica. Tutto sommato l'esperienza si è rivelata positiva, dando la possibilità agli utenti di divertirsi e allo stesso tempo imparare concetti nuovi grazie all'esperienza messa a disposizione da Payload Please. La possibilità di entrare nel mondo della realtà aumentata e virtuale, avendo così la possibilità di espandere ulteriormente gli orizzonti raggiungibili, risulta essere parecchio intrigante e stimolante. Sebbene possano cambiare le versioni del prototipo o le modalità di utilizzo, l'obiettivo rimane sempre e comunque lo stesso: sensibilizzare alle tematiche di Cybersecurity le persone, in modo da avere sempre meno bisogno di riparare i danni causati da errori che molte volte si rivelano essere dovuti ad una semplice distrazione. La prevenzione è sempre meglio della cura, forse è proprio grazie ad essa che si può eliminare l'etichetta di anello debole una volta per tutte.

Capitolo 5

Risultati

5.1 Ciò che rimane dall'esperienza di Payload Please

Una volta terminato anche la fase di testing per il prototipo informatico, è arrivato il momento di tirare le somme e vedere quali sono i risultati ottenuti in questi mesi di lavoro. Per prima cosa bisogna ripartire da quello che era l'obiettivo iniziale: cercare un metodo per applicare correttamente gli elementi di Gamification per poter sensibilizzare le persone alle tematiche della Cybersecurity. Grazie ai vari studi che sono stati presi in considerazione, ci si è subito allontanati dai possibili approcci già utilizzati, andando quindi ad intraprendere una strada del tutto nuova. Attraverso Payload Please è stato possibile scavare nei pensieri degli utenti, analizzare i loro bisogni nel campo della sicurezza informatica, immedesimarsi nei loro problemi quotidiani a riguardo e cercare di risolverli, tutto questo grazie all'applicazione degli studi di Human Computer Interaction. Senza il loro utilizzo non si sarebbe arrivati in così poco tempo ad individuare quelli che sono le maggiori problematiche percepite dalle persone direttamente interessate, contemporaneamente anche la progettazione del prototipo sarebbe stata prolungata. Gli aspetti della HCI più importanti all'interno di questo studio sono:

- L'applicazione del Needfinding: grazie ad esso è stato possibile, invece di brancolare nel buio alla ricerca degli elementi su cui porre maggiore attenzione per la sensibilizzazione degli utenti, chiedere ai diretti interessati quali fossero i problemi principali e discutere, già in questa fase, delle possibili soluzioni. Senza questa prima parte ci sarebbe stato un rallentamento non indifferente per quel che riguarda la formulazione dell'idea che sta alla base di Payload Please; inoltre, in quanto un prodotto simile non avrebbe avuto a tutti gli effetti l'utente al centro di tutto, sarebbe risultato un prodotto con livelli di usabilità probabilmente sotto la media;
- Il passaggio dalla fase di prototipazione cartacea e, successivamente, a quella informatica ha avuto dei risultati molto positivi: grazie ad esso, infatti, è stato possibile analizzare bene le possibili interazioni degli utenti con il sistema, andando quindi a sottolineare gli aspetti più problematici da sistemare e rendendo l'intera simulazione molto veloce grazie alla sua semplicità. In questo modo si è arrivati alla creazione del prototipo informatico con molte informazioni già a disposizione, sia sugli utenti, sia sui loro modi di interagire con il sistema e i test proposti;
- Il questionario di usabilità proposto alla fine della simulazione ad ogni partecipante: esso è stato il metro di paragone migliore che si potesse utilizzare per capire se la strada intrapresa dal prototipo cartaceo fosse quella giusta. Grazie al valore ottenuto dalle risposte è stato possibile catalogare il sistema con un alto livello di usabilità, senza il quale il prototipo sarebbe stato sottoposto a modifiche radicali; nel caso descritto sono, infatti, solamente state prese delle misure di ottimizzazione, così come suggerito dalle risposte degli utenti.

L'applicazione della Gamification in un contesto di "laboratorio" è un concetto molto teorico: non è possibile tenere conto di tutti gli imprevisti che possono verificarsi all'interno di una realtà

come quella aziendale o universitaria. Ci sono insidie che non sono possibili da prevedere ed è proprio in questo che è intervenuta la HCI. Il suo utilizzo, come si è potuto vedere, ha portato moltissimi benefit, limitando il numero di errori in fase di sviluppo informatico e concentrandosi su cosa serve per sensibilizzare maggiormente le persone, riportando casi d'suo realistici, fondamentali per proporre la migliore simulazione possibile attraverso il prototipo. Durante l'applicazione dei suoi concetti, sono stati posti diversi obiettivi, i quali hanno portato all'applicazione degli elementi ludici in quello che poi sarebbe diventato il prototipo descritto nei capitoli precedenti: il primo era quello di portare una ventata di aria fresca all'interno della Gamification e della sua applicazione, cosa riuscita grazie al lavoro che il sistema di simulazioni effettua durante la prima esecuzione "in background". Gli esempi che sono stati presi in considerazione e citati all'interno della tesi sono stati utili in quanto hanno dimostrato come applicare correttamente alcune meccaniche ludiche all'interno del prototipo: con questo approccio nuovo è stato possibile cogliere le reazioni e i pensieri genuini di ogni partecipante, cogliendoli impreparati sul fatto che quello che stessero affrontando in quel momento era stato tutto architettato in precedenza. Grazie a questo aspetto, è stato anche possibile migliorare il prototipo anche per la seconda esecuzione, dove ognuno è consapevole di partecipare al test.

Il secondo obiettivo era rivolto alla sensibilizzazione, tematica al centro di tutto il lavoro. Bisognava trovare un metodo che riuscisse in qualche modo a spiegare quali fossero le cose giuste e quelle sbagliate da fare relative alla Cybersecurity. Questo discorso vale soprattutto per la seconda categoria di personas che sono state descritte nei capitoli precedenti, ovvero quella dei lavoratori non esperti di sicurezza informatica, coloro i quali sono maggiormente soggetti agli attacchi. Basandosi molto anche sulle risposte date dagli utenti stessi durante la fase di Needfinding, si è arrivati alla creazione delle categorie di simulazioni viste sia a livello cartaceo che informatico, portando l'utente a poter toccare con mano questi aspetti e ad immedesimarsi il più possibile grazie anche al lavoro di storytelling e agli attacchi creati ad hoc. Tematiche come l'autenticazione a due fattori, l'importanza dei sistemi di sicurezza come l'antivirus o il firewall, la salvaguardia dei dati riservati aziendali, sono tutti elementi che servono per simulare il più verosimilmente casi realmente accaduti. Arrivare preparati ad un evento simile porta innanzitutto ad essere meno pervasi dall'ansia e da ogni altra emozione negativa, ma soprattutto al fallimento di attacchi che in tempi precedenti avrebbero provocato anche dei disastri. Con il progetto Payload Please si vuole esattamente questo: mettersi alla prova per potersi migliorare, sfruttando i propri colleghi come solidi aiuti nel momento del bisogno oppure come dei degni avversari da sfidare per essere spronati a dare il massimo durante la prova.

L'ultimo obiettivo, ma non per importanza, è quello di far divertire le persone che desiderano utilizzare Payload Please. Il punto di forza maggiore della Gamification è quello di rendere argomenti ostici e complessi, più semplici e alla portata di chiunque grazie a questo importantissimo fattore. Ovviamente bisogna sempre stare attenti su cosa utilizzare e sul come farlo, ma poter contare su un'arma così potente risulta di sicuro vantaggioso. Alla fine di ognuno dei test che sono stati fatti, sia cartacei che informatici, la prima domanda che veniva posta al diretto interessato era se si fosse divertito durante la simulazione, segno dell'importanza di questo elemento, con risultati tutti positivi a riguardo e che ha trovato nel prototipo informatico il massimo livello. Per analizzare al meglio questo aspetto, è stato inserita anche una domanda all'interno del questionario post-test: essa chiedeva un valore da 1 a 5, rappresentante il livello di divertimento percepito durante la simulazione di Payload Please. Il risultato medio raccolto è di 4.1 punti, a cui è stata affincata anche il calcolo della varianza per un'indagine qualitativa, attestatasi ad un valore di circa 0.24, stimata sui valori dati singolarmente per il divertimento percepito e sul suo valore medio: tutto ciò ha sottolineato come i progressi e i cambiamenti apportati abbiano mantenuto il suo livello percepito particolarmente alto. Grazie a questo punto, anche quando l'utente rivedeva i propri errori fatti durante i test, non si faceva pervadere da pensieri negativi, ma anzi in alcuni casi si è ritrovato a concordare con l'esito della simulazione e a confessare di fare sbagli simili molto spesso. Quindi, in fin dei conti, Payload Please è servito sia per sensibilizzare e divertire le persone, sia per effettuare una mini analisi di sé stessi, portando ad ammettere anche i propri errori e arrivando a colmare le proprie lacune, poiché non esiste miglior critico di noi stessi.

Capitolo 6

Conclusioni

6.1 Come continuare il viaggio

Durante tutti questi mesi di studio e lavoro, cercando di sfruttare al meglio la Gamification per sensibilizzare gli utenti sugli aspetti della sicurezza informatica, non sono di sicuro mancate le problematiche e gli ostacoli da superare, ma i risultati ottenuti hanno ripagato gli sforzi fatti. Grazie ai vari paper analizzati e alle testimonianze di esperti del settore, questo lavoro di tesi è riuscito a proporre un nuovo modo di applicare la Gamification alla Cybersecurity, utilizzando la Human Computer Interaction come un potente alleato per adempiere a questo scopo nel migliore dei modi possibili. Il risultato ottenuto non è di certo arrivato ad una versione definitiva, si può sicuramente migliorare e anche esplorare le nuove tecnologie per un maggior coinvolgimento.

Si pensa ovviamente al futuro, a ciò che verrà da qui agli anni a venire e a come le possibili minacce possano sempre e comunque diventare molto più complesse da analizzare e contrastare. Per far fronte a questa eventualità non troppo remota, ci sono alcuni possibili spunti possibili per degli interessanti sviluppi futuri:

- Aggiornamento costante delle tematiche affrontate nelle varie simulazioni, in modo da poter variare sul maggior numero di argomenti possibili, costruendo così una solida conoscenza su ognuno di essi. Le simulazioni cercheranno sempre di risultare soggettive e molto specifiche, facendo sentire i partecipanti sempre coinvolti in prima persona;
- Ausilio di personale tecnico, per avere riscontri molto più realistici rispetto ai prototipi proposti in questa tesi;
- Utilizzo di tecniche "futuristiche", quali realtà virtuale e aumentata, rimanendo sempre e comunque all'interno dei limiti di budget. Bisogna cercare di non esagerare su questo aspetto per mantenere il messaggio che anche Cyber Stability Games [16] vuole trasmettere;
- Maggiore automazione per le simulazioni, in moda da ridurre la necessità di avere persone che le seguano costantemente;
- Creazione di un "filo conduttore" non solo tra le varie casistiche per le singole tematiche, ma anche tra quelle relative ad argomenti diversi: grazie a ciò ed alla distribuzione della simulazione in più giorni, si potrebbe creare una versione di Payload Please ancora più coinvolgente e andare così ad aggiungere elementi "dinamici" nella sua esecuzione;
- Allargamento del bacino d'utenza considerato per questa versione di Payload Please, arrivando quindi a sensibilizzare su queste tematiche anche gli utenti che non fanno parte delle personas considerate in questa tesi. La categoria che potrebbe essere inserita è quella relativa agli studenti delle scuole superiori, in modo da approcciarsi anche ad un contesto più educativo. Partendo dal presupposto che la generazione attuale è considerata quella dei "nativi digitali", cioè coloro che, sin dalla tenera età, hanno a che fare con dispositivi

tecnologici avanzati e, il più delle volte, connessi ad Internet, può essere molto utile imprimere in loro le nozioni base della sicurezza informatica attraverso le conoscenze acquisite dall'applicazione della Gamification, come avviene, ad esempio, in Payload Please;

- Possibile creazione di una versione di Payload Please che metta insieme la Gamification ed i serious game, sfruttando questo approccio ibrido in alcuni contesti particolari: inserendo gli studenti delle scuole superiori come possibile categoria di utenti, potrebbe essere un buon metodo per farli avvicinare al mondo della Cybersecurity, considerando quanto i ragazzi siano legati al mondo videoludico.

Quello che è stato fatto finora ha semplicemente gettato le basi per il futuro, come è possibile intuire anche dalle proposte di migliorie e cambiamenti futuri; dopotutto Roma non è stata costruita in un giorno solo. Ci vuole tempo e molto studio per poter creare una strada perfettamente asfaltata che porti ad un futuro in cui la Cybersecurity non sia solamente qualcosa in più da aggiungere, ma un punto cardine. La partenza è stata segnata, il punto d'arrivo sembra essere lontano, questo è vero, ma bisogna pensare ad un passo per volta e, alla fine, si guarderà a tutta la strada che si è percorsa, senza nemmeno rendersi conto di quanto velocemente si è arrivati a destinazione. L'importante è rimanere concentrati sul proprio obiettivo: è così che l'impossibile diventa possibile, lo è sempre stato e sempre lo sarà.

Appendice A

Questionario su "Cybersecurity e Gamification"

Introduzione al questionario

Salve, sono Alessandro Rio, studente del Politecnico di Torino. Sto lavorando alla mia tesi per la laurea magistrale in Ingegneria Informatica e ho bisogno del vostro aiuto. Sto effettuando una ricerca tra gli studenti universitari dell'orientamento di Cybersecurity e tra i lavoratori più o meno esperti di Sicurezza Informatica per poter analizzare quelle che sono le maggiori problematiche affrontate sempre nel campo della Cybersecurity, in modo da trovare un metodo per poterle attenuare. Quello che vi chiedo all'interno di questo questionario sono solo alcune domande in generale sulla conoscenza della Sicurezza Informatica, sulle esperienze vissute relative ad attacchi di cui si è stati vittima eventualmente e sulle preferenze su alcuni elementi legati al mondo della Gamification. **Non esistono risposte corrette o sbagliate, è solamente un sondaggio creato per raccogliere dati che mi saranno utili per il proseguimento della tesi.**

Il modulo è anonimo, quello che chiedo è solamente di indicare il range di età di appartenenza e l'eventuale occupazione o se si è semplicemente studenti universitari. Lo scopo della mia tesi è riuscire ad allontanare il fattore umano nella Sicurezza Informatica il più possibile dal concetto di "anello debole", in modo da rendere la vita degli attaccanti più difficile.

Se volete condividere questo sondaggio anche tra altri colleghi di lavoro oppure studenti universitari di altri atenei sempre relativi all'orientamento Cybersecurity ve ne sarei grato, maggiore è il numero di dati e maggiore saranno anche le idee per migliorare.

Grazie per il vostro tempo e per le vostre risposte!

Elenco domande:

- Quanti anni hai?
- Che occupazione hai? Oppure sei uno studente universitario dell'orientamento di Cybersecurity?
- Da 1 a 5 quanto ti consideri una persona ansiosa?
- Da 1 a 5 quanto ritieni importante la Cybersecurity?
- Quando ti capita un imprevisto, riesci ad affrontarlo con coraggio oppure ti scoraggi e non sai bene cosa fare?
- Secondo te, le emozioni possono influenzare in maniera positiva o negativa il tuo lavoro / i tuoi studi?
- Nella tua esperienza, la paura di sbagliare o di trovarti impreparato ti hanno mai aiutato o spinto ad imparare concetti nuovi?

- Quando studi argomenti nuovi sulla Cybersecurity, quali sono le emozioni che provi?
  - Possibili risposte: Divertimento, Tristezza, Angoscia, Indifferenza, Allegria, Rabbia, Noia, Altro.
- Un tuo collega di lavoro/universitario ha un problema e si rivolge a te chiedendoti aiuto, come reagisci?
  - Possibili risposte: Lo aiuti volentieri, Lo indirizzi nella strada giusta e lasci che faccia da solo il resto, Scarichi questo fardello ad altri, Non lo aiuti.
- Cosa fai per controllare che il sito su cui stai navigando è sicuro?
  - Possibili risposte: Chiedo consiglio al collega più informato di me, Se non sono sicuro/a al 100% non navigo sul sito, Controllo se nell'Url è presente "https", Lascio tutto nelle mani dell'antivirus, Altro.
- Ti tieni informato/a sul mondo della Cybersecurity? Se sì come?
- Se hai risposto negativamente alla domanda precedente, vorresti approfondire l'argomento?
- Se tu avessi a disposizione una bacchetta magica con la quale poter risolvere uno dei problemi che affligge la Cybersecurity, quale sceglieresti?
- Secondo te, sfidarsi con un collega o un conoscente entrando quindi in competizione, può aiutare le due parti stimolandole a migliorarsi continuamente? Oppure preferisci una cooperazione?
- Sei mai stato/a vittima di un attacco informatico? Se sì, sei riuscito/a a difenderti o sei caduto/a nella trappola? Raccontami, se vuoi, la tua esperienza.
- Secondo te, quali sono le problematiche maggiori nel tuo lavoro/studio relative alla Cybersecurity?
- Se ti nomino la sigla "SAT" a cosa mi riferisco secondo te?
- Secondo te quali sono dei possibili aspetti negativi e positivi relativi alla Cybersecurity?
- Tra questi elementi ludici, presenti anche spesso all'interno dei videogiochi, quali preferisci?
  - Possibili risposte: Punti, Competizione tra colleghi, Competizione tra team di diverse aziende/università, Cooperazione, Ricompense, Livelli da superare, Avatar, Badges/-Trofei, Altro.
- Quando scarichi qualcosa da internet, dai attenzione al sito che stai usando?
- Ipotizza di essere a capo di un'azienda. Del budget a tua disposizione, tenendo in considerazione anche tutti gli altri costi dell'azienda da coprire, in percentuale quanto ne spenderesti per la Cybersecurity?
  - Possibili risposte: <5%, 5%, 10%, 20%, 30%, >30%.
- Utilizzi un antivirus? Lo tieni sempre aggiornato?
- Ipotizza che ti sia appena arrivata una mail o un sms che ti incita a fare una determinata azione, magari anche invitandoti a inviare alcuni tuoi dati personali per verifica. Qual è il tuo primo pensiero?

Appendice B

Questionario System Usability Scale

Il seguente questionario è stato somministrato ad ogni persona che ha preso parte alla fase di testing del prototipo di carta per la valutazione del livello di usabilità. Ad ognuno è stato chiesto di esprimere una valutazione compresa tra 1 e 5, dove 1 rappresenta "Completamente in disaccordo" e 5 "Completamente d'accordo".

- Penso che mi piacerebbe utilizzare questo sistema frequentemente.
- Ho trovato il sistema complesso senza che ce ne fosse bisogno.
- Ho trovato il sistema molto semplice da usare.
- Penso che avrei bisogno del supporto di una persona già in grado di utilizzare il sistema.
- Ho trovato le varie funzionalità del sistema ben integrate.
- Ho trovato incoerenze tra le varie funzionalità del sistema.
- Penso che la maggior parte delle persone potrebbero imparare ad utilizzare il sistema facilmente.
- Ho trovato il sistema molto macchinoso da utilizzare.
- Ho avuto molta confidenza con il sistema durante l'uso.
- Ho avuto bisogno di imparare molti processi prima di riuscire ad utilizzare al meglio il sistema.

Appendice C

Questionario post test per valutare il livello di stress

Il seguente questionario è stato ideato a seguito dei test effettuati con il prototipo di carta al fine di raccogliere informazioni sul livello di stress presente all'interno dell'ambiente in cui si è effettuato il test. A seconda delle risposte ricevute, si può orientare il test verso una versione più "soft" dei casi presentati e la competizione, mentre, nei casi che vedono un livello di stress alquanto elevato, si può arrivare a sospendere temporaneamente l'esecuzione di "Payload Please". Si ipotizza che le seguenti domande vengano poste agli utenti subito dopo la presentazione della classifica finale per la prima simulazione a cui si prende parte e aver spiegato i motivi che hanno portato al suo utilizzo.

- Ti è piaciuta l'idea di "Payload Please" e lo scopo su cui si basa?
  - Possibili risposte: Sì molto; Sì ma non appieno; Non molto ma può avere spunti interessanti; No per niente; Altro.
- Di fronte a situazioni non previste tendi ad arrabbiarti facilmente?
  - Possibili risposte: Sì molto; Sì ma riprendo subito il controllo; No è molto raro che mi capiti; No per niente.
- In quest'ultimo periodo durante il lavoro e nelle attività quotidiane in generale, ti senti pieno di energia?
- Nel caso in cui succeda qualcosa di negativo, tendi ad esagerarne l'importanza e a renderlo un ostacolo più grande di quanto sia effettivamente?
- Come definiresti il rapporto con i tuoi colleghi?
  - Possibili risposte: Abbiamo un ottimo rapporto, sia di amicizia che lavorativo; Il rapporto è esclusivamente lavorativo; Non sono ancora in grado di definirlo, sono stato assunto da poco; Non mi trovo bene con i miei colleghi, ci salutiamo a stento; Preferisco non esprimermi sull'argomento.
- Su una scala da 1 a 5, dove 1 rappresenta molto poco e 5 moltissimo, quanto ti sei divertito/a durante la simulazione offerta da "Payload Please"?
- Se hai commenti in generale o domande scrivile pure qui.

Appendice D

Descrizione di casi d'uso specifici per la simulazione di Payload Please

I seguenti casi presentati in questa appendice sono dei possibili casi d'suo testabili per coloro i quali volessero provare l'esperienza di Payload Please. In particolare, rappresentano le nuove tematiche descritte all'interno del par. 4.13 relative al GDPR, alla Computer Forensics, al firewall e alla VPN, con la definizione delle scelte a cui viene messo davanti l'utente. Entrambi sono stati pensati per un'utenza meno esperta, ma può essere utile anche per riprendere alcuni concetti importanti della Cybersecurity.

- GDPR: durante una normale giornata lavorativa, l'utente viene approcciato da un suo superiore, il quale comunica di aver bisogno di inserire alcuni dati personali e sensibili di alcuni clienti: "Mi servirebbero caricati nel database i dati di Mario Rossi, Luca Bianchi e Giovanni Neri (i nomi sono indicativi, si consiglia di utilizzarne alcuni già sentiti dall'utente sotto test per un maggior coinvolgimento), serviranno per una veloce indagine statistica e tra un paio di giorni verranno cancellati una volta esaurita la loro utilità"; a seguito, ci potrebbe essere un'interazione dell'utente per sapere i motivi più specifici e cosa serve di preciso. Il giorno dopo, viene presentato un progetto richiesto da un cliente, il quale necessita della creazione di un sito web abbastanza particolare: esso, infatti, prevede l'utilizzo di alcuni cookie non strettamente necessari, ma che, nel caso in cui non venissero accettati, porterebbero ad alcuni possibili malfunzionamenti o perdite di performance del sito. Passate alcune ore, un collega durante una pausa chiacchiera con l'utente e propone il suo punto di vista sulla situazione: "Credo che la questione dei cookie di questa pagina sia da rivedere, non è possibile chiedere ad una persona di diffondere alcune informazioni non strettamente necessarie. Sarebbe opportuno minimizzare questo aspetto il più possibile"; si presenta quindi il principio di minimizzazione. Il giorno seguente, un tirocinante dell'azienda fa una richiesta un po' particolare, a detta sua, per il suo lavoro di tesi: "Volevo chiedere se fosse possibile avere alcuni dati personali dei clienti di questa azienda, vorrei fare una piccola introduzione nella mia tesi sul lavoro che si fa qui e sulle persone che richiedono i vostri servizi. Se fosse possibile vorrei avere: nome, cognome, codice fiscale, sesso e data e luogo di nascita. In questo modo dovrei avere tutte le informazioni necessarie". A questo punto dovrebbe iniziare una sorta di "contrattazione" con il tirocinante, spiegando il motivo per cui non è possibile avere tutti questi dati personali e sensibili. L'ultimo giorno di test, l'utente controlla il database creato il primo giorno di test e che ad oggi dovrebbe essere vuoto, ma nota che presenta ancora dei dati all'interno. Parlandone con chi se ne sarebbe dovuto occupare, gli verrà spiegato il perché alcune informazioni siano già state cancellate ed altre ancora no, rimarcando la differenza tra dati sensibili e personali.
- Computer Forensics: l'utente viene approcciato una mattina da una persona che si presenta come un analista forense, incaricato di indagare sulla presenza di un malware all'interno

dei sistemi aziendali e che chiederà di rispondere a qualche domanda per aiutarlo nel suo lavoro. Le domande si baseranno su quali sono stati i dispositivi utilizzati in questi ultimi giorni e se ne ha notato qualcuno di particolare o insolito: "Per caso ha utilizzato una pennetta diversa dal solito? Magari della marca X? Oltre al computer aziendale ha usato altri computer o dispositivi?". Finita la raccolta dati, darà alcuni consigli all'utente per evitare di diffondere ulteriormente il malware, ad esempio utilizzando macchine virtuali. Dopo qualche giorno, un collega si presenta alla scrivania e chiede di poter avere in prestito la sua pennetta per passare dei dati da un PC all'altro, ma al suo interno sono presenti dati personali di clienti: "Non preoccuparti farò solo un semplice copia e incolla dei file che mi servono, ma se non ti fidi potresti cancellare tutti i dati presenti all'interno e poi darmela"; a seconda della scelta fatta in questo scenario ci sarà una conseguenza alla fine. L'ultimo giorno di test ritorna la figura dell'analista forense, il quale spiega che il malware è stato isolato ed eliminato, illustrando anche il mezzo usato per infettare i computer. Nel caso in cui l'utente in precedenza ha prestato la pennetta al collega senza prendere le dovute precauzioni, verrà notificato dall'analista la presenza dei dati presenti all'interno di essa su un database aziendale: "Quello che è accaduto è un possibile caso di data breach, bisogna porre maggiore attenzione quando si gestiscono dispositivi contenenti dati così importanti. Sebbene tu li abbia cancellati e non siano visibili sul tuo computer, è comunque possibile ricostruirli tramite alcuni programmi specifici". Se, invece, sono state prese le dovute precauzioni oppure non ha prestato la pennetta al collega, l'analista si limiterà a chiedere se ha seguito i suoi consigli in questi giorni.

- Firewall: il sistemista aziendale descrive un firewall di nuova generazione che verrà installato a breve in azienda, chiedendo quali sono i servizi che l'utente utilizza maggiormente per evitare di inserirli in blacklist o whitelist: "Considerando che stiamo per installare questo nuovissimo firewall, quali sono i siti che vorresti siano sempre disponibili? Così evitiamo di bloccarli per sbaglio". Qualche giorno dopo, l'utente nota che il suo computer ha subito un rallentamento, possibilità questa accennata anche dal sistemista se viene chiesto. Viene proposta sempre da lui una possibile soluzione: "Purtroppo questa era un'eventualità che avevamo preso in considerazione, al momento non è possibile avere dei nuovi PC in tempi brevi però se vuoi una soluzione immediata si può installare l'immagine iso di Windows XP o 7, il quale è più leggero e dovrebbe sopperire per un po' al problema, almeno finchè non avremo i nuovi computer". Questa casistica vuole evidenziare come i SO più vecchi siano ormai superati e obsoleti, senza neppure più il supporto della casa madre e con impostazioni di sicurezza ormai superate. L'ultimo giorno di test, un collega particolarmente euforico annuncia all'utente di aver trovato una soluzione alla lentezza causata dal firewall: collegarsi alla connessione dati dello smartphone. Accettare su due piedi questa soluzione è un errore, in questo modo si vanno ad evitare i controlli di sicurezza posti dal firewall, ma se si rifiutasse verrebbe proposta una nuova soluzione: "Visto che ci so fare con queste cose, mi daresti l'IP del tuo computer, così mi metto al lavoro e riesco a velocizzarlo". Il pericolo a cui ci si espone è quello di un possibile IP Spoofing: il collega potrebbe fare accessi ad alcuni servizi camuffando il suo IP con quello dell'utente e facendo risultare lui come visitatore.

- VPN: durante una mattina di lavoro, viene assegnato all'utente un nuovo progetto su cui lavorare, ma il sistemista gli annuncia che sarà possibile collegarsi alla VPN solamente durante alcuni slot temporali della giornata a causa di alcuni problemi che stanno cercando di sistemare. Dopo qualche giorno, preferibilmente durante una giornata di smart working, mentre si è collegati alla VPN un collega invia un messaggio all'utente contenente un allegato ed il seguente testo: "Ciao, scusa se ti disturbo ma potresti dare un'occhiata veloce al documento che ti ho inviato? Giusto per controllare che tutto sia stato scritto correttamente". Nel caso in cui l'utente si rifiuti di scaricare il file, il collega cerca di persuaderlo dicendo che è tutto sicuro ed è protetto anche dalla VPN: lo scopo di questa casistica è quello di far capire che essa non è una cura per ogni male informatico, se si dovesse scaricare un file infetto la VPN farebbe ben poco e in quel caso dovrebbe intervenire un antivirus per eliminare la minaccia. Dopo qualche giorno, il sistemista ricontatta l'utente, affermando che per un po' di tempo la VPN sarà offline a causa di alcuni lavori e chiedendo quali operazioni continuerà a fare durante questo breve periodo. Inoltre, spiegherà il motivo dietro a questo piccolo "blackout" temporaneo: "A quanto pare stanno sostituendo uno degli algoritmi di

sicurezza della VPN con uno nuovo, creato dalla nostra stessa azienda e che proprio per questo motivo è più sicuro rispetto al precedente". Sebbene sembrino essere convincenti le parole del sistemista, in realtà stanno descrivendo un caso di applicazione della "Security through obscurity", cosa che negli anni ha provocato molti più danni di quelli che doveva andare ad eliminare.

Bibliografia

[1] Le principali minacce informatiche nel 2022, https://www.ninjaone.com/it/blog/statistiche-sulla-sicurezza-informatica-2022/#leading

[2] Come funziona il phishing? Esempi di attacchi di phishing e definizione, https://www.cisco.com/c/it_it/products/security/email-security/what-is-phishing.html#~come-funziona-il-phishing

[3] Descrizione di 11 tipologie di attacchi Phishing ed esempi reali, https://cio.florence-consulting.it/panda-security-attacchi-phishing

[4] Tutto quello che c'è da sapere sui Malware, https://it.malwarebytes.com/malware/

[5] Descrizione dei diversi tipi di Malware, https://www.kaspersky.it/resource-center/threats/malware-protection

[6] Tattiche di social engineering: quali sono e come difendersi, https://www.dgroove.it/tattiche-di-social-engineering-quali-sono-e-come-difendersi/4469/#:~:text=La%20social%20engineering%20%C3%A8%20l,controllo%20e%20ottenere%20informazioni%20riservate.

[7] Descrizione patch USSVS: "Unità Specializzata Sicurezza Voli Sensibili", https://commons.wikimedia.org/wiki/File:Ussvs_fco.png

[8] Campagna di prevenzione attacchi della gendarmeria francese, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/campagnes-messages-escroquerie-usurpant-identite-police-nationale

[9] M. De Bonis, M. De Simone, "Gamification e Cybersecurity: gli elementi di Gamification e alcuni casi d'applicazione", https://www.ictsecuritymagazine.com/articoli/gamification-e-cyber-security/

[10] Cos'è la Gamification: introduzione all'argomento, https://www.gamification.it/gamification/introduzione-alla-gamification/

[11] I. Rieff, "Systematically applying Gamification to Cybersecurity awareness trainings: a framework and case study approach", 2018

[12] L. A. Thompson, N. Melendez, J. Hempson-Jones, F. Salvi, "Gamification in Cybersecurity Education: The RAD-SIM Framework for Effective Learning", Proceedings of the 16th European Conference on Games Based Learning, Lisbona (Portogallo), 6-7 Ottobre 2022, Vol. 16 No. 1, DOI 10.34190/ecgbl.16.1.504

[13] M. Coenraad, A, Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, D. Weintrop, "Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games", dal libro "Simulation & Gaming", a cura di T. Kikkawa, M. P. Schijven, SAGE Publications, 1988, Vol. 51 Ed. 5, pp. 586-611 DOI 10.1177/1046878120933312

[14] H. Qusa, J. Tarazi, "Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students", IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, (NV, USA), 27-30 Gennaio 2021, pp. 677-682, DOI 10.1109/CCWC51732.2021.9375847

[15] McAfee, "Winning The Game, The challenges facing Cybersecurity organizations and winning factors in Cybersecurity games", Aprile 2018, https://recursos.bps.com.es/files/848/45.pdf

[16] Cyber Stability Games: è in gioco la sicurezza informatica, https://www.securityopenlab.it/news/1665/cyber-stability-games-e-in-gioco-la-sicurezza-informatica.html

[17] Kaspersky Interactive Protection Simulation: An effective way of building Cybersecurity awareness among top managers and decision makers, https://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdf

[18] M. Adams, M. Makramalla, "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach", Technology Innovation Management Review, Vol. 5 No. 1, Gennaio 2015, pp. 5-14, DOI 10.22215/timreview/861

[19] E. G. B. Gjertsen, E. A. Gjære, M. Bartnes, W. R. Flores, "Gamification of Information Security Awareness and Training", Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP), Porto (Portogallo), 2017, pp. 59-70, DOI 10.5220/0006128500590070

[20] Feudal security, it's a feudal world out there, https://www.schneier.com/blog/archives/2012/12/feudal_sec.html

[21] K. Kapp, "The Gamification of learning and instruction: Game-based methods and strategies for training and education", Pfeiffer, 2012, ISBN: 9781118096345

[22] Gamification: lavorare giocando fa bene, ma attenti a privacy ed effetto "uomo criceto", https://tinyurl.com/2p8a78v2

[23] A. M. Toda, P, H, D. Valle, S. Isotani, "The Dark Side of Gamification: An Overview of Negative Effects of Gamification in Education", First International Workshop on Social, Semantic, Adaptive and Gamification Techniques and Technologies for Distance Learning, Maceiò (Brasile), 20-24 Marzo 2017, pp. 143-156, DOI 10.1007/978-3-319-97934-2_9

[24] P. Andrade, E. L. Law, "User-based Evaluation of Gamification Elements in an Educational Application", Proceedings of the 32nd International BCS Human Computer Interaction Conference, Belfast (Gran Bretagna), Luglio 4 - 6 2018, DOI 10.14236/ewic/HCI2018.27

[25] Le basi della Human Computer Interaction: come comunichiamo con i computer, https://www.webaccessibile.org/le-basi/come-comunichiamo-con-i-computer/human-computer-interaction/

[26] An introduction to Gamification in Human Computer Interaction, https://blog.xrds.acm.org/2016/04/introduction-gamification-human-computer-interaction/

[27] M. Carter, J. Downs, B. Nansen, M. Harrop, M. R. J. Gibbs, "Paradigms of games research in HCI: a review of 10 years of research at CHI", CHI PLAY '14: Proceedings of the first ACM SIGCHI annual symposium on Computer-human interaction in play, Toronto (Canada), 19-21 Ottobre 2014, pp. 27-36, DOI 10.1145/2658537.2658708

[28] Corso Human Computer Interaction, Politecnico di Torino, https://elite.polito.it/teaching/02jsk-hci

[29] M. A. Sasse, S. Brostoff, D. Weirich, "Transforming the "Weakest Link" : a Human/Computer Interaction Approach to Usable and Effective Security", BT Technology Journal, Vol. 19, Luglio 2001, pp. 122-131 DOI 10.1023/A:1011902718709

[30] B. Schneier, "Secrets & Lies", John Wiley & Sons, 2000 ISBN: 978-0-471-45380-2

[31] M. M. Eloff, J. H. P. Eloff, "Human Computer Interaction: An Information Security Perspectives", nel libro "Security in the information society", a cura di M. A. Ghonaimy, M. T. El-Hadidi, H. K. Aslan, Springer, 2002, pp. 535-545, DOI 10.1007/978-0-387-35586-3_42

[32] Human Computer Interaction and Security: people don't walk around if they can avoid it, https://www.htogroup.org/2020/11/19/human-computer-interaction-and-security/

[33] I. Cristescu, "Emotions in human-computer interaction: the role of nonverbal behaviour in interactive systems", Accademia di studi Economici, Bucarest (Romania), Informatica Economica No. 2, 2008, pp. 110-116, https://ideas.repec.org/a/aes/infoec/vxiiy2008i2p110-116.html

[34] K. Duggal, L. R. Gupta, "Hope Enabler: A Novel Gamification-Based Approach to Enhance Classroom Engagement", Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019), Chandigarh (India), 12-13 Ottobre 2019, pp. 501-519, DOI 10.1007/978-981-15-3369-3_38

[35] How HCI should be shaping Cyber Security, https://www.linkedin.com/pulse/how-hci-should-shaping-cyber-security-mckell-gomm/

[36] How to protect yourself? Think like a hacker, https://www.cnbc.com/2014/10/03/how-to-protect-your-data-think-like-a-hacker.html

[37] D. Katsabas, S. M. Furnell, A. D. Phippen, "IT Security: A Human Computer Interaction Perspective", nel libro "Advances in Network and Communications Engineering 2", a cura di S. M. Furnell, P. S. Dowland, University of Plymouth Network Research Group, 2005, pp. 35-42, https://www.cscan.org/?page=paperdetails&id=240

[38] R. Kainda, I. Flechais, A. W. Roscoe, "Security and Usability: Analysis and Evaluation", International Conference on Availability, Reliability and Security, Krakow (Poland), 2010, pp. 275-282, DOI 10.1109/ARES.2010.77

[39] Usability: the key to Cybersecurity in small and medium-sized businesses, https://www.watchguard.com/wgrd-news/blog/usability-key-cybersecurity-small-and-medium-sized-businesses

[40] Avoiding the choice between Security and usability: you can have it all, https://www.ncsc.gov.uk/blog-post/security-and-usability--you-can-have-it-all-#:~:text=Usability%20is%20sometimes%20seen%20as,systems%20the%20business%20runs%20on.

[41] Usability vs Security: The myth that keeps CISOs up at night, https://cybertechaccord.org/usability-vs-security-the-myth-that-keeps-cisos-up-at-night/

[42] H. Garg, T. Choudhury, P. Kumar, S. Sabitha, "Comparison between significance of usability and security in HCI", 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad (India), 9-10 Febbraio 2017, pp. 1-4 DOI 10.1109/CIACT.2017.7977269

[43] J. Grant, C. Boonthum-Denecke, "Analysis of Human-Computer Interaction Implication in Cyber Security", ADMI 2021: The Symposium of Computing at Minority Institutions, Online Conference, 25-27 Marzo 2021, https://par.nsf.gov/biblio/10284700

[44] Y. Chang, Y. Lim, E. Stolterman, "Personas: from theory to practices", NordiCHI '08: Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges, Lund (Svezia), 20-22 Ottobre 2008, pp. 439-442, DOI 10.1145/1463160.1463214

[45] A. Cooper, "The Inmates are Running the Asylum", Software-Ergonomie '99, Walldorf/Baden (Germania), Marzo 1999, pp. 17, DOI 10.1007/978-3-322-99786-9_1

[46] E. Corazziari, "Quando un progetto di Gamification rischia di fallire?", https://news.sap.com/italy/2017/01/esiste-davvero-il-lato-oscuro-della-gamification/

[47] F. Tchakounté, L. Kanmogne Wabo, M. Atemkeng, "A Review of Gamification Applied to Phishing", Preprints.org, Marzo 2020, DOI 10.20944/preprints202003.0139.v1

[48] R. J. Baxter, D. K. Holderness, D. A. Wood, "Applying Basic Gamification Techniques to IT Compliance Training: Evidence from the Lab and Field", Journal of Information Systems, American Accounting Association, Vol. 30 No. 3, Settembre 2016, pp. 119-133 DOI 10.2308/isys-51341

[49] D. Thornton, G. Francia, "Gamification of Information Systems and Security Training: Issues and Case Studies", Information Security Education Journal, DLINE, Gennaio 2014, pp. 16-24, https://www.dline.info/isej/fulltext/v1n1/3.pdf

[50] J. Brooke, "SUS: A quick and dirty usability scale", nel libro "Usability Evaluation in Industry", a cura di P. W. Jordan, B. Thomas, B. A. Weerdmeester, I. L. McClelland, CRC Press, 1996, pp. 189-194

[51] Benefici, considerazioni e definizione delle domande inerenti al System Usability Scale (SUS), https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

[52] Phishing tool "HiddenEye", GitHub repository, https://github.com/Morsmalleo/HiddenEye

[53] Phishing tool "Nexphisher", GitHub repository, https://github.com/htr-tech/nexphisher

[54] Phishing Campaign Toolkit "King Phisher", GitHub repository, https://github.com/rsmusllp/king-phisher

[55] Professional Phishing Alert Templates "PhishMailer", GitHub repository, https://github.com/BiZken/PhishMailer

[56] C. O. Breda, "Gamification for Improving Cybersecurity", Tesi di Laurea Magistrale, Politecnico di Torino, Anno Accademico 2021-2022, https://webthesis.biblio.polito.it/22846/1/tesi.pdf

[57] G. Vaudano, "Analisi e sviluppo di metodologie contrastanti attacchi di social engineering", Tesi di Laurea, Politecnico di Torino, Anno Accademico 2019-2020

[58] R. Hammady, M. Ma, N. Temple, "Augmented Reality and Gamification in Heritage Museums", Joint International Conference on Serious Games, Brisbane (Australia), 26-27 Settembre 2016, pp. 181-187, DOI 10.1007/978-3-319-45841-0_17

[59] H. Alqahtani, M. Kavakli-Thorne, "Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)", Information, Vol. 11 No. 2, Febbraio 2020, pp. 121, DOI 10.3390/info11020121

[60] J. H. Seo, M. Bruner, A. Payne, N. Gober, D. R. McMullen, D. K. Chakravorty, "Using Virtual Reality to Enforce Principles of Cybersecurity", The Journal of Computational Science Education, Vol. 10 No. 1, Gennaio 2019, pp. 81-87, DOI 10.22369/issn.2153-4136/10/1/13

[61] M. Salazar, J. Gaviria, C. Laorden, P. G. Bringas, "Enhancing Cybersecurity learning through an augmented reality-based serious game", IEEE Global Engineering Education Conference (EDUCON), Berlino (Germania), 2013, pp. 602-607, DOI 10.1109/EduCon.2013.6530167

[62] V. D. Dissanayake, "A review of Cyber security risks in an Augmented reality world", University of Sri Lanka, Institute of Information Technology, Malabe, Sri Lanka, 2019, https://www.researchgate.net/profile/Viraj-Dissanayake/publication/339941469_A_review_of_Cyber_security_risks_in_an_Augmented_reality_world/links/5e6e3c2a299bf12e23c8ba56/A-review-of-Cyber-security-risks-in-an-Augmented-reality-world.pdf

[63] A. Fato, "Tecniche di attacco e difesa per sistemi firewall", Tesi di Laurea, Università di Bologna, 2018 https://amslaurea.unibo.it/17219/1/tesi_Andrea_Fato.pdf

[64] Le navigazioni in privato e le VPN sono davvero sicure?, https://www.kaspersky.it/resource-center/definitions/how-does-vpn-keep-me-safe-online#

[65] "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679#d1e40-1-1

[66] Windows 11 più sicuro con TPM 2.0, https://www.agendadigitale.eu/sicurezza/windows-11-piu-sicuro-con-tpm-2-0-ma-non-corriamo-a-cambiare-pc/

[67] Cos'è un firewall? Definizione e spiegazione, https://www.kaspersky.it/resource-center/definitions/firewall

[68] Security Through Obscurity (STO): History, Criticism and Risks, https://www.okta.com/identity-101/security-through-obscurity/#:~:text=The%20concept%20of%20security%20through,it%20is%20no%20longer%20secure.

[69] Investigazioni informatiche forensi, utile strumento per la tutela del patrimonio aziendale, https://tinyurl.com/4hbrunu6

[70] Wonderscope: lo storytelling con la Realtà aumentata su iPad, https://www.robertosconocchini.it/realta-virtuale-e-aumentata/6782-wonderscope-lo-storytelling-con-realta-aumentata-su-ipad.html

[71] Sito web per l'applicazione sulla realtà aumentata Metaverse, https://studio.gometa.io/landing