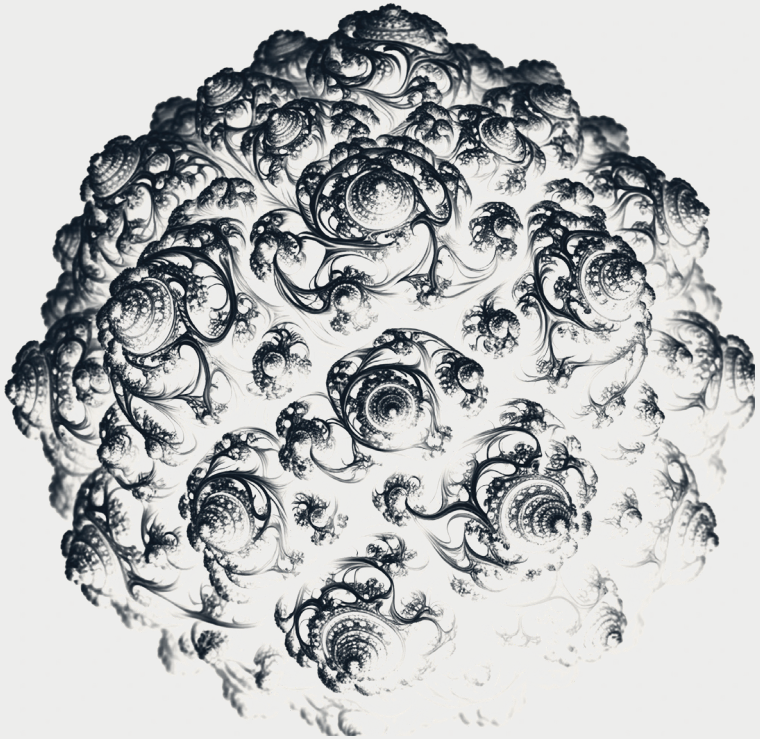
Fractal



User Experience Design e Comunicazione per la Cyber-security

Politecnico di Torino

RELATRICE
Antonella Frisiello

CANDIDATO
Luca Buffa - s271842

INSEGNAMENTO
UX Design

POLITECNICO DI TORINO

DIPARTIMENTO DI **ARCHITETTURA** E **DESIGN**
CORSO DI LAUREA IN **DESIGN E COMUNICAZIONE VISIVA**

A.A. **2023/2024**

TESI DI LAUREA DI PRIMO LIVELLO

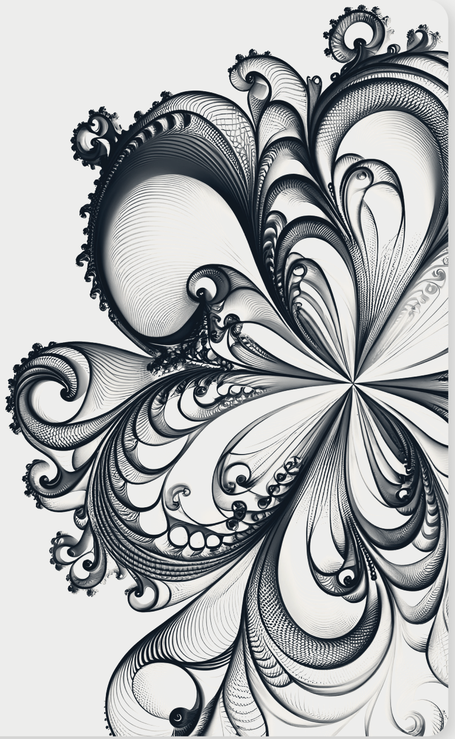
USER EXPERIENCE DESIGN E COMUNICAZIONE PER LA CYBER-SECURITY.

Politecnico di Torino

Abstract

Il seguente progetto di tesi si pone come obiettivo quello di riconsiderare il ruolo degli utenti non esperti all'interno del dominio della cybersecurity, proponendo di fatto un cambio di paradigma che identifichi nell'individuo una risorsa cruciale nel contrasto alle sempre crescenti minacce digitali, valutando al contempo in che modo gli strumenti del Design e della comunicazione possano rispondere alle sfide che propone l'attuale scenario discusso. Attraverso un approccio incentrato sull'utente, viene in fine avanzata una proposta progettuale, il Prototipo interattivo di un'app mobile, ideato e sviluppato tenendo in considerazione i dati emersi in fase di analisi di scenario e ricerca bibliografica, ricavati anche grazie agli strumenti ed alle tecniche caratterizzanti dello User Experience Design.

La Cyber-security è una responsabilità diffusa



Indice

0

Introduzione

In un mondo sempre più complesso e interconnesso, per la quasi totalità degli individui i sistemi informatici sono divenuti parte integrante della quotidianità, dall'intrattenimento, ai servizi fino alla gestione aziendale. Purtroppo, di pari passo parallelamente al progresso tecnologico continua ad accentuarsi inesorabilmente anche il fenomeno della cyber-criminalità, sempre più diffuso, competente, impattante e consapevole delle nostre vulnerabilità in quanto utenti. Paradossalmente ci ritroviamo spesso ad avere a che fare con strumenti di cui non comprendiamo a pieno le potenzialità e funzionalità, ma, che sono integrati indissolubilmente nella nostra routine, cosa ben risaputa dai Cyber-criminali che invece, al contrario, pare siano molto consci e abili nel destreggiarsi per la rete.

Nel libro "Secrets & Lies", Bruce Schneier afferma che le persone spesso rappresentano l'anello più debole della filiera della sicurezza e sostiene che siano cronicamente responsabili degli errori dei sistemi di sicurezza (Schneier, 2000, p. 257). Secondo questa narrazione, gli utenti, ovvero i cittadini connessi alla rete nell'uso di sistemi e servizi per ragioni private, di studio e lavoro, vengono identificati come "l'anello debole" nel ciclo di erogazione e fruizione dei servizi digitali.

E se così non fosse? In una visione meno banalizzante e soprattutto più articolata e moderna della Cyber-security, gli utenti (supportati da strumenti idonei) possono essere considerati una variabile positiva in grado di incrementare il livello di sicurezza informatica. Attorno a questa prospettiva ruotano le attività di ricerca e design oggetto del presente elaborato, il cui obiettivo principale è quello di conoscere, approfondire e comunicare principi di Cyber-security in un'ottica Human Centred, ovvero finalizzati a suscitare consapevolezza e competenza in utenti non specializzati.

Per raggiungere gli obiettivi stabiliti ho affrontato il processo di lavoro seguendo la metodologia dello User Experience Design, approccio che privilegia la prospettiva degli attori coinvolti, per identificare soluzioni progettuali volte a diffondere maggiore consapevolezza e competenza migliorando la qualità del rapporto fra gli utenti e la rete.

L'elaborato presenta le attività di ricerca che includono un'analisi di scenario (Capitolo1) basata su fonti on-line e casi studio che mi ha permesso di conoscere il dominio specifico della Cyber-security e successivamente delle interviste per approfondire l'analisi degli attori coinvolti (stakeholders). Successivamente vengono approfondite le dinamiche che mettono in correlazione il phishing, l'ingegneria sociale e lo User Experience Design (capitolo 2) procedendo in seguito a una disamina di "best practices" ovvero un raccolta di procedure e consigli su come riconoscere, intervenire e affrontare rischi e attacchi digitali. La panoramica risultante dall'analisi preliminare mi ha permesso di definire più precisamente il problema, che viene qui affrontato con la particolare prospettiva dello User Experience Design e alcuni principi dell'Ingegneria Sociale per la realizzazione di un Applicativo per dispositivi mobile e desktop (descritto nel capitolo 3) che intende sistematizzare una raccolta di conoscenze basilari, best practice e procedure operative finalizzate alla prevenzione e risoluzione delle criticità, in un format che vuole rendere i contenuti facilmente comprensibili e utilizzabili in contesti reali. Il concept si basa su una piattaforma web, libera e consultabile da chiunque e in ogni momento.

Gli strumenti di informazione e comunicazione qui proposti identificano come target ideale professionisti e imprese che vogliano valorizzare il ruolo attivo e positivo delle persone nella prevenzione e protezione di dati e sistemi rispetto a rischi e attacchi potenzialmente (o meglio quasi sicuramente) dannosi per le aziende e i singoli individui.

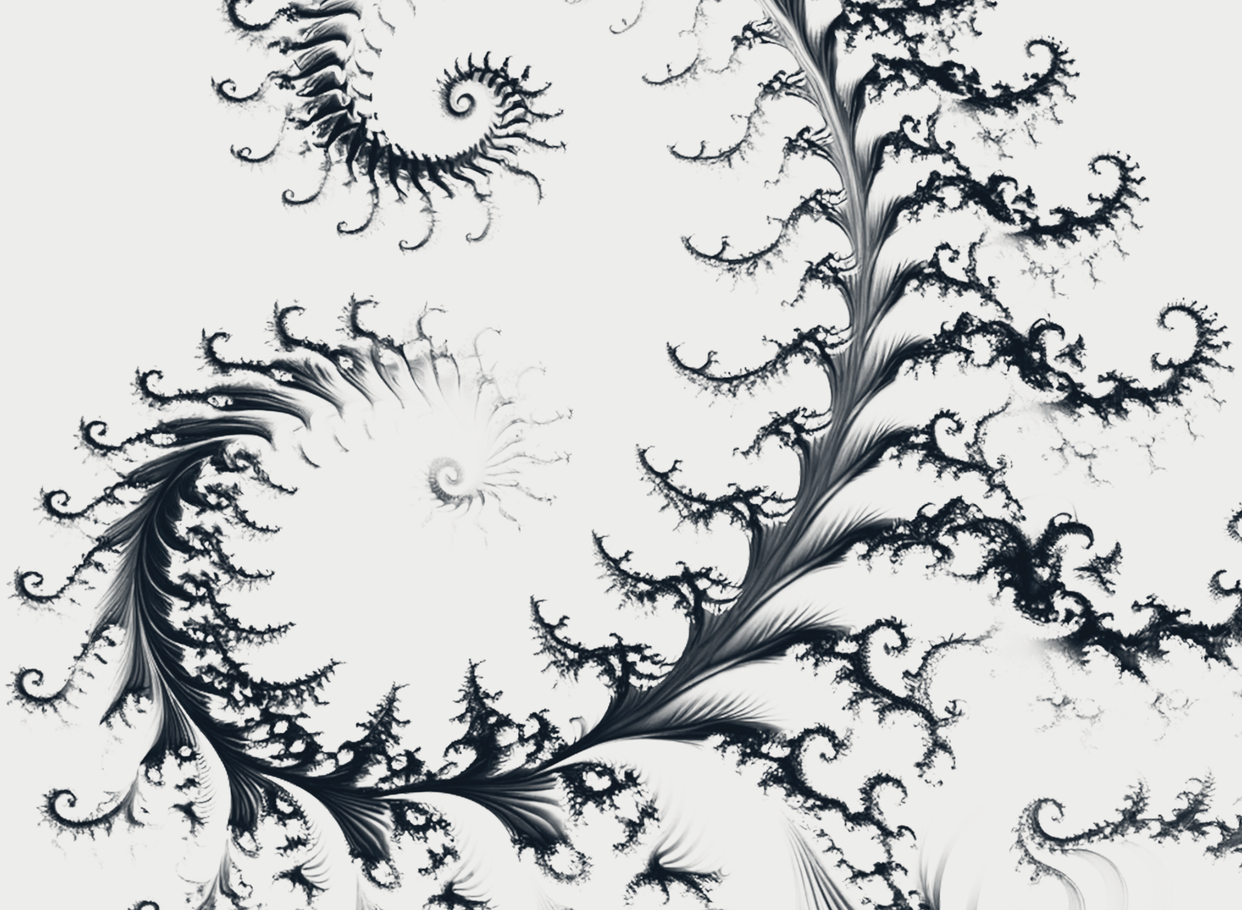
Fractal

1

Analisi di Scenario

Lo scopo di questo capitolo è definire il concetto di Cyber-security, i processi e gli strumenti che caratterizzano la disciplina.

L'analisi preliminare, condotta su fonti documentali reperite online da enti ufficiali e letteratura scientifica, definisce il perimetro del dominio e i concetti di base, gli attori principali, gli approcci e le sfide aperte.



1.1

Definizione e sviluppo storico

La **Sicurezza informatica** o **Cyber-security** è riassumibile come "Ramo dell'informatica che si occupa di tutelare i sistemi di elaborazione, siano essi reti complesse o singoli computer, dalla possibile violazione, sottrazione o modifica non autorizzata di dati riservati in essi contenuti. (Enciclopedia Treccani online, 2023). Più in dettaglio, la Cyber-security è una **branca delle discipline informatiche** che include competenze legate alla **gestione dei sistemi**, delle reti e del software. Nella sua applicazione la Cyber-security implica anche l'inevitabile coinvolgimento di qualunque **individuo** o **organizzazione** che può essere colpito. Chiunque utilizzi apparecchiature elettroniche connesse alla rete, a prescindere dalla competenza, dal settore di appartenenza o dall'estrazione sociale, oltre a essere un potenziale target, gioca un ruolo attivo e cruciale nella possibilità di favorire rischi, minacce e soluzioni preventive o protettive.

Secondo il **Kaspersky Lab**, una rinomata azienda russa specializzata nello sviluppo di software antivirus e soluzioni per la sicurezza informatica, questa pratica vede la sua nascita nei primi **anni '70** con il malware **CREEPER**[1]. Negli anni l'onda dello sviluppo tecnologico dei sistemi, dei servizi e della diffusione di internet, ha fornito al mondo grandi opportunità di crescita ed evoluzione così come considerevoli minacce. L'obiettivo della Cyber-security è **mantenere** lo stesso passo in termini di **innovazione** per contrapporre e **difendere** un uso lecito e sicuro della **rete**, cercando primariamente di **prevenire** rischi e in seguito di contenere e mitigare i danni derivanti da **attacchi informatici** deliberati.

Nel seguente elaborato si fa spesso riferimento al termine **"hacking"**, il cui significato può essere poco chiaro o addirittura negativo a causa delle **rappresentazioni superficiali** fornite dai **media**. In realtà, gli **hacker** sono **persone esperte** di informatica che utilizzano le loro conoscenze per **esplorare**, **modificare** e sfruttare i sistemi informatici.

Nonostante siano spesso associati a comportamenti illegali e dannosi, gli **hacker** possono svolgere un **ruolo** importante e **positivo** nella comunità informatica, aiutando a identificare vulnerabilità nei sistemi e a sviluppare **soluzioni di sicurezza**.

1. CREEPER:

Primo malware storicamente riconosciuto che ha infettato la prima forma embrionale di internet come lo conosciamo chiamato ARPANET.

2. Phone phreak:

Utenti che per primi si accingevano a manipolare le reti telefoniche pubbliche in maniera non convenzionale intorno agli anni '50 del 900.

Esistono due tipi principali di hacker, cosiddetti **"white hat"** e **"black hat"** (Kaspersky Resource Center, 2023). I white hat sono gli **esperti** di sicurezza informatica che si occupano della **prevenzione** degli attacchi informatici e della **protezione** dei sistemi da eventuali violazioni. Essi utilizzano le loro **conoscenze** informatiche per individuare le **vulnerabilità** nei sistemi e per **sviluppare soluzioni** al fine di mitigarle. Questi professionisti sono spesso assunti da aziende e organizzazioni governative per **proteggere** i propri dati sensibili.

D'altra parte, i **"black hat"** sono gli hacker che utilizzano le loro **conoscenze** informatiche per **violare** i sistemi informatici e **causare danni**. Questi individui possono cercare di accedere a informazioni sensibili o di **danneggiare** sistemi informatici per motivi **personali** o **finanziari**. I "black hat" possono causare gravi danni alle imprese e alle organizzazioni, violando i loro dati sensibili e compromettendo la loro reputazione.

Come raccontato in un articolo di **Guerre di Rete**, progetto editoriale italiano indirizzato alla **divulgazione** dei temi dell'**informatica** e della **Cyber-security** (2023) riguardante la nascita di questa pratica divenuto movimento culturale genericamente inserito negli anni '**50** e '**60** del 900, si racconta come originariamente **l'hacking** nasca negli Stati Uniti come **pratica** di **ricerca** al Massachusetts Institute of Technology attuata dai primi e pochi esperti del settore informatico per scopi **accademici**, o come attività di libera **sperimentazione** e **attivismo** civile di appassionati, con l'intento di far emergere falle di sicurezza nei sistemi di aziende o organizzazioni pubbliche e di **sensibilizzare** l'opinione pubblica sulle questioni legate alla **privacy**, la libertà di parola e la **giustizia sociale** in generale. L'attività di hacking condotta per scopi accademici e attività di sperimentazione libera o attivismo civile, si può ricondurre ai cosiddetti **phone phreak**[2], definiti dal professor Mazzini come *<<i progenitori degli hacker>>* e sviluppatisi all'incirca nello stesso periodo ma in luoghi differenti (Mazzini, 2023).

Fra gli esperti che ebbero un impatto significativo sulla storia della Cyber-security è importante menzionare per esempio **Whitfield Diffie** e **Martin Hellman** per le innovazioni nel campo della **crittografia**[3], **Kevin Mitnick** per esser stato fra i primi hacker ad aver raggiunto una notorietà mondiale anche grazie alle sue abilità di ingegneria sociale e per ultimo ma non meno importante, **Aaron Swartz** per il suo impegno come attivista che ha tracciato un prima e un dopo riguardo la libertà d'informazione e l'anonimato online.

Whitfield Diffie e Martin Hellman

Crittoanalisti e **matematici statunitensi**, sono celebri per aver introdotto il primo algoritmo di crittografia a chiave pubblica. Questa innovazione ha notevolmente rafforzato la sicurezza dei dati scambiati attraverso reti informatiche che non richiede la condivisione della stessa chiave segreta tra le parti coinvolte nella comunicazione. Il loro lavoro pionieristico è stato presentato per la prima volta nell'articolo del 1976 intitolato New Directions in Cryptography (Wired, 2023).

Kevin Mitnick

Noto per le sue grandi abilità nel lanciare attacchi informatici, ha dimostrato il suo talento anche come hacker "white hat" divenendo riconosciuto a livello **internazionale** successivamente all'arresto nonostante i trascorsi illeciti. Ha collaborato con svariate aziende per migliorare il loro livello di sicurezza e ha provveduto alla pubblicazione di diversi libri in tema, contribuendo alla divulgazione della Cyber-security da un punto di vista più ampio rispetto a quello accademico (Wired, 2023).

3. Crittografia:
si riferisce a metodi e tecnologie per la protezione dei dati mediante una loro conversione da un formato leggibile ad uno incomprensibile (detto cifrato o criptato) e viceversa, possibile solo per chi è in possesso dell'autorizzazione all'accesso ed alla lettura delle informazioni.

Aaron Swartz

Uno dei personaggi più importanti, amati e noti del settore (**Figura 1.0**). Oltre ad aver contribuito allo sviluppo di diverse tecnologie, tra cui il formato **RSS** per i feed di notizie e la piattaforma di condivisione di file **SecureDrop**, Swartz è principalmente noto per essere stato anche uno degli attivisti più rilevanti per la libertà d'informazione e la libera diffusione della conoscenza. La sua morte prematura nel 2013 a soli 26 anni di età ha portato alla luce importanti questioni **etiche** riguardo **l'accesso** alla **conoscenza** e la **protezione dei dati** (Guerre di rete, 2023).

Figura 1.0 – Aaron Swartz, protesta contro lo "Stop Online Piracy Act" (2012).

Oggi giorno, la **Cyber-security evolve** in primis per rispondere all'**esigenza** di **tutelare** la nostra vita digitale, in senso lato. Che si tratti dell'identità, dell'immagine pubblica, del nostro conto corrente, del diritto alla privacy o addirittura della nostra incolumità fisica, la **Cyber-security** trova nell'**innovazione tecnologica** e **metodologica** le sue principali armi. Tuttavia, stando all'attuale situazione, risulta che nonostante l'avanzato stato delle tecnologie disponibili e impiegate, esistono ancora importanti **lacune culturali** e applicative che vanificano gli sforzi e i mezzi adoperati. Cittadini, strutture pubbliche e aziende spesso sono **molto distanti** è **disinteressati** o semplicemente non sufficientemente informati sull'argomento.

Man mano che il progresso fa il suo corso le **sfide** della **Cyber-security** non si fossilizzano alle sole discipline ingegneristiche ma bensì si **diramano** nei campi più disparati che vanno per esempio dall'**etica** all'**economia** fino alla **politica**, ponendosi la domanda di quali saranno le future implicazioni sociali dei sistemi che ci circondano.

Generalmente, in letteratura emerge con forza l'importanza di **promuovere comportamenti etici** e **responsabili** nella **comunità** informatica, al fine di proteggere la sicurezza dei sistemi informatici e dei dati sensibili e in ultima analisi cittadini, aziende, istituzioni.

Gli hacker sono parte integrante della comunità informatica, poiché svolgono un ruolo fondamentale nella protezione dei sistemi e dei dati sensibili. Comprendere il ruolo di queste figure nella società informatica è essenziale per garantire una maggiore sicurezza online.

1.2

Le dimensioni del fenomeno

L'**Agenzia dell'Unione Europea per la Cyber-sicurezza** (ENISA) è un'organizzazione nata nel **2004** con sede ad **Atene**, che si occupa specificatamente di sicurezza informatica nei limiti dei confini Europei. Operativamente parlando, l'ENISA opera nella **certificazione** e **valutazione** di prodotti e sistemi **digitali** interni al mercato europeo, supportando le istituzioni governative per lo sviluppo di politiche sensibili ai temi della Cyber-security, con risorse informative e documentazione. L'agenzia **rilascia** periodicamente **report** e **strumenti** per lo studio e il monitoraggio delle dinamiche riguardanti tutto ciò che concerne la sicurezza digitale.

Il più recente rapporto di ENISA sulle minacce informatiche emergenti e le tendenze nella Cyber-sicurezza in Europa (2022), sottolinea come l'attuale situazione in termini di attacchi informatici a istituzioni, imprese, individui risulti sempre più critica.

Gli aspetti concorrenti sono molti, tra i quali la nascita di nuove forme di attacco basate sul **machine learning**[4], la disinformazione potenziata dall'intelligenza artificiale (**Deepfake**[5]), l'impiego di nuove vulnerabilità **zero-day**[6] e il crescente numero di casi di **Hacking as a service**[7].

Oltre a questi aspetti, lo scenario è ulteriormente complicato dal **conflitto russo-ucraino** scoppiato nel **2022** e in particolare dagli svariati attacchi perpetrati dalle forze informatiche russe contro infrastrutture ucraine (Wired, 2023). Questi eventi offrono una dimostrazione delle particolari abilità nell'utilizzo di strumenti sofisticati per compromettere sistemi e reti digitali, anche in una strategia di guerra, come vere e proprie armi cibernetiche. Tali attacchi possono causare ripercussioni di vasta portata, sebbene l'attenzione mediatica sia concentrata soprattutto sui danni causati dalle armi tradizionali.

4. Machine learning:
Branca dell'intelligenza artificiale che si occupa dello sviluppo e dello studio di sistemi autonomi, in grado di apprendere e migliorare attraverso i dati che elaborano (Oracle, "Cos'è il machine learning?").

5. Deepfake:
Tecnologia che sfrutta gli algoritmi per l'emulazione del volto di uno specifico utente, successivamente sovrapponibile al volto di un altro individuo all'interno di immagini o contenuti video.

6. Zero-day:
Bug, errori informatici o falle nei sistemi ancora sconosciuti.

7. Hacking as a service:
Letteralmente "hacking come servizio", diversi gruppi fra i più noti e capaci mettono a disposizione le proprie competenze di attacco per un tornaconto economico.

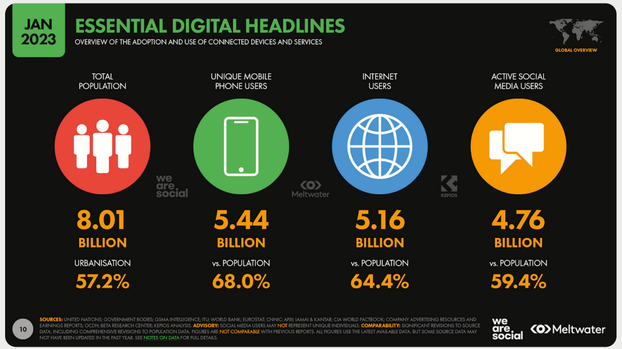
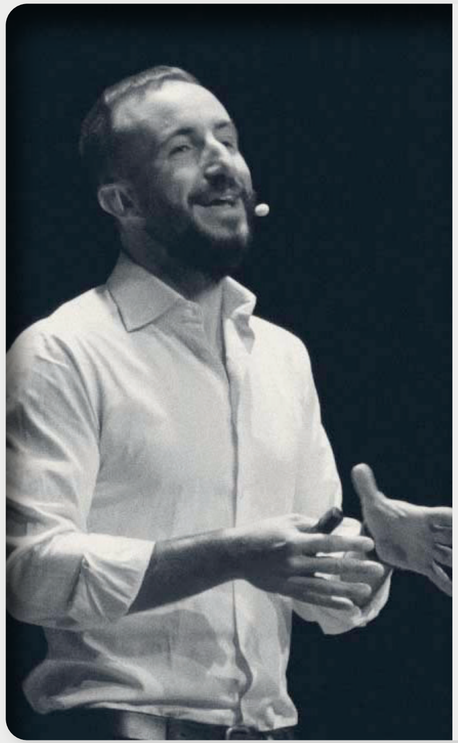


Figura 1.1 – Diffusione di internet a livello globale (Fonte: DIGITAL 2023, pp.10)

Le dinamiche **politiche** ed **economiche** sono **complementari** a quelle del settore **tecnologico**, sempre in continua evoluzione, accelerato da una massiccia e globale diffusione di dispositivi e servizi digitali.

Come dimostra il report Digital 2023 dell'agenzia **We Are Social**, anche quest'anno viene segnalato un **aumento** degli utenti attivi su internet (Figura 1.1).



<<Per una volta, possiamo dire che sono le economie più avanzate tecnologicamente che sono più a rischio>>.

Filippo Lubrano, TEDxVerbania, 5 Gennaio 2022

Figura 1.2 – Speech di Filippo Lubrano, *Storia della Cybersecurity: dalla guerra fredda ai ransomware.*

L'aumento dei **rischi** trova una sua correlazione **proporzionalmente** all'aumento dei **dispositivi** con cui un utente si interfaccia o che comunque impiega quotidianamente, dove oltre ai dispositivi ed ai servizi legati alla sfera lavorativa si vanno ad integrare l'intrattenimento, la gestione delle finanze, l'identità digitale, e molto altro, portandolo potenzialmente ad una maggiore esposizione su più fronti rispetto ad una condizione di scarsa digitalizzazione.

L'esperienza quotidiana dimostra la **pervasività** delle **tecnologie**, che sono utilizzate sempre più spesso in modo ibrido, senza distinzioni tra sfera privata e professionale o tra offline e online.

Questi aspetti sono diventati parte integrante dell'esperienza umana in un contesto di continuità e sinergia, che Luciano Floridi, filosofo ed esperto di etica dell'informazione (una nuova disciplina filosofica applicata alla tecnologia dell'informazione), definisce "onlife" (Floridi, 2014).

La **digitalizzazione** è diventata **strutturale** in moltissimi ambiti di **vita** e **lavoro** (es. domotica, e-banking, smart-health, Dad), sono però al contempo anche terreno di attività di soggetti, gruppi e organizzazioni malevoli, che attraverso attacchi informatici di vario tipo e portata minano la sicurezza di dati, sistemi, servizi e quindi la sicurezza di individui, imprese e istituzioni per scopi economici e/o politici. Soggetti e gruppi di hacker specializzati alterano la propria identità (a questo si aggiungono eventi meno visibili e conosciuti come il rebranding finalizzato all'elusione della legge), per sferrare attacchi informatici.

1.2.1 Minacce

Per loro natura, i **rischi** del web possono apparire come **lontani** o **intangibili**, senza ripercussioni evidenti sulla **vita quotidiana**, prima però di procedere con l'approfondimento specifico sulle minacce nell'ambito della Cybersecurity, è essenziale stabilire una chiara comprensione dei concetti di rischio e danno come descritti nella norma **IEC 120:2023**.

✧ Il Danno (Harm):

si definisce **danno l'insieme** delle **conseguenze** di un incidente, che nell'ambito di riferimento possono riguardare **informazioni** e **beni** o **l'ambiente** (IEC 120:2023, 3.8). Le **conseguenze** possono avere anche un **diretto effetto** sulle persone in termini di **sicurezza** e **benessere**. Queste conseguenze possono variare ampiamente a seconda dell'evento: possono ad esempio includere perdita di dati sensibili, violazione della privacy, interruzione dei servizi, danni finanziari e danni alla reputazione dell'organizzazione, oltre che alla compromissione fisica di persone o cose.

✧ Il Rischio (Risk):

risulta dalla **probabilità** che un certo **rischio** si verifichi e dalle **gravità** dei **danni** che potrebbero derivarne. Il rischio include una serie di variabili, come la probabilità di un attacco, le vulnerabilità nei sistemi e le possibili conseguenze per l'organizzazione, i dati e i servizi (IEC 120:2023, 3.11).

Con minacce informatiche si intendono le diverse azioni perpetrate da agenti che definiremo Attaccanti, e finalizzate al danneggiamento, al furto o alla manomissione di dati e/o sistemi per colpire individui, organizzazioni, istituzioni. Le minacce informatiche vengono attuate attraverso diversi Vettori di attacco, ossia tecniche e strumenti con i quali i target (persone, organizzazioni) vengono identificati e colpiti.

Si distinguono diverse tipologie di vettori, i quali possono suggerire anche ipotesi sugli intenti e le possibilità di azione degli Attaccanti. Nella grande varietà di vettori, i principali indicati da ENISA (2022) per incidenza e quantità di casistica sono i seguenti.

✧ *Ingegneria sociale* ✧

Con ingegneria sociale si intendono una serie di attività che sfruttano la manipolazione psicologica, comportamenti abitudinari ed errori umani per generare possibilità di accesso a informazioni o servizi protetti da password e sistemi di sicurezza.

In questa categoria rientrano tecniche come il Phishing, con cui si ingannano gli utenti target con mail, sms e messaggi fasulli, inviati da falsi indirizzi. I messaggi contengono un link malevolo, che porta a pagine web fraudolente, imitano a volte perfettamente servizi digitali reali. I messaggi sono costruiti per cercare di indurre le persone ad aprire il link malevolo e usare le proprie credenziali o estremi di carte di credito sul sito fasullo, da cui vengono letteralmente rubati.

Una variante di questa tecnica è detta "man in the middle", dove il criminale si introduce segretamente in una conversazione fra due interlocutori cercando di ingannare una o entrambe le parti modificando i messaggi ricevuti e inviati.

Una costante alla base di questa particolare tecnica è che non si tratta di attacchi che mirano alla manomissione dei sistemi di sicurezza, ma al furto di dati di accesso, credenziali, estremi bancari attraverso l'impiego di meccanismi di persuasione.

Per "dati sensibili" si intendono informazioni che hanno un grado di rilevanza nettamente superiore rispetto a quelle di pubblico dominio. Questi dati garantiscono spesso l'accesso a servizi, beni ed ulteriori informazioni possedute da uno specifico utente o organizzazione. Tra i dati sensibili ci sono ad esempio le credenziali di accesso agli indirizzi di posta elettronica, i numeri di telefono, i PIN o le password per ogni sorta di servizio, e molto altro ancora. Tuttavia, i dati sensibili non si limitano a informazioni di tipo utilitaristico come i codici di accesso, ma possono includere anche conoscenze relative alla nostra sfera privata. Proprio per questa loro natura, in grado di alterare o comunque influenzare con grande incidenza le nostre vite, questi dati sono oggetto di interesse da parte sia dei Cyber-criminali che di chi ha come obiettivo la tutela del nostro diritto alla privacy e alla sicurezza.

Malware ✧

Con questo termine si indica un codice malevolo. Può trattarsi di poche righe di programma, interi software o apparecchiature elettroniche, che vengono inseriti volontariamente in un dispositivo o in un sistema, con l'intento di danneggiarlo o alterarne il normale funzionamento.

Ransomware ✧

I ransomware sono una specifica tipologia di malware che una volta infiltrati nei sistemi, limitano le possibilità di utilizzo da parte degli utilizzatori. La maggior parte delle volte, questi attacchi vengono sferrati per estorcere denaro. Il pagamento del riscatto (il ransom, appunto) può bastare per riavere il controllo del dispositivo violato, ma non è sempre garantito. Si parla di "Cryptor" per indicare i software in grado di rendere i file contenuti nel dispositivo attaccato inaccessibili o inutilizzabili, appunto criptandoli, i "Blocker" invece impediscono agli utenti l'accesso all'intero dispositivo attaccato.

Minacce ai Dati ✧

In questa categoria rientrano vettori conosciuti come "data leak" o il "data breach", attacchi con cui vengono acquisiti e diffusi o venduti dati privati, sensibili o protetti da segreto industriale, professionale. I data leak sono eventi di natura involontaria, dovuti a errori umani, di codice o vulnerabilità di sistema. I data breach sono invece volontarie compromissioni da parte di Cyber-criminali, finalizzate alla diffusione di materiale sensibile per scopi prevalentemente ideologici, economici.

Attacchi DDOS ✧

Gli attacchi Distributed Denial of Service (DDoS) comportano l'impossibilità da parte degli utenti di accedere a uno specifico servizio digitale per via dell''insostenibile quantità di accessi effettuati attraverso specifici software in grado di stressare i server di una piattaforma.

Minacce a Internet

In questa categoria rientrano tutte le iniziative dedite a interrompere o compromettere il regolare funzionamento della connessione alla rete di uno specifico utente limitando o annullando completamente la sua capacità di usufruirne.

Una delle tecniche per raggiungere questo bioetico è l''IP hijacking" o dirottamento di indirizzo IP, che consiste nella compromissione della navigazione per via di una errata comunicazione fra i sistemi dell'utente e la rete.

L'interruzione può accadere in circostanze involontarie ma può essere provocata anche intenzionalmente con le giuste capacità.

Disinformazione

ENISA identifica nelle fake news e nell'omissione parziale o totale delle informazioni una minaccia per l'intero web, divenuto nel tempo una fonte da cui milioni di utenti attingono per mantenersi aggiornati riguardo a notizie da tutto il mondo.

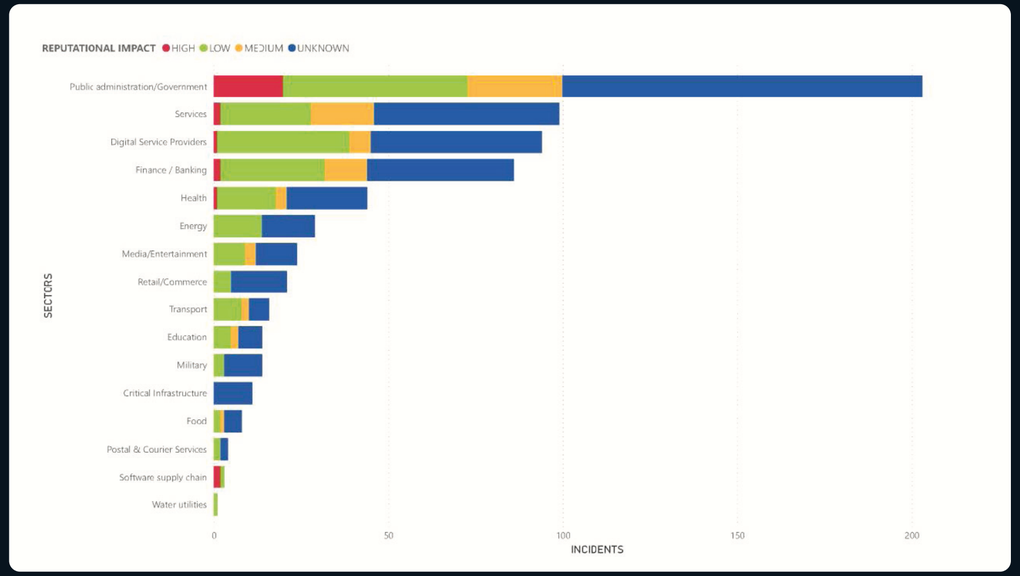


Figura 1.3 – Grafico relativo ai danni "reputazionali" provocati dagli attacchi per settore nel periodo Luglio 2021-Giugno 2022 (Fonte: ENISA 2022, p.15)

1.2.2 Danni

A fronte di un attacco possono essere svariati i danni perpetrati.

Nell'intento di riassumere i danni provocati complessivamente, dagli attacchi informatici, **ENISA** utilizza una serie di **parametri chiave** che permettono di **identificare danni** di diverso tipo, illustrati nel seguito.

Danni reputazionali

In questa categoria si Includono **danni** relativi **all'immagine**, sono potenzialmente impattanti sui soggetti colpiti siano che si tratti di individui, gruppi o organizzazioni. Questo tipo di danni è collegato anche con **conseguenze** più **difficili** da **quantificare** quali perdita di stima, fiducia o credibilità.

Nel grafico in Figura 1.3 sono elencati e stimati complessivamente i danni reputazionali sofferti da organizzazioni di vari settori nel 2022. Il grafico mostra come il danno reputazionale risulti più impattante e gravoso per le organizzazioni pubbliche.

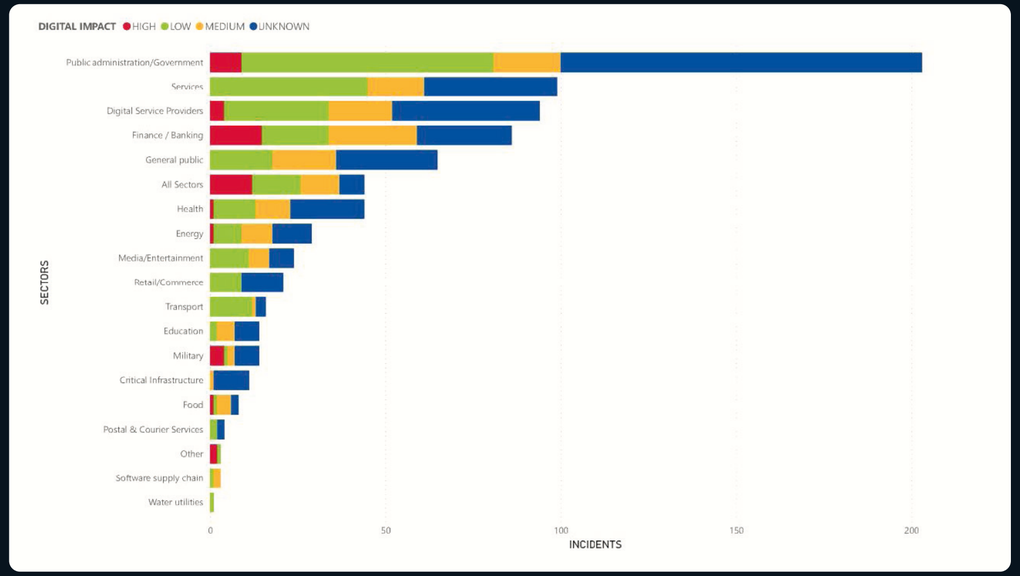


Figura 1.4 – Grafico relativo ai danni "digitali" provocati dagli attacchi per settore, periodo Luglio 2021-Giugno 2022 (Fonte: ENISA 2022, p.16)

Danni digitali

Includono danneggiamento, corruzione ed espropriazione di dati, sistemi informatici.

L'entità di questi danni viene identificato come medio-basso nella maggior parte dei settori campionati, ad eccezione per l'amministrazione pubblica, per le finanze e per i fornitori di servizi digitali, dove sono stati registrati incidenti con impatti elevati, causati per lo più da attacchi ransomware (Figura 1.4).

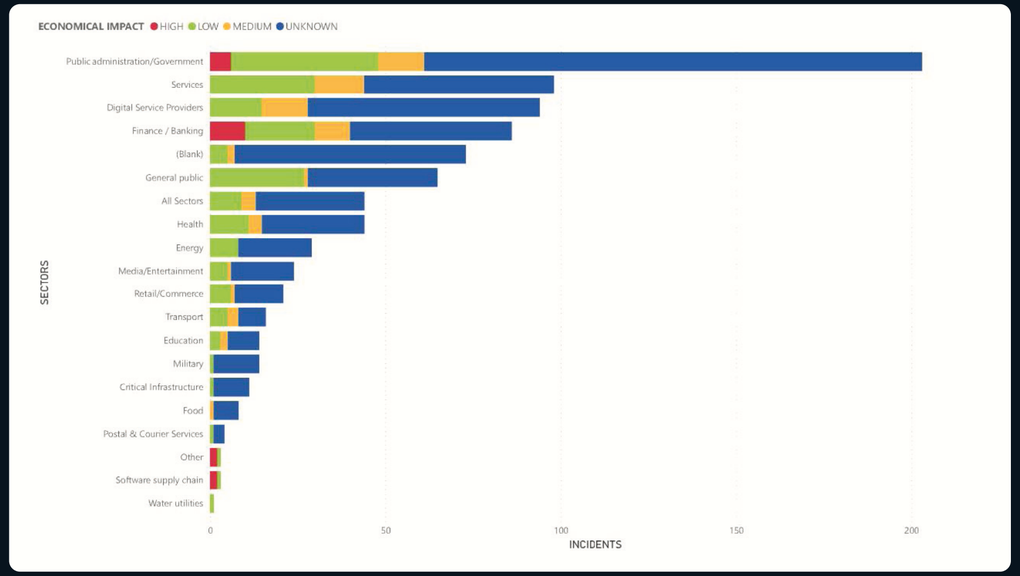


Figura 1.5 - Grafico relativo ai danni "economici" provocati dagli attacchi per settore, periodo Luglio 2021-Giugno 2022 (Fonte: ENISA 2022, p.16).

Danni economici

Sono relativi alla **perdita** diretta di **capitali** ai danni del **target** di attacco o di terzi associati.

Come mostra la Figura 1.5, si è osservato che i settori dell'amministrazione pubblica e delle finanze hanno subito alcuni degli impatti più elevati, in conseguenza delle molte violazioni di dati personali e furti di dati o di dettagli bancari.

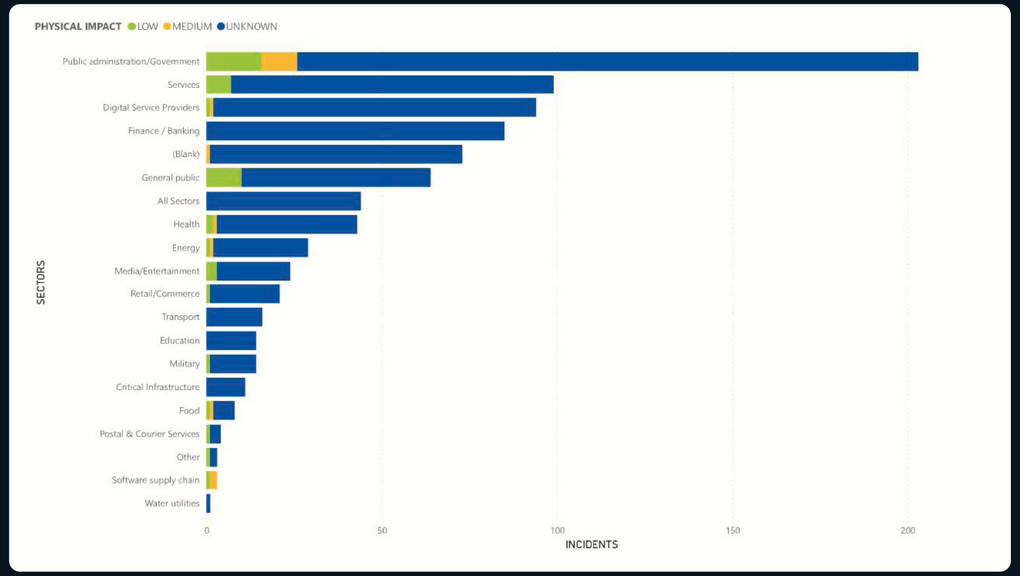


Figura 1.6 – Grafico relativo ai danni "fisici" provocati dagli attacchi per settore, periodo Luglio 2021-Giugno 2022 (Fonte: ENISA 2022, p.17).

Danni fisici

Si riferiscono al **danneggiamento** diretto di **persone** e/o **strutture** e **infrastrutture**.

Come mostra la Figura 1.6, questo genere di danni resta la tipologia più sconosciuta, a causa della mancanza di informazioni affidabili disponibili e pubblicate in proposito.

Questa mancanza di dati certi potrebbe essere presumibilmente riconducibile alla ancor più scarsa propensione delle vittime a condividere informazioni, per paura di ripercussioni relative alla propria (o altrui) salute e sicurezza.

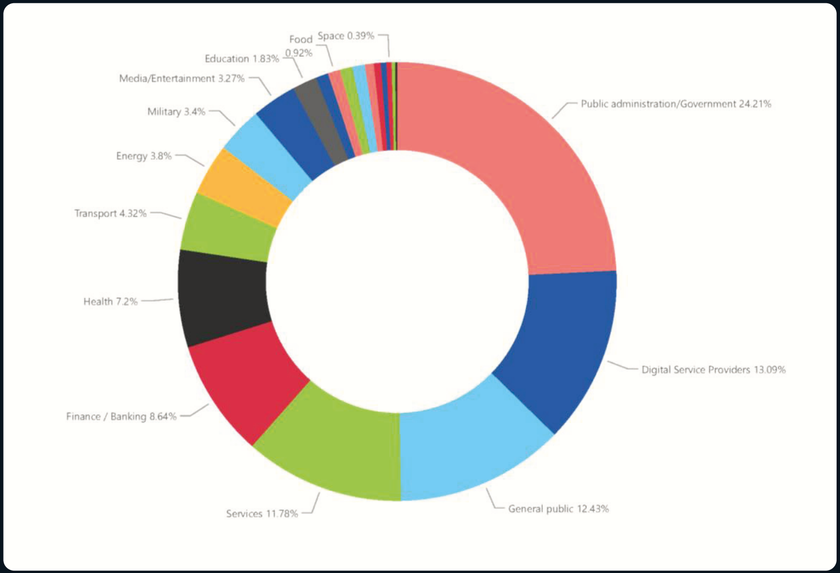


Figura 1.7 - Distribuzione degli attacchi per settore nel periodo di Luglio 2021-Giugno 2022 (Fonte: ENISA 2022, p.14)

Distribuzione attacchi per settore

Lo scenario si delinea più chiaramente consultando i dati aggregati per settore. Secondo ENISA (2022), i soggetti maggiormente colpiti in Europa dalle diverse tipologie di attacco prima citate sono la Pubblica amministrazione (24,21%), provider di servizi digitali (13,09%), il pubblico generale (12,43%) i l settore servizi (11,78%), il settore finanziario e banche (8,64%), la sanità (7,2%).

In percentuale minore sono interessati i settori di trasporti, energia, militare, intrattenimento e media, educazione, alimentare e spazio (Figura 1.7).

Tra questi dati, il numero di attacchi rivolti a privati cittadini, non identificati per un settore specifico (Pubblico generale) risulta inaspettatamente più colpito rispetto ai settori finanziario e sanitario, che ci si aspetterebbe essere considerati più redditizi per i gruppi di Cyber-criminali.

E' importante evidenziare che i report che monitorano regolarmente il settore soffrono e denunciano evidenziano anche la difficoltà di raccogliere dati e quindi le **lacune** dei **dati disponibili sui danni**, la **gravità** e **l'impatto**. Questo fenomeno fa luce sulla **difficoltà** di **raccogliere** e **aggiornare dati** relativi agli attacchi informatici subiti, per la maggior parte delle volte non denunciati dai soggetti colpiti. Tra le cause, si possono presumere la scarsa consapevolezza delle modalità di prevenzione e risposta, delle azioni da compiere in caso di pericolo e di attacco, la scarsa conoscenza di **best practice** e fonti di informazione da cui recuperarle, insieme alla frequente e volontaria omissione dovuta al timore di ripercussioni economiche e legali.

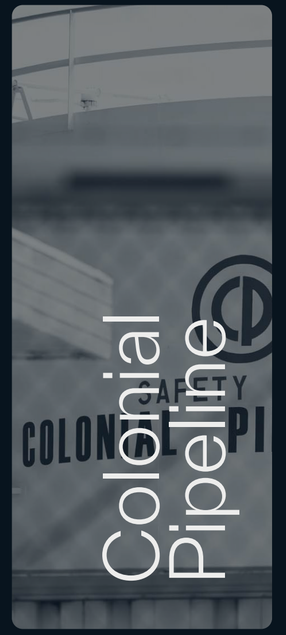
A questo punto, lo scenario generale suggerisce alcune domande: la consapevolezza degli utenti in relazione alle minacce coincide con la reale situazione riportata da ENISA? Quali soluzioni possono informare in modo più efficace, personalizzato e tempestivo un pubblico generalista e ovviamente poco interessato alla tematica? ed infine, come si può rendere l'individuo più fragile una componente di successo nella sicurezza?

1.3

Casi studio

Sono diversi gli **incidenti** che, salendo agli onori della cronaca, riescono a fornire un'idea sulle varie tipologie di attacco e conseguenze verificabili. Per comprendere meglio il tema sono stati dunque selezionati e analizzati tre importanti avvenimenti accaduti nel **2021** riferiti a diversi tipi di attacchi e danni provocati: l'incendio occorso presso il data center della multinazionale **OVH**, l'attacco ad un'azienda del settore petrolifero **Colonial Pipeline** e l'attacco ransomware subito **Ferrovie dello Stato**.

Questi casi studio esemplificativi permettono di comprendere come si svolgono gli attacchi a cui sono esposti i sistemi di grandi compagnie, organi statali e molti altri, aiutando a scorgere i diversi possibili interventi che avrebbero potuto prevenire o mitigare i danni.



L’Incendio del datacenter OVH

Figura 1.8 – Aaron Swartz, protesta contro lo “Stop Online Piracy Act” (2012).

OVHcloud è una **multinazionale francese** di grande rilievo nel settore del **web hosting** che offre ai suoi clienti uno spazio dove poter mantenere o creare il proprio **dominio**[8], sito web o database, questa grande mole di dati viene **conservata** all’interno degli appositi **server** posseduti da **OVH** e situati in diverse nazioni come Francia, Stati Uniti, Germania e altri. Nel marzo del 2021 alle ore 00:47, uno dei data center di sua proprietà chiamato **Sbg2** e situato a **Strasburgo** è stato colpito da un **incendio** che ha distrutto gran parte dell’infrastruttura.

L’incendio sarebbe stato causato da un problema elettrico, ma successivamente si è scoperto trattarsi di un attacco hacker di tipo **DDoS** (Distributed Denial of Service) che aveva lo scopo di distruggere i dati custoditi dall’azienda.

Secondo alcune ricostruzioni (DCD, 2021; The Register, 2021;), l’incendio ha distrutto **quattro** dei **dodici** sistemi presenti nell’infrastruttura (Figura 1.8). I data center di OVH non sarebbero stati pronti ad affrontare l’emergenza incendio in ogni caso in quanto non dotati di estintori automatizzati e di interruttori automatici di sicurezza elettrica, ad aggravare ulteriormente la situazione hanno concorso fattori come la difficoltà di accesso al quadro elettrico generale, il soffitto in legno di Sbg2 e le connessioni tra i sistemi di condizionamento che hanno favorito la propagazione delle fiamme. Per questa serie di ragioni l’incendio non è stato prontamente soppresso ed è stato molto difficile mitigare i danni dimostrando anche come un buon sistema di comunicazione interna avrebbe con molta probabilità facilitato la mitigazione del danno causato grazie ad un intervento più tempestivo. Le analisi successive rivelano che buona parte dei clienti non avessero attivato prontamente dei backup di sicurezza dei loro dati o addirittura in alcuni casi questi ultimi furono immagazzinati all’interno degli stessi server oggetto dell’incendio, conseguendo nella chiusura definitiva dei data center Sbg1 e Sbg4.

In conclusione, **una parte** dei servizi attivi è stata **riallocata** in strutture differenti sempre appartenenti a **OVH** e la stessa azienda ha deciso di **automatizzare** da lì in poi la procedura di **backup** per ogni cliente, presentando il report di analisi dei danni ufficiale successivamente a giugno 2022 Investigation report located in Strasbourg (67) on March 10, 2021. On the fire in the OVH data. Si stimano dunque danni per un ammontare di diversi milioni di Euro (circa 105), in parte solamente correlati al valore dell’immobile perso nell’incidente.

8. Dominio:
Indirizzo univoco per il riconoscimento di uno specifico sito web composto principalmente da due parti quali il nome del dominio (scelto dall’acquirente) come “google” e la sua estensione che può essere per esempio “.com”, “.net”, “.org”, generando insieme appunto “google.com”.

L’attacco ransomware a Colonial Pipeline

Il **6 maggio 2021** un attacco informatico ha preso di mira l’azienda statunitense **Colonial Pipeline**, che **gestisce** un importante **oleodotto** situato negli **Stati Uniti**. Obiettivo dell’attacco era quello di **bloccare l’operatività dell’oleodotto**. L’arresto è **durato** per **6 giorni**, necessari al completo ripristino dei sistemi, costringendo l’azienda a interrompere temporaneamente le operazioni di trasporto di carburante. Secondo un articolo del New York Times (2021), **l’attacco** è stato condotto dal gruppo hacker noto come **DarkSide**, che ha richiesto un riscatto di 4,4 milioni di dollari in bitcoin per il rilascio delle chiavi dei dati da loro resi inaccessibili.

L’attacco ha avuto un **impatto** significativo **sull’economia** e la società americana, causando un **aumento** dei prezzi del **carburante** e suscitando **preoccupazione** per la sicurezza degli **approvvigionamenti energetici** come afferma Repubblica (2021) in un articolo dedicato.

Stando alle informazioni rilasciate relative alle dinamiche di attacco si evince che la causa sia riconducibile a un vettore di tipo **Ransomware** rivolto ai **sistemi** di distribuzione e di **fatturazione** che ha imposto successivamente un blocco in via precauzionale di molti altri sistemi di gestione non coinvolti. Si presume che inizialmente una e-mail con **allegato** o **link malevolo** abbia raggiunto uno fra i dipendenti di **Colonial Pipeline**, che avrà inconsciamente avviato un **download** reputato sicuro o innocuo scambiandolo per un documento di lavoro, rendendo il dispositivo dal quale operava “infetto”, a questo punto l'organizzazione criminale (Darkside) è entrata in possesso di un punto di **accesso**[9] ai sistemi aziendali, che permette la manomissione della rete aziendale garantendone dunque il controllo, in questo caso **bloccando** tutti i possibili **utenti** al di fuori degli attaccanti. In questa fase il gruppo hacker avanza la richiesta di un riscatto fornendo le istruzioni a schermo tramite il display del dispositivo infettato precedentemente, da notare come la richiesta di denaro sotto forma di **Bitcoin** non sia casuale poiché l’impiego della **criptovaluta** garantisce il totale anonimato del ricevente.

In conclusione, per quasi una settimana, Colonial Pipeline è stata messa in ginocchio da una serie di fattori come la concomitanza di sistemi off-line, file aziendali criptati e server cifrati, mostrando anche come il gruppo abbia puntato sull’isolamento e sul distanziamento dei singoli reparti aziendali impedendo fra loro la comunicazione per rallentare e ostacolare la ripresa.

9. Punto di accesso:
il mezzo che permette ad un utente di potersi intromettere in un sistema altrui via wireless, che può essere come in questo caso di attacco un dispositivo infettato da un virus, un account la cui password è già nota al Cyber criminale, una connessione wi-fi aperta o il bug in un software.

L’attacco ransomware a Ferrovie dello stato

Le Ferrovie dello Stato Italiane, nel marzo 2022, hanno visto il gruppo Cyber-criminale **Hive attaccare** il sistema informatico di **Trenitalia**, la principale compagnia ferroviaria nazionale.

Secondo Wired (2022), **l’attacco**, con il quale sono stati crittografati i dati sensibili di Trenitalia, era **finalizzato** alla richiesta di un **riscatto** per renderli nuovamente accessibili, il caso presenta **similarità** con quello di **Colonial Pipeline** precedentemente discusso per quanto riguarda la tipologia del vettore di attacco (Ransomware), con l’aggravante però di una **pessima gestione** della **crisi** da parte dell’azienda, data la **scarsa preparazione** del personale e la **negligenza** di un **singolo dipendente** che ha contribuito alla diffusione attraverso l’app **Telegram**[10] di informazioni sensibili fornite dai criminali, di fatto una fase critica di questo tipo di attacchi è proprio quella del contatto diretto tra l’azienda ed il gruppo criminale che avendo necessità di fornire le istruzioni per il pagamento instaura un canale.

L’errore ha permesso l’accesso alla chat da parte di una grande quantità di **utenti non autorizzati** da Ferrovie dello Stato, finendo per provocare un rincaro del riscatto da **5** fino a **10 milioni** di euro per la restituzione del controllo dei sistemi.
Vanno considerati inoltre, i rischi legati ai dati personali dei viaggiatori (anagrafiche e dati relativi ai pagamenti) che sono stati trafugati e messi in serio pericolo, Trenitalia anche in questo caso non ha saputo reagire prontamente con una comunicazione rivolta ai suoi clienti in grado di informarli dell’accaduto e di come i loro dati sensibili vengano conservati all’interno della rete aziendale.

10. Telegram:
App di messaggistica per smartphone nota per avere una funzione simile a quella di Whatsapp ma con un maggiore livello di profondità, dato dalla presenza di “canali” o “gruppi” ospitanti anche decine di migliaia di utenti e con un particolare focus sul mantenimento dell’anonimato.

1.4

Contromisure

In questa sezione, saranno approfondite le best practice formulate per essere applicate in modo efficace al fine di proteggere persone, organizzazioni, dispositivi, dati e in ultima analisi servizi e processi dalle molteplici minacce della rete con un particolare focus su contesti di carattere aziendale.

Per agevolare la comprensione dei contenuti queste pratiche verranno suddivise in “Famiglie di azioni” che possono essere di natura organizzativa oppure tecnologica, distinte in “Controlli minimi” più immediati e semplici, e “Controlli avanzati”, ovvero misure più articolate o che possono prevedere un background tecnologico più specialistico.

Per cominciare definiamo “Best practice” un comportamento, un processo o una singola azione che si è dimostrata essere particolarmente valida nell’ottenimento di un risultato specifico, nel nostro caso dunque il nostro risultato atteso sarà la tutela degli utenti, dei dati e dei mezzi digitali, una navigazione sicura o la limitazione dei danni in un possibile attacco e molto altro.
Gli strumenti sia tecnologici che organizzativi riportati vengono argomentati e affrontati attraverso la commistione di conoscenze personali in concomitanza di una verifica di varie fonti online autorevoli e riconosciute come le documentazioni di ENISA, Kaspersky, HP ed altri enti anche governativi di stampo estero come il National Institute of Standard and Technology.

1.4.1 Controlli minimi

Seguendo le opportune accortezze ognuno di noi può essere in grado di usufruire della rete in modo sicuro, a prescindere dai software di protezione sono i nostri micro comportamenti e le nostre abitudini a determinare una buona **igiene informatica**[11] nel medio lungo periodo.

Misure organizzative

Quando parliamo di misure organizzative ci riferiamo alle linee guida messe in atto per garantire con continuità il regolare svolgimento delle attività in rete. Queste misure sono tipicamente messe in essere dalle organizzazioni che nello strutturare processi e sistemi per la sicurezza informativa. Tipici di queste misure sono documenti che stabiliscono i rischi potenziali e un piano per il trattamento dei rischi specifici. In queste iniziative è inclusa anche tutto il corpus di informazioni e azioni da fornire al personale sul corretto utilizzo di software e dispositivi presenti negli ambienti di lavoro.

11. Igiene informatica:
in questo concetto si racchiudono la corretta mentalità e il giusto comportamento adottabile da un utente o gruppo di utenti per un sicuro impiego della rete e dei dispositivi digitali, comprendendo tutte le best-practices e misure tecnologiche in grado di definire un sistema (composto da utenti e dispositivi) orientato alla sicurezza in senso lato (Kaspersky Resource Center).

Inventario

Come anticipato, una pratica essenziale è l'inventario di dispositivi e software presenti e utilizzati nel perimetro aziendale. Di fatto monitorare nel tempo lo stato dei sistemi attraverso un catalogo ben organizzato rende più facile agire puntualmente e più efficacemente durante l'incombere di problematiche nonché verificare lo stato generale dell'intera struttura. Questa misura è facilmente attuabile tramite strumenti appositi come fogli di calcolo Excel condivisi sui quali è possibile consultare in tempo reale quali e quanti dispositivi (e relativi software attivi) siano effettivamente messi a disposizione in azienda, permettendo anche di verificare a chi sono stati affidati. L'inventario dei sistemi facilita anche una generale manutenzione degli stessi agevolando l'operato dei profili tecnici che presidiano le infrastrutture e i servizi. Gli inventari degli asset sono anche fondamentali a seguito di un attacco, per risalire al punto di origine di un tentativo di attacco, permettendo anche in questo caso una messa in sicurezza più efficace.

Gestione dei fornitori

in una concezione ampia della Cyber-sicurezza, distribuita lungo una filiera di rapporti e di servizi, le organizzazioni possono definire protocolli e contratti con i fornitori (organizzazioni o utenti terzi o secondari che per erogare un servizio ricevono e trattano dati sensibili) che prevedano clausole e protocolli di sicurezza, anche a tutela della privacy per organizzazioni, dipendenti e clienti coinvolti. Queste misure permettono di ottimizzare la prevenzione ed eventualmente di limitare la propagazione di eventuali vettori d'attacco.

Gestione degli incidenti

La definizione e l'attuazione di procedure predefinite, concordate e validate dall'organizzazione è lo strumento principe della protezione della sicurezza informatica. il protocollo di gestione degli incidenti include la prevenzione e specifica la catena di comando e azione da seguire durante l'incidente e dopo: una volta scongiurata la criticità, l'organizzazione colpita avrà la responsabilità di informare personalmente gli utenti i cui dati siano stati manipolati, sottratti o cancellati durante l'attacco, con apposite comunicazioni multi-target (comunicati stampa, social media, o tramite altri eventuali mezzi) che descrivano gli avvenimenti, le conseguenze e le possibili azioni di recovery.

Un Piano di Gestione degli incidenti include anche tutte le azioni volte a garantire la Continuità operativa. Il concetto si riferisce alla capacità di un'organizzazione di non interrompere drasticamente i lavori nonostante eventi imprevisti o catastrofici, come ad esempio un disastro naturale, un'interruzione dell'alimentazione elettrica o un attacco informatico. Il piano di"disaster recovery" (DR) include un insieme di procedure e protocolli chiari e precisi da seguire in caso di emergenza, al fine di ripristinare le attività principali dell'azienda il prima possibile e riprendere con la produzione.

Conformità

questo termine di riferisce all'obiettivo che le organizzazioni si pongono di riuscire ad applicare e preservare nel tempo (se possibile anche migliorare progressivamente) le politiche e norme che un'azienda si autoimpone, essere conformi dunque significa fondamentalmente rispettare e soddisfare tutti i criteri stabiliti nelle fasi di organizzazione e preparazione della sicurezza. Attività di "audit interno periodico", ovvero di controllo effettuato da profili aziendali in modo indipendente e l'obiettivo sia delle singole attività che dei processi svolti dall'organizzazione, permettono di identificare eventuali problemi o aree di miglioramento, ridurre il rischio di frodi o errori e aumentare la trasparenza e "l'assunzione di responsabilità".

L'audit interno viene solitamente effettuato da un team di professionisti che non fanno parte della gestione operativa dell'organizzazione e che hanno competenze specifiche in materia di controllo interno e di gestione dei rischi. Una fattispecie di questa misure è la "verifica dell'operato degli amministratori di sistema" che consiste nel monitoraggio appunto degli utenti a cui vengono garantite maggior potere decisionale e libertà nell'impiego di strumenti e informazioni. L'obiettivo di questi controlli è quello di assicurare che gli amministratori di sistema agiscano in modo etico e professionale, rispettando le politiche e le normative proprio in quanto individui chiave nella loro attuazione e nel mantenimento della sicurezza informatica generale; la prassi può includere la revisione delle attività svolte dagli amministratori di sistema, la verifica della formazione ricevuta e la verifica della presenza di eventuali conflitti di interesse e molto altro.

Consapevolezza e Responsabilità

Far sì che ogni utente sia in possesso di un livello di competenza informatica avanzata all'interno di un'organizzazione è pressoché impossibile oltre che superfluo. Una soluzione consolidata è quella di distribuire i ruoli coinvolgendo individui più esperti in modo da offrire supporto a più aree possibile nella maniera più efficiente. Uno dei ruoli chiave per gestire la sicurezza informatica in azienda è il Chief Information Security Officer o CISO, che ricopre il ruolo di responsabile della sicurezza informatica che predispone e monitora tutti i processi necessari a prevenire e mitigare i rischi potenziali. Il CISO è anche la figura che coordina la valutazione dei rischi e a cui di fatto, si possono rivolgere i colleghi e i collaboratori sia in situazioni di potenziale rischio che nei processi di revisione e controllo. Il referente per la sicurezza si occupa di censire, oltre ai rischi potenziali, gli asset e le risorse che potrebbero essere attaccati e il loro valore, identificando misure specifiche per la protezione. Questa figura può avvalersi - anzi è auspicabile il coinvolgimento - di diverse risorse, dedicate o prestate da altri settori, per poter distribuire la responsabilità relativa alle informazioni sensibili dell'intera organizzazione. Coinvolti o meno in ruoli specifici per la Cyber-security, tutti gli utenti che hanno accesso ai software e ai dispositivi dell'azienda sono potenzialmente predisposti a subire attacchi Per questo è fondamentale l'azione di informazione e formazione e divulgazione dei contenuti elaborati dal CISO, rielaborati in formati che li rendano accessibili e fruibili da tutti i profili, in modo continuativo nel tempo.

In questo senso è fondamentale che lo stesso CISO possa accedere a diverse fonti di informazione in merito alla sicurezza, naturalmente (nuovi software o sistemi, casi di attacco recenti e molto altro), per allinearsi agli standard più attuali e valutare potenziali minacce in grado di coinvolgere anche il nostro contesto di lavoro o la nostra persona. Ma anche per venire a conoscenza delle iniziative e delle innovazioni più efficaci per la promozione delle conoscenze e competenze che possono portare i singoli ad agire in modi più sicuri e integrati con le politiche di sicurezza.

Contromisure personali

Contromisure personali: A prescindere dai sistemi di sicurezza di cui un'organizzazione possa essere provvista, questi sono incompleti e parzialmente efficaci se non accompagnato da azioni di informazione e formazione (o alfabetizzazione) dei propri dipendenti e delle figure esterne con cui si interfacciano in modo da garantire un livello minimo di capacità generalmente diffusa d'uso sicuro dei sistemi digitali. Questo implica non solo sapere come si usa un dispositivo o un servizio, ma quali rischi possono incorrere e quindi quali accorgimenti adottare nell'uso. Tali azioni devono coinvolgere anche le figure apicali e manageriali che possono contribuire a rinforzare le politiche e le pratiche di sicurezza a tutti i livelli.

Sicurezza fisica

Per garantire una continuità operativa è necessario tutelare la struttura aziendale (oltre che digitalmente) anche da un punto di vista prettamente fisico, eseguendo le opportune revisioni periodiche e manutenzioni (spesso indicate dai fornitori dei dispositivi e dei servizi di cui l'impresa fa uso) dei sistemi come server, cablaggi e reti e dei relativi impianti di alimentazione elettrica.

Questa contromisura serve a scongiurare danni (anche potenzialmente letali sia per le persone che per le organizzazioni). Eventi come incendi, cortocircuiti e malfunzionamenti possono essere causati involontariamente o dalle condizioni delle strutture che ospitano i beni aziendali e dal loro stato di usura; nulla vieta però che ingenti danni possano verificarsi anche volontariamente attraverso manomissioni dolose come raccontato nel caso studio "Incendio del datacenter OVH".

Misure tecnologiche

Controllo degli accessi

un valido controllo degli accessi possiede la sua notevole importanza, ad esempio adottando:

- La limitazione degli accessi rendendo disponibili ai dipendenti solo i dati e i sistemi necessari, conferendo il ruolo di amministratore solo a specifici utenti "prioritari" rispetto ad altri.

- La segregazione dei dati, suddividendo (anche fisicamente in hard disk o server separati) differenti tipologie di informazioni come i dati dei clienti e quelli dell'azienda in due distinti database.

- Una modalità di archiviazione su misura creando un sistema di cartelle e strutture di sotto cartelle comprensibili e ordinate sia per il personale che per agevolare ad esempio l'inventario. Una possibile struttura potrebbe essere una prima suddivisione per tipologia di informazione (aziendale, dei fornitori o dei clienti, ecc...), una sub sezione che distingua le cartelle cronologicamente (anno e mese) e successivamente la creazione di ulteriori sottocartelle ordinate per ogni dipendente in ordine alfabetico con relativi backup di sicurezza.

- Stabilire un processo di gestione delle credenziali specifico a partire dalla loro creazione (conducibile secondo criteri standard ISO 27001 5.17), modifica o cancellazione alla loro assegnazione per garantire password efficaci e sicure, ciò è possibile ideando sequenze complesse (Cyber-news, 2023)

- Un'altra possibilità è la gestione delle autorizzazioni e relativo riesame periodico, un processo che fondamentalmente richiede di assicurarsi che le autorizzazioni vengano assegnate in modo corretto, questo anche allo scopo di convalidare periodicamente gli utenti a cui vengono attribuite per prevenire eventuali accessi non autorizzati.

- Il Controllo degli accessi degli amministratori di sistema per verificare regolarmente gli accessi di questi ultimi per garantire che siano coerenti con le loro funzioni, riducendo il rischio di abusi (per esempio un impiego sospetto o eccessivo non previsto delle risorse a loro disposizione).

Gestione dei sistemi IT e dei dispositivi

Computer, smartphone e tablet di un'azienda rappresentano "banchi di lavoro digitali" sui quali avviene lo svolgimento di specifiche mansioni, rappresentando il tramite per tutto il flusso di lavoro. Un approccio inadeguato alla loro gestione può comportare seri rischi per la sicurezza, ad esempio, il "processo di ritiro dei dispositivi e cancellazione delle memorie" richiede il corretto smantellamento dell'hardware e del software, dove gli apparecchi devono essere riportati allo stato originario della memoria attraverso una formattazione del disco e non devono più contenere traccia alcuna di dati sensibili.

La "cifratura dei dispositivi" rappresenta un ulteriore sistema di protezione che impedisce ad attori esterni di accedere ai dati sensibili. Consiste nell'applicare un algoritmo di crittografia ai dati memorizzati sul dispositivo, rendendoli leggibili solo da chi possiede la chiave di decrittazione.

La "gestione dei cambiamenti dei sistemi informatici" invece prevede il continuo aggiornamento e monitoraggio dello stato delle nuove funzionalità, come spesso accade nei sistemi operativi, per minimizzare gli effetti negativi sul funzionamento del sistema e garantire che i cambiamenti vengano implementati in modo coerente. Per concludere, i "software anti-malware" rappresentano una contromisura ottima per proteggere i sistemi informatici (passivamente poiché attivi parallelamente alle nostre attività) da programmi dannosi, come virus, spyware e malware. È altrettanto importante prevedere dei backup periodici, ovvero la creazione di una copia di sicurezza dei dati del sistema, per ripristinarli in caso di perdita o danneggiamento dei dati (Il piano di conservazione delle copie di backup a lungo termine garantisce che i dati siano recuperabili anche a distanza di anni).

Il processo di "Logging con raccolta su sistema dedicato" consiste nel registrare e monitorare gli eventi di sistema (le azioni che accadono) come l'accesso utente, gli errori del sistema e le attività dei software, tramite strumenti informatici chiamati appunto di logging. Le informazioni raccolte vengono salvate in un sistema dedicato, come un server, che centralizza la gestione dei dati e ne garantisce l'integrità e la sicurezza, l' approccio è particolarmente utile per gli amministratori di sistema per identificare e risolvere rapidamente eventuali problemi o violazioni.

Infine l'aggiornamento automatico e semi-automatico di server e dispositivi, che consiste nell'installazione automatica dell'ultima versione del sistema operativo e di altri software per facilitare la risoluzione di bug, malfunzionamenti o falle nel codice che possono risultare utili per gli hacker.

Sicurezza di rete

Nell'ambito della sicurezza di rete le pratiche consigliate si pongono l'obiettivo di verificare ed all'occorrenza bloccare ciò che entra od esce dal nostro dispositivo, abbiamo per esempio il sistema di FIrewall, un dispositivo o un programma che permette di filtrare il traffico di rete in entrata e in uscita, bloccando i pacchetti di dati non autorizzati e prevenendo quindi gli accessi non autorizzati al sistema. Un'altra tecnica utilizzata per la sicurezza di rete è l'utilizzo di canali di trasmissione cifrati, ossia canali di comunicazione in cui i dati trasmessi sono criptati ovvero resi illeggibili a chiunque non possieda la chiave di decrittazione. Questa tecnica è utile per proteggere i dati sensibili, come ad esempio le informazioni di login e password degli utenti, dalle intercettazioni e dall'accesso non autorizzato.

Sicurezza applicativa

Nello specifico si tratta di regole e vincoli di cui tener conto per uno sviluppo delle applicazioni generalmente più sicuro senza danneggiare le funzionalità del codice. Alcuni esempi potrebbero essere righe di codice che richiedono all'utente di verificare la propria identità durante l'utilizzo del programma (tendenzialmente all'avvio) o che assicurino la protezione dei dati mentre vengono inseriti dall'operatore.

1.4.2 Controlli avanzati

Se i controlli minimi vengono presentati come un insieme di best practice alla portata più o meno di tutte le imprese, medie e grandi, quelli avanzati rappresentano una serie di attività più complesse che richiedono una conoscenza più approfondita delle tecnologie informatiche e della Cyber security o che necessitano un dispendio maggiore di risorse.

Mentre i primi si concentrano principalmente sull'educazione degli utenti e sulla protezione di base dei sistemi informatici, i controlli avanzati richiedono un approccio più proattivo e un'analisi approfondita delle minacce. Questi controlli prevedono l'utilizzo di strumenti avanzati di monitoraggio, di analisi dei dati e di gestione dei rischi, nonché l'implementazione di politiche e procedure di sicurezza più rigide. Nella grande varietà di tecniche esaminate ci focalizzeremo di seguito su una selezione delle più coerenti ai temi della User Experience e agli attacchi per noi di maggior interesse, quelli di phishing.

Formazione de visu

All'interno dei percorsi di formazione del personale è opportuno prevedere esercitazioni che permettano ai partecipanti di verificare le proprie competenze non solo a livello teorico ma anche attraverso concrete simulazioni di attacco. Tali attività permettono innanzitutto ai formatori di correggere eventuali lacune o comportamenti non corretti nell'esatto momento in cui si verificano, e al contempo gli utenti destinatari della formazione hanno l'opportunità di vivere in prima persona le situazioni discusse a livello teorico permettendo una più immediata (e probabilmente più coinvolgente) associazione dei contenuti alle attività che quotidianamente svolgono nel contesto lavorativo.

Riconoscimento biometrico

Con riconoscimento biometrico intendiamo una tecnologia sempre più diffusa (basti pensare a metodi di sblocco per smartphone come il faceID o il lettore di impronte posizionato nella superficie opposta al display) in grado di espandere lo spettro di possibilità nella creazione di "chiavi di sicurezza" attraverso il rilevamento di caratteristiche biologiche uniche e distintive di ogni essere umano come le impronte digitale, la retina, la fisionomia del volto o ad esempio la voce. L'autenticazione dell'identità fino ad oggi ha richiesto solitamente l'inserimento di una sequenza di caratteri alfanumerici (numeri, lettere o caratteri speciali) nota come password. La robustezza di quest'ultima dipende principalmente dalla sua lunghezza e dalla varietà dei caratteri utilizzati nella sequenza, tutti questi sono fattori che rendono più difficile per gli attaccanti superare i sistemi di sicurezza, tuttavia, esistono software come i keylogger o i programmi di detti di "brute force" che consentono agli aggressori di oltrepassare le difese anche in presenza di password complesse.

I programmi di "brute force", ad esempio, sono chiamati così proprio perché sfruttano la "forza bruta" per individuare la password corretta, tentando le più disparate combinazioni di caratteri alfanumerici senza una precisa logica (si va dalle centinaia fino alle migliaia di combinazioni in pochi secondi a seconda della potenza hardware a disposizione). Proprio per questa sua natura, il processo richiede elevate risorse computazionali e tempo, ma può lo stesso avere successo grazie innanzitutto all'avanzare tecnologico che fornisce una sempre più elevata potenza di calcolo e nel caso in cui la password risulti troppo semplice o breve, situazione ben differente da quella che caratterizza un riconoscimento biometrico che invece fa affidamento sulla grande quantità di imperfezioni o micro differenze che rendono unico ogni utente.

In conclusione la tecnologia del riconoscimento biometrico offre numerosi vantaggi rispetto ad altre tecniche più tradizionali garantendo:

- Esperienza più rapida e meno invasiva rispetto alle tradizionali password o PIN, eliminando la necessità di inserire manualmente le credenziali di accesso (bassissimo sforzo cognitivo).
- Maggiori possibilità di personalizzazione, adattando l'autenticazione alle esigenze dell'utente e migliorando la user experience complessiva (ad esempio scegliendo una gesture inusuale ma facile da ricordare per l'utente).
- Alto livello di sicurezza, poiché le informazioni biometriche dell'utente sono uniche e difficilmente duplicabili.
- Elimina il rischio di smarrimento o furto di password, rendendo la gestione delle credenziali più sicura e semplice per l'utente.

Uso di sistemi di autenticazione a più fattori

che accede ai servizi aziendali, una soluzione comune è quella di aggiungere uno step di verifica supplementare. L'autenticazione a più fattori è già comunemente adottata da aziende come Google, Microsoft e praticamente la maggior parte dei servizi web oggi l'adottano. Anche imprese più piccole possono trovare servizi che gestiscono questa funzione per i sistemi aziendali (es.LastPass, Authy, Yubico). Questi sistemi generano convalidano dei codici alfanumerici detti one-time password (OTP), ovvero chiavi di accesso con validità limitatissima nel tempo (generalmente dai 5 ai 15 minuti) e che non possono essere riutilizzate successivamente. Questo codice può essere inviato all'utente che intende accedere attraverso diversi canali. Tra questi, l'invio tramite SMS è considerata meno sicura rispetto perchè più suscettibile di:

- Intercettazione: gli SMS possono essere intercettati o rubati, sia attraverso l'uso di malware (come "Triout", un trojan per dispositivi Android scoperto nel 2018 e diffusosi passando per applicazioni provenienti da store non ufficiali) o grazie all'hacking delle reti cellulari all'insaputa dell'utente.
- Clonazione: è possibile clonare una SIM per ricevere i medesimi SMS in due dispositivi differenti.

Impiego di strumenti di controllo dei dispositivi (AD, MDM)

L'adozione di strumenti come gli l'Active Directory (AD) e il Mobile Device Management (MDM) è un'altra pratica comunemente consigliata per la gestione e il monitoraggio degli strumenti forniti a ogni dipendente per svolgere le proprie mansioni (telefoni, tablet e laptop aziendali):

- L'Active Directory (AD) è uno strumento di controllo centralizzato (dedicato ai Personal Computer) utilizzato per gestire e proteggere gli account degli utenti e le risorse all'interno di una rete, grazie al quale è possibile assegnare e revocare l'accesso ai singoli utenti o gruppi di utenti per garantire che solo le persone autorizzate possano accedere alle informazioni sensibili.

- I sistemi di gestione dei dispositivi mobili (MDM) consentono di proteggere e gestire in modo più efficiente questi dispositivi controllando gli accessi, i permessi e le autorizzazioni per ogni singolo device, oltre che monitorando l'utilizzo dei dati e delle applicazioni, In caso di perdita o furto, consentono la cancellazione remota dei dati sensibili per evitare che i dati finiscano nelle mani sbagliate.

Questi utilissimi tools forniscono maggiore controllo ai responsabili dell'IT e della sicurezza come il CISO che attraverso il loro impiego avranno la possibilità di intervenire direttamente e rapidamente alla risoluzione del problema a seguito per esempio di un furto o di una manomissione di account.

Considerazioni conclusive sulle best practices

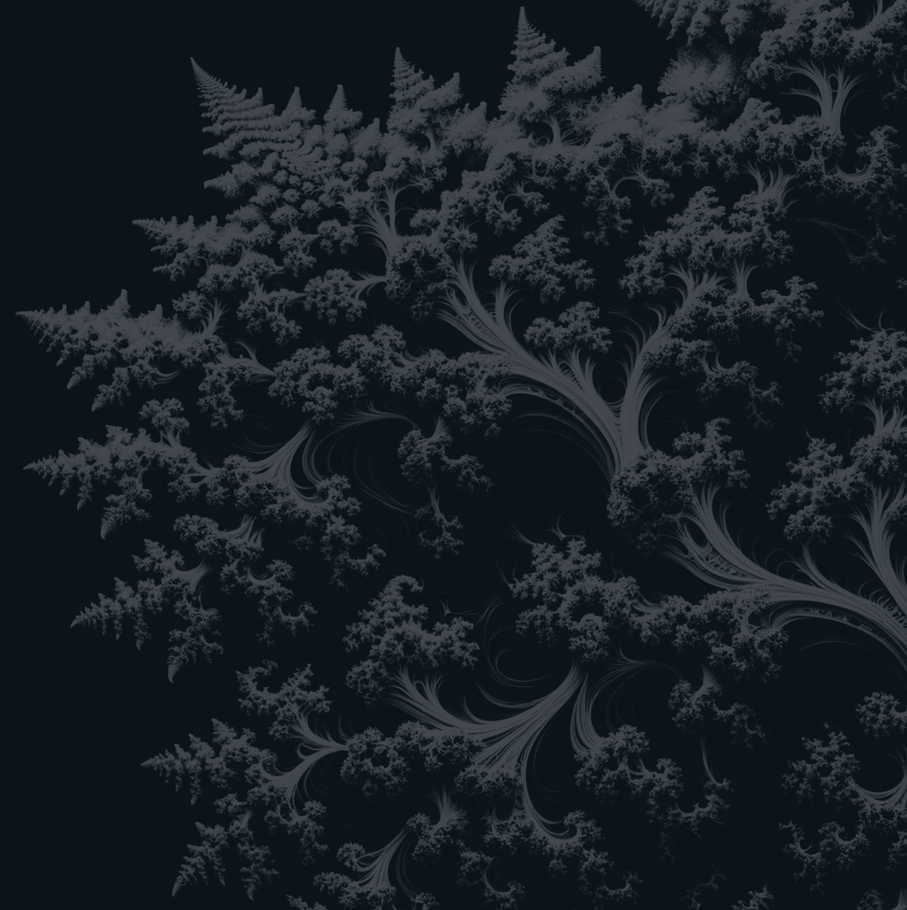
Le procedure fin qui identificate e descritte offrono solamente uno spunto di partenza per una protezione efficace di dispositivi e dati. Se da un lato l'implementazione di queste best practices richieda sforzi significativi (in termini di tempo e risorse) è riconosciuto che i benefici che ne derivano sono inestimabili, se si considerano i rischi e i danni non solo economici che possono gli attacchi informatici possono infliggere alle e spesso alla incolumità e al diritto alla privacy di tutti.

A prescindere dall'entità delle sfide e delle complessità delle situazioni che si possono creare, emerge come la Cyber-security sia soprattutto un lavoro di squadra. ,on il coinvolgimento attivo, promuovendo la consapevolezza dei rischi e favorendo piccole ma importanti abitudini quotidiane, in tutti gli utenti è possibile creare processi di lavoro sicuri, favorendo non solo le attività produttive e la continuità operativa ma proteggendo chi ogni giorno vive e lavora in questi contesti.

Fractal

2

La mente hackerabile



La mente hackerabile

La quantità o meglio la sovrabbondanza di informazioni e stimoli (notifiche, badge) a cui siamo tutti sottoposti nell'utilizzare prodotti e servizi digitali è un fatto riconosciuto. Per districarsi tra questi stimoli e raggiungere i nostri obiettivi, tutti noi attuiamo meccanismi psicologici volti a rendere la consultazione e le nostre azioni più rapide ed efficaci. Daniel Kahneman, psicologo premio Nobel per l'economia, ha introdotto il concetto di "euristiche" nell'ambito della psicologia cognitiva (Kahneman, 2011). Le euristiche sono regole o strategie mentali semplificate che le persone utilizzano per prendere decisioni rapide in situazioni complesse o incerte. La controparte delle euristiche, sono i Bias, ovvero possibili errori che possono verificarsi per la velocità o la mancanza di informazioni che nelle scorciatoie decisionali possono verificarsi.

Tali debolezze cruciali nella protezione dei dati e della privacy online. Un esempio può derivare da comportamenti tipici nell'uso dei social media. Immaginiamo un utente che si imbatte in post che dal suo punto di vista risulta particolarmente discutibile o inopportuno. Il dissenso può già iniziare nell'istante in cui scorge il titolo. A quel punto, la reazione è innescata (per esempio un senso di rabbia) e influenzerà la lettura del post, come dei commenti, dove probabilmente saranno notati in particolare quelli di altri utenti che esprimono un disappunto esplicito. L'esempio appena descritto dimostra come può manifestarsi il cosiddetto "Bias di conferma", ovvero la tendenza, influenzata dalle emozioni o fattori esterni, a privilegiare argomenti che rafforzano le nostre preesistenti convinzioni, trascurando al contempo fonti e contenuti altrettanto affidabili ma che contrastano o smentiscono le nostre attuali credenze, consolidando le nostre idee ma impedendoci di arricchire e ampliare le informazioni a nostra disposizione.

Anche se comunemente ci consideriamo individui razionali, guidati dalla logica e dai fatti, spesso sottovalutiamo l'influenza di fattori inconsci sui nostri processi decisionali. Riflettendo sugli episodi quotidiani in cui la nostra razionalità viene messa alla prova, emerge una domanda: in quanti altri ambiti della nostra vita potremmo agire in modo non del tutto consapevole? E quanto queste scelte possono effettivamente influenzare la sicurezza informatica?

Ma che cosa sono i Bias? Come influenzano il nostro comportamento e come si collegano agli attuali problemi della Cyber-security? Lo User experience design può contribuire a migliorare la Cyber-sicurezza, realizzando interfacce che prevengono errori umani ed evidenziano scelte più sicure?

2.1

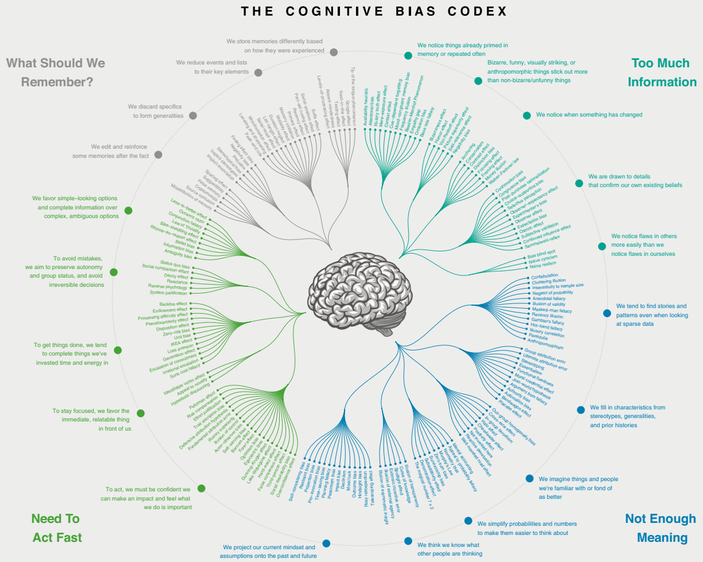


Figura 2.0 – Cognitive Bias Codex (elaborato svg di John Manoogian III).

I Bias cognitivi

Secondo Daniel Kahneman, le euristiche sono come “shortcut” o regole mentali rapide che usiamo per prendere decisioni veloci. Sono “scorciatoie” che utilizziamo per risparmiare tempo, che funzionano bene in ambienti conosciuti ma che possono anche indurre a commettere errori sistematici chiamati “ Bias”. I Bias sono errori sistematici, preconcetti che ricorrono in maniera prevedibile in particolari circostanze». (Kahneman, 2011, pp. 4.). Kahneman assieme al suo collaboratore Amos Tversky, hanno dedicato gran parte della carriera allo studio di questi errori, e, attraverso una serie di esperimenti e ricerche accuratamente condotti, hanno dimostrato che le nostre decisioni e valutazioni non sono sempre il frutto di un ragionamento razionale e ponderato. Al contrario, in determinate situazioni, siamo vittime di errori ricorrenti che influenzano il nostro modo di percepire, elaborare e valutare le informazioni. I processi che portano al manifestarsi di un Bias sono spesso guidati dalla nostra esperienza passata, dalle emozioni e da altri fattori inconsci e incontrollabili. A prescindere dal background di partenza e dal livello di scolarizzazione siamo tutti soggetti a questi errori, che, d’altra parte, non sono inevitabili, ma possono essere anticipati e mitigati da una buona progettazione.

Il numero dei Bias definiti in letteratura è molto alto, come evidenzia la tavola di data visualization chiamata Cognitive Bias Codex (Manoogian, 2016), in cui vengono raccolti ben 188 Bias cognitivi, suddivisi in 4 principali famiglie, in base alla causa sottostante (Figura 2.0).

Uno strumento visivo come il “Codex” può essere molto utile in fase progettuale, per approfondire le condizioni e gli errori che possono verificarsi nell’interazione con un prodotto digitale e identificare i Bias maggiormente coinvolti nelle tecniche di attacco informatico oltre che al loro impatto sull’operato dell’utente. Conoscerli in anticipo, permette ai progettisti di formulare soluzioni preventive e contro-offensive valide per lo specifico prodotto o contesto di riferimento.

Esistono quattro famiglie di condizioni scatenanti:

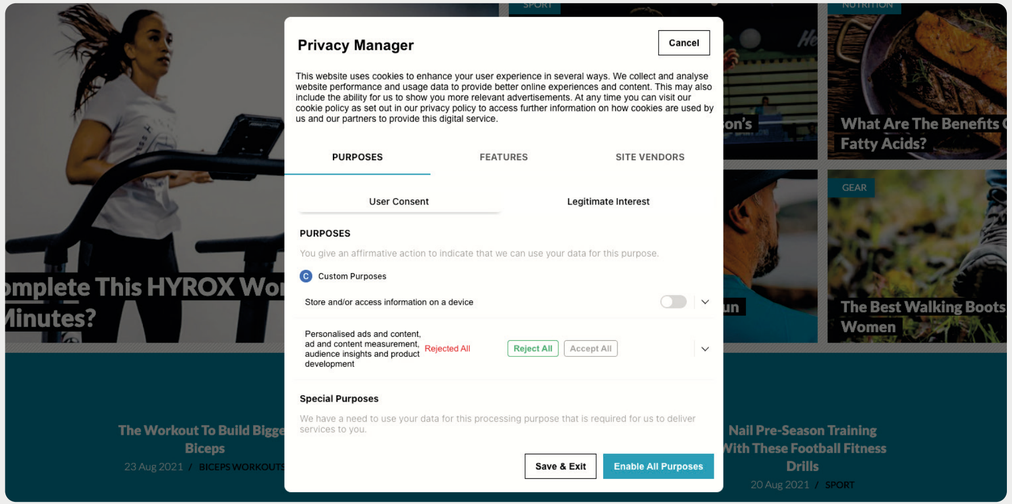


Figura 2.1 – Too much information: esempio di interfaccia che a causa della densità di elementi selezionabili può bloccare l'utente o costringerlo ad accettare termini in modo frettoloso e non consapevole. In figura, un banner per l'autorizzazione al trattamento dei dati personali che, progettato in questo modo, favorisce un maggior consenso (ai cookie richiesti) da parte dell'utente poiché disincentivato alla lettura integrale delle policy.

Sovrabbondanza di informazione (Too much information):

In questa area sono raggruppati gli errori che si manifestano a fronte di **problemi complessi**[12], ossia quando dobbiamo rispondere a una grande varietà di stimoli che non possiamo elaborare interamente o con facilità. L'eccesso di informazioni sovraccarica la nostra mente e ciò può portare al verificarsi di errori nel tentativo di prendere una decisione. Un caso comune è quello legato alla sovrabbondanza di scelte (**choice overload**[13]).

Un esempio efficace in cui questo problema si presenta è rappresentato dai molti banner per il consenso alla Privacy e alla Cookie policy divenuti obbligatori per la maggior parte dei siti web e applicazioni software (**Figura 2.1**).

12. Problemi complessi:
Quando si parla di problemi complessi ci riferiamo a situazioni o quesiti la cui difficoltà è definita specificatamente dalla quantità elevata di informazioni e delle variabili coinvolte.

13. Choice overload:
Si verifica quando l'utente ha di fronte a sé una quantità sovrabbondante di opzioni, portandolo ad una condizione di costante incertezza e valutazione delle opzioni anche per diverso tempo.

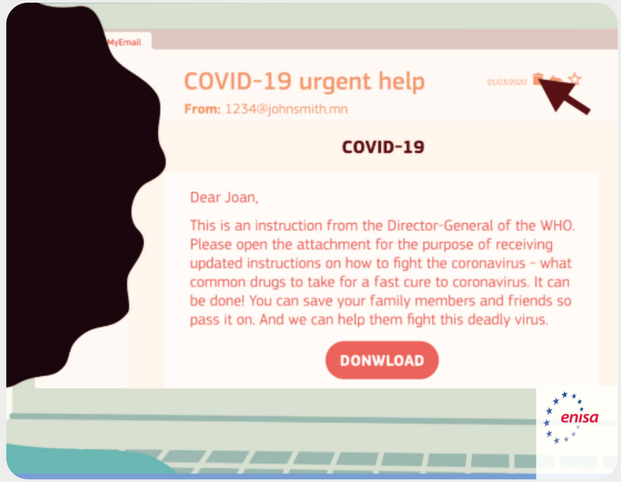
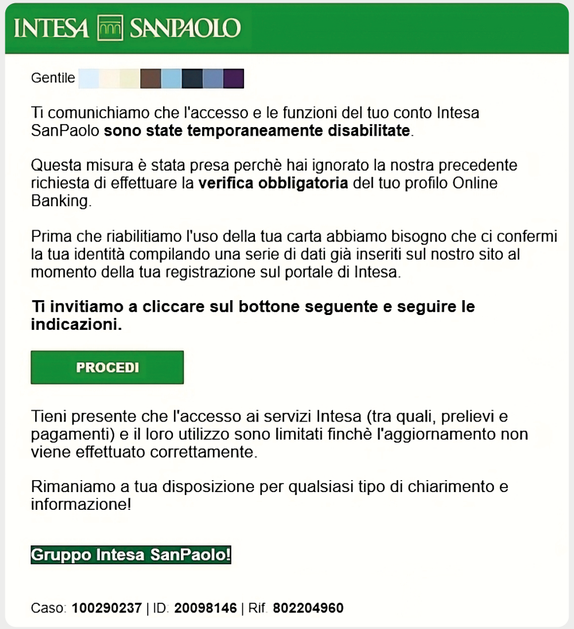


Figura 2.2 – Not enough meaning: Esempio riportato da ENISA e dalla testata Cyber-Security 360, riguardante i numerosi casi di phishing registrati durante la pandemia da COVID-19, in questo scenario diversi Cyber-criminali hanno mascherato i loro attacchi presentandosi come un'organizzazione autorevole quale è la World Health Organization (WHO), ingannando così una grande quantità di utenti.

Informazioni irrilevanti (Not enough meaning):

i Bias raccolti in questa categoria si verificano in contesti che presentano informazioni insufficienti o irrilevanti, impedendo un'elaborazione utile alla decisione. Per sopperire a queste lacune, la mente cerca di elaborare idee attraverso associazioni tra pattern (situazioni simili già note all'individuo) e conoscenze pregresse reputate simili.

Spesso queste associazioni non sono supportate da basi concrete e "contaminando" erroneamente il nostro comportamento. In un contesto di Cyber-sicurezza, un utente esposto a una minaccia che non sia in grado di comprendere o prevedere, data la scarsità di informazioni ricavabili dal vettore di attacco (caratteristica per esempio del phishing), potrebbe sottostimare le conseguenze comportando un significativo aumento del livello di rischio (**Figura 2.2**).



Scarsità di tempo (Need to act fast):

In questo gruppo, si riscontrano bias che emergono principalmente in situazioni in cui la limitazione di tempo spinge gli individui a prendere decisioni con rapidità. La fretta favorisce scelte e comportamenti istintivi ed impulsivi, spesso legati alla memoria di situazioni simili o all'adozione di schemi precedentemente utilizzati per risparmiare tempo ed energie.

Un esempio tangibile di questo fenomeno si riscontra quando si ha a che fare con i servizi bancari, in cui la necessità di risposte immediate da parte degli utenti è un comune denominatore e il cui comportamento è solitamente spinto da un senso di urgenza o priorità, per via del potenziale impatto percepito sulla propria vita. (**Figura 2.3**).

Figura 2.3 - Need to act fast: Esempio contestuale alla tipologia di Bias che fa leva sul senso di urgenza, l'utente bersaglio di questo tentativo di phishing viene intimato di agire al più presto possibile per risolvere un problema bancario ed invitato a procedere con un click sull'apposito bottone allegato al testo.

Dipendenza dalla memoria (What should we remember):

In questa famiglia troviamo casi legati al funzionamento della memoria, che può causare distorsioni dei ricordi nel tempo, informazioni incomplete dovute all'esperienza soggettiva. Un fenomeno particolarmente comune è l'effetto primacy che si verifica per esempio nella lettura di un testo o una lista di dati prolissa, portando l'utente a ricordare o dare priorità ai contenuti posizionati in cima o in fondo al testo, sperimentando un calo di attenzione procedendo nell'operazione. Su questo meccanismo si basano diverse tecniche di comunicazione con cui i contenuti "critici" vengono posposti. Questo fenomeno può avere un ruolo per esempio nei problemi legati al phishing, in cui la priorità data alle informazioni ricevute in prima posizione, possono distrarre o dissuadere la persona nell'analisi più approfondita del messaggio.

In ognuno degli esempi mostrati emerge una chiara componente di intenzionalità, promossa da chi ha progettato i contenuti mostrati, indipendentemente dalla loro legittimità. Questo fenomeno trova nei bias che ci hanno sempre influenzato, una nuova e potente espressione nell'era digitale riconosciuta con il nome di Dark Pattern, un concetto che verrà esplorato più dettagliatamente nel capitolo 2.2, ma solo dopo aver chiarito alcuni aspetti necessari per una comprensione basilare delle interfacce, ossia il "mezzo" attraverso il quale gli errori sistematici vengono artificiosamente innescati da hacker o aziende.

2.2

L’interfaccia utente

Le interfacce sono un elemento fondamentale per l’utilizzo e l’esperienza di qualsivoglia servizio, prodotto, sistema, siano essi hardware o software, **analogici**[14] o digitali. L’interfaccia utente è un artefatto che abilita l’interazione fra l’uomo e la macchina traducendo i dati complessi in stimoli sensoriali comprensibili. In questo modo, offre all’utente una rappresentazione di quello che il servizio o sistema può svolgere.

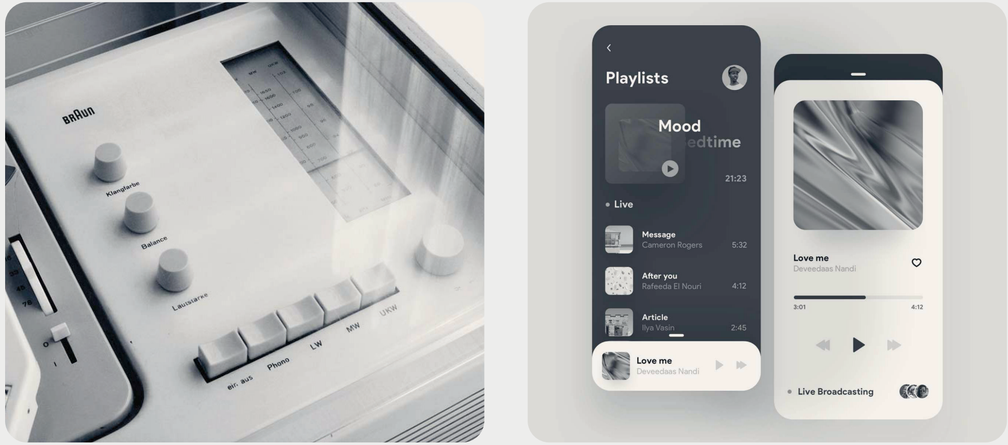
In questo senso, rappresenta uno degli elementi su cui si focalizzano i diversi ambiti applicativi del design applicato all’innovazione (service design, interaction design, user experience design).

Oggi siamo circondati di interfacce in ogni ambito: i pannelli di controllo di elettrodomestici, auto, le applicazioni mobile e il web sono tra gli esempi più semplici da identificare (**Figura 2.4**).

Nel processo di UX design, l’interfaccia è l’ultimo step progettuale, che viene anticipato da fasi strategiche di analisi dei bisogni degli utenti target e delle caratteristiche del contesto. Questi elementi portano poi all’identificazione di e requisiti utili a rispondere al bisogno rilevato, che progressivamente vengono concretizzati in un processo di prototipazione progressivo, con fedeltà sempre maggiore (Rizzo, 2020).

Il processo inizia con la definizione di scenari d’uso e user journey, in cui si prototipa la sequenza di azioni e strumenti che possono caratterizzare un’esperienza, per procedere con la definizione più dettagliata di architettura dei contenuti, progettazione dell’interazione e infine dell’interfaccia grafica. A questo livello, chi progetta definisce la disposizione degli elementi di input e output sullo schermo assicurandosi di offrire un flusso logico, comprensibile, agevole a tutte le tipologie di utenza considerate.

Figura 2.4 – Esempio di un’interfaccia analogica (giradischi Braun SK4 Phonosuper di Hans Gugelot e Dieter Rams) a sinistra e una digitale a destra. Entrambi gli esempi sono relativi ad un sistema per la lettura della musica.



A questo punto è doveroso argomentare alcune nozioni importanti per poter visualizzare con più accuratezza quali sono le fondamenta teoriche a supporto del Design per le interfacce utente, quali L’affordance ed il Feedback. Queste tematiche di fatto torneranno di seguito quando verranno trattati fenomeni nel gergo di settore conosciuti come Dark Pattern.

Affordance

Uno dei principi fondamentali nello UX Design ricade nel concetto di Affordance (**Figura 2.5**), coniato dallo psicologo statunitense James Jerome Gibson nel 1979 e successivamente approfondito da Donald Arthur Norman, che tradotto letteralmente con "autorizzazione" descrive la reciproca relazione che si instaura tra un agente e l'ambiente (Forma Mentis, 2016, pp.26).

Nello specifico, l'affordance si riferisce alle qualità sensoriali (ottiche, tattili, sonore, geometriche, ecc.) possedute da uno stimolo e che sono in grado di suggerire uno specifico utilizzo. Come afferma Norman <<Quando questi inviti all'uso sono opportunamente sfruttati, basta guardare per sapere che cosa si deve fare, senza bisogno di figure, etichette o istruzioni>> (La caffettiera del masochista, 2019, pp.23). Le Affordance possono riferirsi a oggetti naturali o a prodotti artificiali e contraddistinguono proprietà percepibili chiamate "Percettili" che <<oltre a renderli individuabili, contengono anche una serie di "istruzioni" utili per poterle adoperare.>> (Forma Mentis, 2016, pp.27).

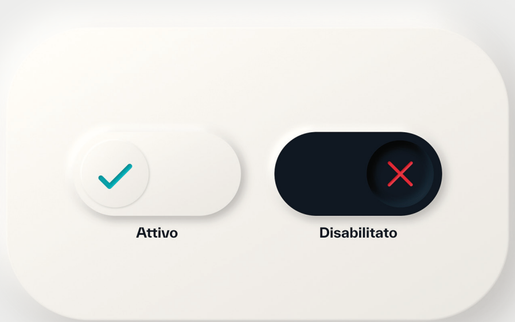


Figura 2.5 – Esempio di affordance digitale

Sempre nel suo libro, approfondendo il concetto, Norman aggiunge:

<<L'affordance dà forti suggerimenti per il funzionamento delle cose. Una piastra liscia è fatta per spingere. Manopole e maniglie sono da girare. Le fessure sono fatte apposta per infilarci dentro qualcosa. Una palla è da lanciare o far rimbalzare.>>
(La caffettiera del masochista, 2019, pp.23)

Feedback

Detto anche "informazione di ritorno", il Feedback è un termine nativo della cibernetica e della teoria dell'informazione, e di riferisce a un elemento fondamentale nella progettazione di sistemi e prodotti, il cui ruolo è quello di tenere l'utente informato riguardo a ciò che sta accadendo mentre interagisce con l'oggetto.

<<L'informazione di ritorno dice all'utente quale azione ha effettivamente eseguito, quale risultato si è realizzato>>
(La caffettiera del masochista, 2019, pp.42).

Nel dominio del Design spesso si traduce in stimoli di varia natura che si verificano in risposta alle azioni dell'utilizzatore, come per esempio i messaggi d'errore, le richieste di conferma, la leggera vibrazione del telefono quando viene attivata la modalità silenziosa (feedback aptico) o i suoni prodotti dal tastierino QWERTY degli smartphone (**Figura 2.6**).

Figura 2.6 – Durante la composizione di un messaggio la tastiera non si limita solamente a fornire i caratteri necessari alla scrittura ma attraverso un apposito insieme di feedback che possono andare dalla vibrazione a specifici suoni, ne conferma l'inserimento del carattere nel testo, fenomeno percettivo simile alla reale esperienza di scrittura con una classica tastiera meccanica.

<<L'informazione di ritorno dice all'utente quale azione ha effettivamente eseguito, quale risultato si è realizzato>>
(La caffettiera del masochista, 2019, pp.42).

2.3

I Dark Pattern

Il termine Dark Pattern è stato introdotto per descrivere elementi dell'interfaccia utente che vengono progettati in modo ambiguo per spingere gli utenti a svolgere le azioni desiderate, limitando o nascondendo quando non impedendo, altre alternative possibili. Tipicamente queste configurazioni si trovano applicate sulle procedure di acquisto online, di sottoscrizioni di servizi, di concessione di autorizzazioni riguardanti la raccolta e l'uso di dati personali. Questi pattern sfruttano le convenzioni più conosciute dagli utenti, applicate in modo scorretto. La confusione che generano può interessare sia persone inesperte, così come esperti che si trovino in situazioni non favorevoli (overload di informazioni, fretta, ...) Questi vengono applicati in modo ingannevole o impercettibile, e possono essere difficili da identificare per gli utenti. In particolare, questi schemi sfruttano alcuni bias cognitivi al fine di influenzare il comportamento degli utenti.

Il designer Harry Brignull ha identificato una lista di quelli che ha definito **Deceptive Patterns**[15], ovvero esempi di schemi di interfaccia ambigui, descritti anche attraverso casi studio e completati da raccomandazioni utili a riconoscerli e contrastarli. Il suo lavoro include una sorta di hall of shame che riguardano casi presi da grandi aziende come Amazon, Meta, Google.

Alcuni Dark Pattern sono più comuni e frequenti sul web rispetto ad altri. Una selezione di questi viene riportata nella Figura 2.5, dove alla descrizione è associato il bias cognitivo (preponderante o principale) su cui si basa.

Un esempio di pratica ingannevole è il cosiddetto **Confirmshaming** (**Figura 2.7**), una pratica comune in particolare nei siti di e-commerce che si manifesta non solo nelle fasi finali dei processi di acquisto ma che può comparire anche in altre interazioni come l'iscrizione a newsletter o durante la chiusura di pop-up promozionali. Questo Dark Pattern si caratterizza per l'uso di un **copywriting**[16] che induce senso di colpa o vergogna nell'utente che suggerisce la scelta desiderata dall'azienda come strategia implicita per farvi fronte. La modalità può includere l'aggiunta di prodotti non richiesti, l'adesione a piani di abbonamento più lunghi, o altre opzioni non inizialmente selezionate. Questa tattica si avvale di espressioni testuali che implicano sottilmente come rifiutare l'offerta sia una scelta meno intelligente o saggia con frasi che frasi che etichettano l'opzione non preferita dall'azienda in modo negativo o che esaltano eccessivamente l'opzione da essa promossa, alludendo così una mancanza di logica o empatia in chi sceglie diversamente.

I bias cognitivi sfruttati da questa pratica includono il consistency bias, che si riferisce alla tendenza delle persone a rimanere coerenti con le loro scelte precedenti, o il framing, che riguarda l'influenza del modo in cui le informazioni sono presentate.

15. Deceptive Patterns:
www.deceptive.design

16. copywriting:
Termine con cui si indica una metodologia di scrittura per fini commerciali, nella quale rientrano per esempio i testi promozionali presenti negli advertising di ogni genere, le informazioni presenti in un sito web o addirittura il contenuto testuale dei suoi pulsanti.

Figura 2.7 – Esempio di Confirmshaming: l'interfaccia suggerisce quali azioni sarebbe più opportuno compiere attraverso elementi visivi più evidenti come il grande bottone nero od il testo messo in risalto, allo scopo di proseguire con un codice sconto, mentre a livello verbale, attraverso l'unica opzione cliccabile che permette di evitare questp step (un semplice testo quasi impercettibile posto sotto al pulsante principale) si intima come la scelta di rinunciare a questa opportunità sia poco sensata.

2.4

Cyber-attacchi e persuasione

Attraverso una comprensione capillare delle singole euristiche è possibile contrastare in parte questi automatismi indesiderati che in concomitanza a una progettazione più attenta rende possibile garantire agli utenti una migliore esperienza online.

In ultima considerazione, i Dark Pattern possono avere un impatto negativo con conseguenze di tipo economico o amministrativo (violazione della privacy). A fronte di questi rischi, gli strumenti di informazione e di consapevolezza, così come le misure di prevenzione e protezione diventano fondamentali, nonostante non siano tutt'ora abbastanza diffuse e propriamente divulgate.

Nel riavvicinarsi al contesto della Cyber-security, successivamente alle argomentazioni del capitolo 2.2, non è difficile ritrovare un filo conduttore che lega l'uso di Dark Pattern con alcune modalità e passaggi che caratterizzano gli attacchi informatici che fanno leva sulla persuasione del destinatario, manipolato per scopi differenti ma sempre sfruttando i Bias cognitivi. Il fenomeno del Phishing è un esempio chiave di come la strutturazione di un Dark Pattern sia applicato in manovre illecite come la frode online o il furto di identità. L'uso dei Dark Pattern in contesti di sicurezza informatica ha rappresentato negli ultimi anni un'evoluzione inevitabile di un fenomeno, quello del Phishing, già di per sé in crescita.

Di fatto il phishing, viene spesso basato sull'emulazione di contenuti, solitamente di carattere commerciale o informativo, come email, banner, contenuti inviati attraverso le app di messaggistica. Mimando fedelmente aspetti distintivi del messaggio (dall'indirizzo al layout), il contenuto fraudolento propone link e azioni che puntano a sistemi fraudolenti. Gli scopi possono essere diversi: catturare dati personali, informazioni sensibili, derubare direttamente o indirettamente le vittime.

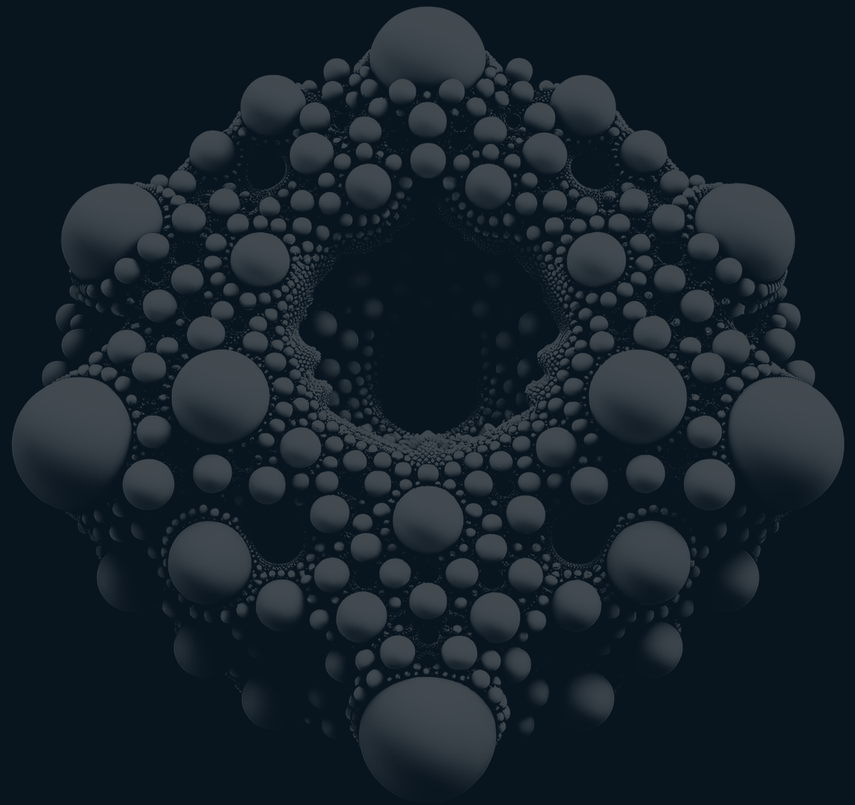
Analisi dei Dark Pattern ed Euristiche più comuni

DARK PATTERN	FAMIGLIA DI BIAS COGNITIVI	BIAS PREVALENTE	DESCRIZIONE	STATO D'ANIMO PREVALENTE
Prevenzione dal confronto	Sovrabbondanza di informazione	Focusing effect	L'utente trova difficile confrontare prodotti a causa di un'organizzazione complessa delle informazioni o della mancanza di dati essenziali.	Confusione
Confirmshaming	Informazioni irrilevanti	Consistency bias	L'utente è manipolato emotivamente per fare qualcosa che altrimenti non avrebbe fatto attraverso il senso di colpa o sensazioni negative.	Senso di colpa
Pubblicità occulta	Sovrabbondanza di informazione	Framing	L'utente viene esposto ad una o più pubblicità, inserite in un elenco di prodotti e riadattate graficamente per assomigliare ad un contenuto appartenente alla lista.	Frustrazione
Scarsità fittizia	Scarsità di tempo	Loss aversion	L'utente è spinto ad agire a causa di una falsa indicazione di disponibilità limitata.	Urgenza
Popolarità fittizia	Sovrabbondanza di informazione	confirmation bias	L'utente è portato a credere che un prodotto sia più valido di quanto non sia in realtà a causa di recensioni o testimonianze false.	Fiducia
Falsa urgenza	Scarsità di tempo	Loss aversion	L'utente è spinto a compiere un'azione a causa di un'apparente limitazione temporale.	Urgenza
Azione forzata	• Scarsità di tempo • Dipendenza dalla memoria • Sovrabbondanza di informazione	• Sunk cost fallacy • Suggestibility • Choice-supportive bias	L'utente viene impossibilitato ad agire come vorrebbe e limitato nella scelta per poter proseguire.	Frustrazione
Difficoltà di cancellazione	Dipendenza dalla memoria	Suggestibility	L'iscrizione ad un servizio è di gran lunga più semplice rispetto alla sua cancellazione, resa volontariamente un'operazione complicata e prolissa.	Frustrazione

DARK PATTERN	FAMIGLIA DI BIAS COGNITIVI	BIAS PREVALENTE	DESCRIZIONE	STATO D'ANIMO PREVALENTE
Costi occulti	Informazioni irrilevanti	Anchoring bias	Il prezzo di un prodotto mostrato in pubblicità non corrisponde al suo effettivo costo o non è realmente conveniente, risultando più elevato in fase di check-out.	Confusione / Delusione
Sottoscrizione involontaria	Informazioni irrilevanti	Automation bias	L'utente viene iscritto a un abbonamento ricorrente o a un piano di pagamento senza una chiara divulgazione o un consenso esplicito.	Frustrazione
Nagging	Sovrabbondanza di informazione	Ostrich effect	Si tenta in maniera persistente (e talvolta non contestuale all'esperienza) di deviare l'utente su altre azioni, servizi o prodotti, attraverso continue interruzioni o banner allo scopo di rallentarlo o dissuaderlo dal continuare.	Frustrazione
Ostruzione	Sovrabbondanza di informazione	confirmation bias	Il sistema rende complesso e difficile il raggiungimento di informazioni o il completamento di un'azione da parte dell'utente.	Frustrazione
Preselezione	Dipendenza dalla memoria	Suggestibility	All'utente viene presentata un'opzione di scelta predefinita, già selezionata dal sistema per influenzare la sua decisione.	Inconsapevolezza
Sneaking	Informazioni irrilevanti	Anchoring bias	Si omettono o posticipano informazioni rilevanti per l'utente, nel tentativo di portarlo a compiere azioni che non farebbe se in possesso di tutti i dati.	Frustrazione / Confusione
Trick wording	Sovrabbondanza di informazione	Framing	Il linguaggio e la terminologia usata per fornire informazioni all'utente è volontariamente confusionario o fuorviante.	Confusione
Interferenza visiva	Sovrabbondanza di informazione	Framing	L'interfaccia non permette all'utente di comprendere a pieno ciò che accade perché approssimativa o male organizzata, le informazioni e gli elementi di interfaccia sono nascosti, oscurati o fuorvianti.	Frustrazione

3

Proposta progettuale



3.1

L’approccio UCD e UX: perchè l’esperienza al centro.

Una volta compreso il funzionamento degli automatismi involontari che affliggono gli utenti, è fondamentale prendere consapevolezza del fatto che anche i progettisti non sono esentati dalla loro influenza. Anche gli addetti ai lavori, infatti, per quanto competenti e consapevoli rimangono comunque esposti agli effetti dei Bias, risultando per loro di assoluta priorità l’impiego di una metodologia chiara e che li mantenga il più possibile in una condizione di consapevolezza e controllo delle scelte progettuali per garantire i risultati desiderati, la soluzione risiede nel porre al centro di tutto l’utente e i suoi bisogni (Bottà, 2018).

Lo User experience design (UX design) è una disciplina che si occupa di progettare prodotti e servizi digitali in modo che risultino facili da usare, intuitivi e piacevoli. L’obiettivo è quello di creare un’esperienza utente positiva, che renda l’interazione con il prodotto o il servizio un’esperienza piacevole e gratificante. L’approccio UX si basa su alcuni principi fondamentali, tra cui:

- Usabilità: i prodotti e i servizi devono essere facili da usare e da capire, anche per gli utenti meno esperti.
- Intuitività: gli utenti devono essere in grado di capire come usare il prodotto o il servizio senza bisogno di istruzioni.
- Piacevolezza: l’esperienza utente deve essere piacevole e coinvolgente.

L’UX design si è sviluppato negli anni ‘90, in risposta alla crescente complessità dei prodotti e dei servizi digitali. In precedenza, l’attenzione era concentrata principalmente sulla funzionalità dei prodotti, mentre l’esperienza utente era spesso trascurata. Con l’avvento di Internet e dei dispositivi mobili, l’esperienza utente è diventata un fattore sempre più importante per il successo di un prodotto o di un servizio. Oggi, l’UX design è una disciplina diffusa in diversi settori, tra cui la tecnologia, il marketing, l’istruzione e l’assistenza sanitaria. Gli UX designer lavorano in collaborazione con ingegneri, sviluppatori e altre figure professionali per progettare prodotti e servizi che siano in grado di soddisfare le esigenze degli utenti.

I capisaldi di questo approccio progettuale includono:

- La centralità dell’utente, la cui prospettiva viene assunta a punto di vista da conoscere e approfondire attraverso attività di ricerca attraverso tecniche dirette e indirette volte a raccogliere informazioni sugli utenti e comprendere i loro comportamenti.
- L’ empatia, come orientamento necessario per comprendere i bisogni e le aspettative degli utenti. La ricerca è un processo fondamentale.
- La prototipazione, come attività utile a concretizzare progressivamente le soluzioni, attraverso un processo iterativo che consente di testare le idee e di raccogliere feedback dagli utenti.
- Il testing, come processo fondamentale per valutare l’esperienza utente e identificare eventuali problemi.

Questi concetti derivano e ampliano quelli dello Human-centred Design, approccio originato dal lavoro seminale di Donald Norman e oggetto dello Standard internazionale **ISO 9241-210**[17] che ne fornisce la definizione univoca:

<<approach to systems design and development that aims to make interactive systems more usable by focusing on the use of the system and applying human factors/ergonomics and usability knowledge and techniques.>>.

<<The term "human-centred design" is used rather than "user-centred design" in order to emphasize that this document also addresses impacts on a number of stakeholders, not just those typically considered as users. However, in practice, these terms are often used synonymously.>>.

<<Usable systems can provide a number of benefits, including improved productivity, enhanced user well-being, avoidance of stress, increased accessibility and reduced risk of harm.>>.

Questo approccio di empatia e ascolto rappresenta un'evoluzione di discipline quali La Human computer Interaction e l'**Ergonomia cognitiva**[18], il cui scopo è quello di fornire al pubblico un prodotto o servizio che oltre ad essere desiderabile per le sue caratteristiche, offra anche un'esperienza di fruizione ottimale, tenendo in considerazione oltre agli aspetti più tecnici dello sviluppo, i fattori psicologici che guidano gli utenti all'utilizzo di tali prodotti, che si tratti di comuni app per smartphone, siti web o altre tipologie di software.

17. ISO 9241-210:
Dall'inglese International Organization for Standardization (ISO) è la principale organizzazione di normazione tecnica al mondo, il codice numerico successivo alla sigla (appunto ISO) serve ad identificare la specifica norma.

18. Ergonomia cognitiva:
Scienza che studia la relazione fra l'uomo, il contesto e gli oggetti che lo circondano dal punto di vista comportamentale (Forma Mentis, 2014). Nel campo del design ci si riferisce spesso all'ergonomia come quella qualità che distingue un prodotto progettato per essere ottimale nella fruizione da parte degli esseri umani, ponendo dunque particolare attenzione alle esigenze (fisiche, psicologiche, ecc) dell'utente stesso.

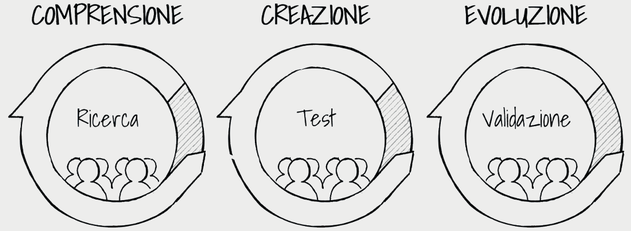


Figura 3.0 - Fasi del processo: Framework di progettazione human centred (Bottà, 2018).

Le fasi operative

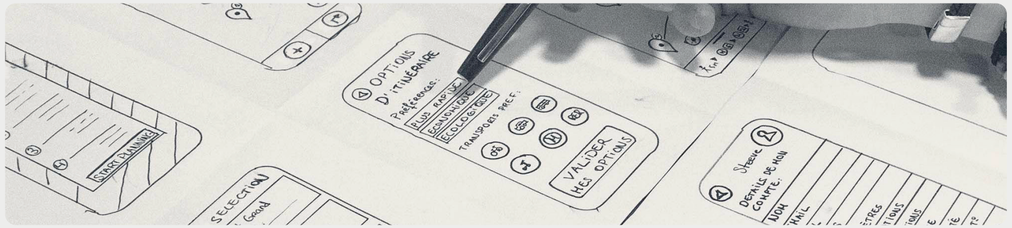
L'approccio Human Centered Design, enfatizza la centralità dell'esperienza umana nel processo di progettazione di prodotti e servizi. Questo approccio, applicato in diversi contesti, propone alcuni passaggi operativi per la realizzazione dei risultati attesi. Il modello a tre fasi (**Figura 3.0**), viene proposto da IDEO (2011) e Bottà (2018) allo scopo di delineare un workflow genericamente affidabile per ogni possibile circostanza progettuale. Esso prevede imprescindibilmente uno sviluppo iterativo e un diretto coinvolgimento degli utenti, in tutte le fasi, al fine di conseguire un continuo affinamento del progetto sulla base di informazioni e riscontri dal contesto reale. Il processo iterativo è uno dei capisaldi dello UX Design, consiste nella ripetuta revisione e rielaborazione di ciò che il team di sviluppo ha prodotto, non limitandosi a una singola fase ma estendendosi su tutto l'arco del progetto. Dalla prima bozza alla versione finale, ogni elemento è soggetto a esame e rifinitura, in un ciclo di perfezionamento che si nutre del coinvolgimento attivo degli utenti (feedback) e nella ricerca di errori o risultati inattesi.

Secondo quest'ottica progettuale, la variabile del fallimento sviluppa un ruolo cardine che non viene interpretato come un ostacolo da evitare, ma anzi, una fonte di conoscenza e parte integrante (ed inevitabile) della progettazione. Le fasi principali che costituiscono il processo di User Experience Design sono Comprensione, Creazione ed Evoluzione.

Comprensione

Fase nella quale i progettisti si concentrano sulla raccolta di informazioni riguardanti il contesto d'uso, i portatori d'interesse, le loro esigenze, necessità e ambizioni per definire il problema su cui formulare la sfida progettuale da risolvere. L'insieme di conoscenze acquisite guiderà tutte le scelte successive, espresse in requisiti e soluzioni. Le attività di comprensione dei bisogni dell'utenza includono l'applicazione di tecniche conoscitive quali l'osservazione, l'intervista, il questionario, che aiutano dunque i progettisti a comprendere i diversi punti di vista presenti nel contesti di riferimento e a focalizzarsi su determinati aspetti di maggior rilevanza e pertinenza in ottica user-centred.Gli strumenti di analisi della User research tipicamente usati in questa fase sono la stakeholder map, user personas, user journey. Si tratta di strumenti visivi che sintetizzano le informazioni raccolte e , aiutano a maturare una prospettiva meno influenzata dai bias e più empatica.

Figura 3.1 – Wireframing: l'esempio in figura mostra un "wireframe". La bozza (in questo caso cartacea) di un'app per smartphone, rappresenta un primo scheletro di interfaccia utente.



Creazione

Le conoscenze acquisite nella prima fase sono utilizzate per iniziare a progettare la soluzione. Compreso il problema dai diversi punti di vista mappati, la fase creativa inizia con l'ideazione di diverse soluzioni che possono rispondere al problema, con attività di brainstorming e rielaborazione collettiva dei dati acquisiti L'identificazione della soluzione da sviluppare avviene sulla base delle priorità, delle caratteristiche, dei vincoli e delle opportunità presenti nel perimetro del progetto. Una volta identificata la soluzione, il percorso progettuale consiste nella prototipazione graduale dell'idea Dal modello concettuale, a sketch di bassa fedeltà, si procede per verifiche intermedie a raffinare un prototipo di crescente grado di fedeltà. Tutti gli artefatti permettono ai designer di valutare progressivamente diversi aspetti del progetto conutenti e stakeholders.La valutazione riguarda non solo aspetti di fattibilità e funzionalità. È considerata fondamentale la semplicità di fruizione o usabilità, per assicurare un'esperienza utente fluida ed efficace. In un processo di UX per il design o il redesign di una soluzione user-centred la progettazione dell'interfaccia grafica è l'ultimo step, che si realizza e consolida i passaggi progettuali precedenti.

Evoluzione

Questa fase raccoglie tutte le attività che permettono di valutare e migliorare il progetto digitale. Inizia naturalmente durante la fase di creazione e continua anche dopo il rilascio, per supportare una logica di miglioramento continuo basato sui feedback degli utenti, raccolti in cicli di aggiornamenti e perfezionamenti. Questo processo implica un monitoraggio periodico e, quando necessario, una reiterazione del progetto. Anche se il prodotto è stato completato e rilasciato, sarà comunque soggetto a modifiche, minori o sostanziali, a seconda delle reazioni del mercato e del target di utenti. Queste variazioni vengono spesso implementate tramite **patch**[19], ciò garantisce che il prodotto si adatti in modo agile e reattivo alle esigenze in continuo cambiamento degli utenti e alle tendenze del mercato (**Figura 3.2**).

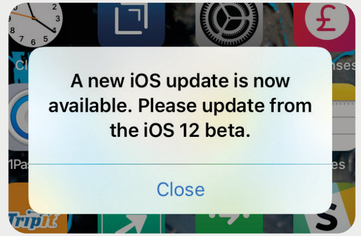


Figura 3.2 – Notifica per patch di aggiornamento: l'immagine mostra un avviso relativo alla disponibilità di un nuovo aggiornamento del sistema operativo.

19. patch:
Termine nativo dell'informatica che identifica una o più porzioni di codice, atte all'aggiornamento di un software già rilasciato.

3.2

Fase 1) La User research

Nel seguito vengono descritte le attività, gli strumenti e i risultati intermedi che sono stati messi in pratica e raccolti nel processo di sviluppo del presente progetto.

Conclusasi la ricerca documentale riguardante il dominio della Cyber-security in senso lato (capitolo 1), che ha permesso di comprendere e definire il contesto e raccogliere dei riferimento dello stato attuale, sono state realizzate delle interviste con l'obiettivo di conoscere e comprendere le attuali reali esigenze, vincoli e opportunità in chiave soggettiva. In particolare, sono state realizzate due interviste con esperti di settore, realizzate online nel periodo che va da Dicembre 2022 (05/12) a Gennaio 2023 (23/01) che hanno permesso di approfondire necessità e criticità a partire dalla loro personale esperienza. Dai bisogni irrisolti sono emersi alcuni spunti progettuali.

Le informazioni raccolte sia dalle interviste che dalla documentazione sono state elaborate per definire e descrivere gli utenti target di riferimento, distinti qui tra attori a rischio e attaccanti. La prospettiva di ciascuno dei due punti di vista differenti (attacco e difesa) è stata descritta attraverso strumenti specifici dello UX design, quali i Personas, e lo User journey.

Per ultimo invece, verrà enunciato il Diagramma delle affinità (detto anche Metodo KJ, inventato negli anni '60 dall'antropologo giapponese Kawakita Jiro) atto ad organizzare la grande mole di dati. Lo strumento è fondamentale principalmente per identificare pattern o temi ricorrenti, permettendo di avviare una prima generazione di concept, da subito attento ad eventuali vincoli, limitazioni o opportunità riscontrate in fase di ricerca.

3.2.1 Le interviste

Per il presente progetto sono stati intervistati due specialisti della Cyber-sicurezza, Il Chief Security Officer (CSO) e Cofounder di un'impresa specializzata in Cyber-security localizzata nella città di Torino ed il ricercatore responsabile di un'unità di ricerca in Cyber-security, sempre con sede a Torino. Entrambi gli incontri tenuti sono stati registrati con il consenso dei partecipanti al fine di garantire una trascrizione precisa ed una conseguente rilettura del pensiero di ognuno dei due partecipanti il più possibile oggettiva e priva di Bias. L'obiettivo ultimo di questo passaggio è stato quello di arricchire maggiormente la comprensione delle dinamiche, delle esigenze e delle sfide che caratterizzano questo campo in rapida evoluzione.

Per la raccolta dei dati è stata utilizzata una traccia progettata per affrontare i temi obiettivo del progetto, riportata di seguito.

1) Il suo lavoro

- Per cominciare, sapresti darmi la tua definizione di cyber security?
- Chi richiede una vostra consulenza solitamente?
- Per quale motivo? (In linea di massima)
- Cos'è l'ingegneria sociale, come la usa nella sua esperienza?
- Quanto è diffuso il fenomeno?

2) il substrato che incontra nelle aziende: barriere, fattore umano, formazione minima

- Quali sono le principali criticità che riscontri in una consulenza?
- Queste criticità si ripresentano spesso? od ogni consulenza propone situazioni molto distinte tra loro?
- Quali sono le responsabilità ed i doveri di un addetto alla cyber security?
- Quando è necessario richiedere l'ausilio di un esperto?
- A suo parere, cosa potrebbe fare un'azienda (od un utente) per rendere il tuo operato più semplice ed efficace?
- Che ruolo ha il fattore umano in un caso di attacco?
- Cosa è in grado di determinare un successo quando ci si difende da un attacco?

3) Base necessaria

- Quanto deve essere competente (digitalmente parlando) un dipendente per offrire un livello di sicurezza basilare?
- Gli utenti con cui hai spesso a che fare risultano sufficientemente preparati?
- Se no, quali sono le principali mancanze?

4) Approfondimento

- Sapresti descrivermi secondo la tua esperienza il profilo di un hacker / cyber criminale?

5) Spunti progettuali

- Come possono gli strumenti del design e della comunicazione, supportare la cyber security?

Interviste: Chief Security Officer

L'intervista condotta, ha riguardato un professionista nel settore della Cyber-security, permettendo di svelare aspetti fondamentali del contrasto all'ingegneria sociale e delle dinamiche di sicurezza informatica in ambiente lavorativo.

La capacità di influenzare comportamenti attraverso il linguaggio si pone come una delle maggiori sfide quotidiane, una modalità di attacco che si annida nelle interazioni digitali quotidiane di ogni utente.
La conversazione ha rivelato che le richieste di consulenza provengono prevalentemente da PMI, spesso dopo aver subito un attacco, delineando un quadro in cui la prevenzione sembrerebbe cedere il passo alla reazione.

Tale approccio si associa, in genere, a un silenzio culturalmente radicato, un meccanismo di difesa che mira a nascondere vulnerabilità e danni subiti a clienti e competitor, evitando parallelamente ogni contatto con le autorità competenti per paura di nuove ritorsioni o danni d'immagine. Il rifiuto di segnalare e condividere gli incidenti di sicurezza emerge come una delle principali criticità espressa vividamente dall'intervistato che afferma <<Si sentono stupidi, e quindi credo che un buon 40% (di attacchi) non viene nemmeno denunciato>>. Un'altra conseguenza negativa di questo approccio riguarda la riduzione delle capacità di sviluppare strategie di sicurezza efficaci a seguito del danno subito.

Per quanto riguarda le competenze digitali di utenti non specializzati, l'accento è posto sulla necessità di formazione continua e test pratici. Questi strumenti sono fondamentali per costruire una consapevolezza che permetta di riconoscere e reagire alle minacce in maniera efficace e tempestiva. L'intervistato enfatizza l'importanza di offrire formazione mirata per incrementare le competenze specifiche: <<facendo piccole pillole e facendo dei test>>.

L'analisi dell'intervista lascia trasparire che, nonostante le sfide, c'è una crescente sensibilità da parte del management soprattutto delle PMI, riguardo la sicurezza dei dati, la percezione del rischio e la responsabilità legale. Su questi temi, le imprese si stanno muovendo per equipaggiare il proprio personale con gli strumenti necessari per proteggere se stessi e l'organizzazione. Il cambiamento di atteggiamento, rispetto a solo due anni fa, è un indicatore positivo del progresso verso una cultura di sicurezza più matura.

Le implicazioni di queste scoperte per il design di soluzioni di sicurezza sono molteplici. Sottolineano l'importanza di sviluppare prodotti che siano non solo tecnologicamente avanzati ma anche intuitivi e capaci di educare gli utenti in modo proattivo, inoltre, emerge la necessità di considerare l'aspetto umano e culturale nella progettazione di strategie di Cyber-security, che affianchino la soluzione tecnica con una comprensione psicologica e comportamentale degli eventi.

Interviste: Ricercatore specializzato in Cyber-security

La conversazione avvenuta con il ricercatore ha soprattutto riguardato le potenziali innovazioni in termini di approcci organizzativi.

Dal punto di vista di chi si occupa di ricerca applicata, finalizzata al trasferimento tecnologico verso le imprese, la sfida che emerge è la mancanza di specifiche chiare fin dall'inizio. Questo problema emerge spesso quando le aziende non hanno un'idea definita di ciò di cui necessitano in termini di sicurezza per i loro sistemi.

Secondo l'intervistato, <<a volte l'impresa stessa non ha idea, di che cosa ha bisogno>>, sottolineando un'area critica nel dialogo tra chi offre e chi richiede soluzioni di sicurezza. La criticità non risiede nella mancanza di competenze tecniche, poiché anche i tecnici qualificati possono avere difficoltà a esprimere le proprie esigenze in modo che informino correttamente le specifiche di un progetto.

Il processo di accompagnamento dell'organizzazione per definire queste specifiche diventa quindi una parte cruciale del processo. In queste fasi di lavoro a stretto contatto con i beneficiari, si svolge anche una funzione educativa nell'aiutare a comprendere meglio le proprie necessità e a formulare richieste che possano trasformarsi in soluzioni di sicurezza efficaci. In questa fase emerge l'importanza di una comunicazione chiara e di un approccio collaborativo nella definizione degli obiettivi di sicurezza, che devono essere ben compresi da tutte le parti coinvolte per garantire l'efficacia delle soluzioni sviluppate. La capacità di trasformare le necessità non articolate in specifiche tecniche concrete è essenziale per creare prodotti che non solo soddisfino i requisiti di sicurezza ma che siano anche al passo con le aspettative del mercato.

Ancora una volta si cita come il possesso di software di sicurezza avanzati,non escluda l'importanza di acquisire una "igiene informatica", ovvero un insieme di buone pratiche e procedure da attuare a livello individuale e organizzativo, per costruire e mantenere un ecosistema Cyber-sicuro. Tra queste basi, vengono citate ad esempio, la gestione dell'autenticazione e buone pratiche di navigazione. Questo genere di strumenti è fondamentale per contrastare comportamenti e abitudini quali la poca cautela nel rilascio di dati personali, la scarsa analisi preventiva dei messaggi ricevuti, in grado celare tentativi di phishing.

In conclusione, l'intervista sottolinea anche il ruolo che design e comunicazione possono giocare nel supporto alla Cyber-security. Soluzioni innovative in questo ambito, vengono identificate in corsi di formazione specifici e l'uso del storytelling per narrare casi di phishing, per incentivare la consapevolezza delle persone.

L'intervistato sottolinea inoltre che un grande potenziale risiede nel miglioramento delle interfacce utente, spesso non efficaci nel fornire informazioni utili, comprensibili e tempestive all'utente non esperto, evidenziando un'area cruciale di potenziale sinergia fra design e sicurezza informatica.

3.2.2 Stakeholders map

Le domande che hanno guidato la user research e la mappatura degli attori sono: Chi sono i portatori di interesse? Come si comportano? Che relazione hanno fra loro? Come sono influenzati e come influenzano loro stessi la Cyber-security?

Per fornire una lettura più completa e dettagliata dello scenario è importante definire, raccontare e ordinare gli attori coinvolti nelle dinamiche discusse. La vasta gamma di attori coinvolti nel dominio della Cyber-security è intrinsecamente complessa, sorge dunque la necessità di una visione più astratta e che faciliti una categorizzazione logica dei portatori d'interesse, che aiuta a definire e distinguere alcuni macro gruppi.

Figura 3.3 – Grafico sulla reciprocità degli attori a rischio.

Utenti

- Tutti noi cittadini, che nel nostro quotidiano interagire con servizi e strumenti digitali, possono influenzare il livello di sicurezza delle aziende e dello stato in cui vivono.

Aziende

- che attraverso la loro attività produttiva, non solo contribuiscono al progresso tecnologico ma anche alla promozione di una cultura della sicurezza in virtù proprio delle regolamentazioni imposte dallo stato (oltre che per necessità), essendo direttamente esposte ai rischi di Cyber-attacchi.

Governi

- Esercitano la loro autorità attraverso politiche e regolamentazioni, influenzando sia le aziende che gli individui nel comportamento e nelle possibilità, definendo dei limiti (leggi e normative).

Questi attori sono protagonisti di traiettorie di influenza e interdipendenza molto complesse (Figura xxx). All'interno di questo ambito, diventa fondamentale identificare chi sono le potenziali vittime, chi si occupa della loro tutela e chi si trova all'origine di un attacco, in modo da poter costruire una mappa completa, ed è secondo questa triplice chiave che vengono riassunti gli attori identificati in tre distinti ruoli e mappe rappresentanti: Bersagli, DIfensori e Attaccanti.

Figura 3.4 – Diagramma di Venn rappresentante potenziali macro gruppi a rischio.

Bersagli di attacco

Singoli utenti (A)

Questo gruppo comprende gli individui che, nella loro vita quotidiana, sia produttiva che privata, possono incorrere in pericoli quali il furto di identità, la violazione della privacy e molto altro. Questi rischi non solo compromettono la sicurezza individuale, ma possono anche avere ripercussioni su scala più ampia, minacciando la sicurezza collettiva e l'integrità dei sistemi informativi a cui gli utenti sono connessi.

Aziende (B)

Sono entità che attraverso la produzione e distribuzione di beni e servizi promuovono lo sviluppo tecnologico e sono direttamente influenzate dai rischi di sicurezza. Le aziende sono a rischio di attacco poiché rappresentano bersagli economici rilevanti, per il capitale di dati personali, economici, know-how e informazioni strategiche che detengono.

Governi (C)

Si configurano come bersagli strategici nel panorama della sicurezza informatica, questo a causa del loro accesso a volumi considerevoli di dati sensibili, essi infatti raccolgono e archiviano informazioni fondamentali non solo per l'amministrazione pubblica ma anche per la sicurezza nazionale, l'economia o la politica. I dati in questione includono informazioni personali dei cittadini, segreti industriali e di stato, nonché dettagli operativi critici per il funzionamento delle infrastrutture del paese.

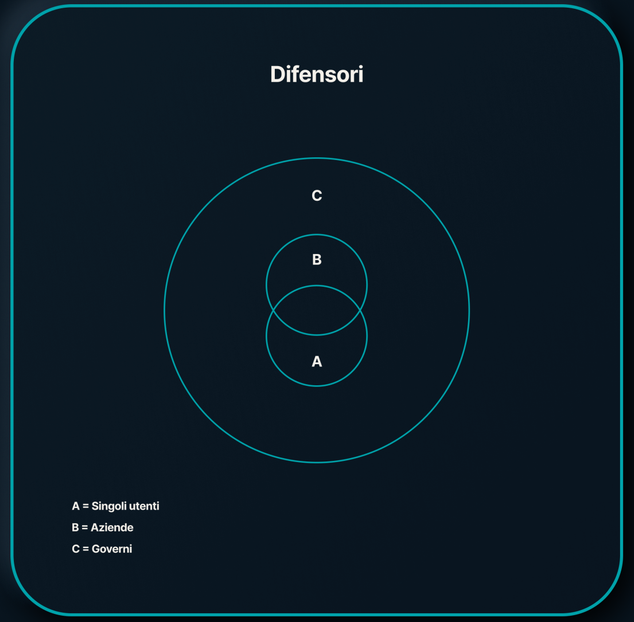


Figura 3.5 – Diagramma di Venn relativo agli attori responsabili della Cyber-sicurezza.

Difensori

Correlato agli attori della Cyber-security precedentemente discussi in Figura 3.2.1, ogni stakeholder citato possiede una controparte specializzata che collabora attivamente nella protezione di sistemi e utenti, come illustrato in Figura 3.2.3.

Singoli utenti (A)

Ogni individuo è un nodo di una rete più vasta. La consapevolezza di questo attore e le misure di sicurezza da esso adottate sono essenziali non solo per la propria protezione ma anche per poter definire un ambiente (dunque stati ed aziende) nettamente più protetto nel complesso, questo rende ogni singolo utente una variabile attiva nella difesa della collettività, sia che si tratti del proprio posto di lavoro che della propria casa o vita privata.

Aziende (B)

Le aziende specializzate in Cyber-security offrono consulenze e distribuiscono servizi, software e hardware critici per la sicurezza, promuovendo anche lo sviluppo di nuovi sistemi e la diffusione di best practice. Queste entità lavorano a stretto contatto con organizzazioni governative e private per costruire una rete di difesa robusta e reattiva. In generale le imprese possono (se adeguatamente supportate) giocare un ruolo di agenti di promozione della sicurezza e del processo di sviluppo tecnologico relativo, al contempo è però importante ricordare che il possesso stesso di tecniche e tecnologie le espone inevitabilmente ad attacchi hacker mirati al furto di armi informatiche e conoscenza in materia. Contando su esperti in sicurezza che ammontano a circa 6000 a livello nazionale, sono il pilastro su cui poggia la tutela quotidiana nell'ambito digitale. Professionisti che operano sia come consulenti indipendenti sia in ruoli chiave all'interno di aziende, come i CISO, i DPSO e i CRA, sono essenziali per valutare, gestire i rischi informatici e garantire la sicurezza dei dati, senza sottovalutare il contributo degli hacker etici, che con la loro expertise supportano organizzazioni e cittadini nella difesa contro le minacce informatiche.

Governi (C)

Vengono identificati come entità con il potere di influenzare nel lungo termine gli altri attori attraverso l'implementazione di politiche e regolamentazioni. Questo suggerisce la loro azione su una scala più ampia, influenzando sia le aziende che gli individui che le compongono. Organi pubblici come ENISA, svolgono un ruolo cruciale nel monitoraggio e nella comunicazione tra Stato, imprese e utenti, provvedendo all'innovazione e al rispetto delle normative e dei diritti civili, o diversamente invece, organizzazioni come la polizia postale, assumono un ruolo più operativo nella conduzione di azioni speciali per la sicurezza e la salvaguardia.

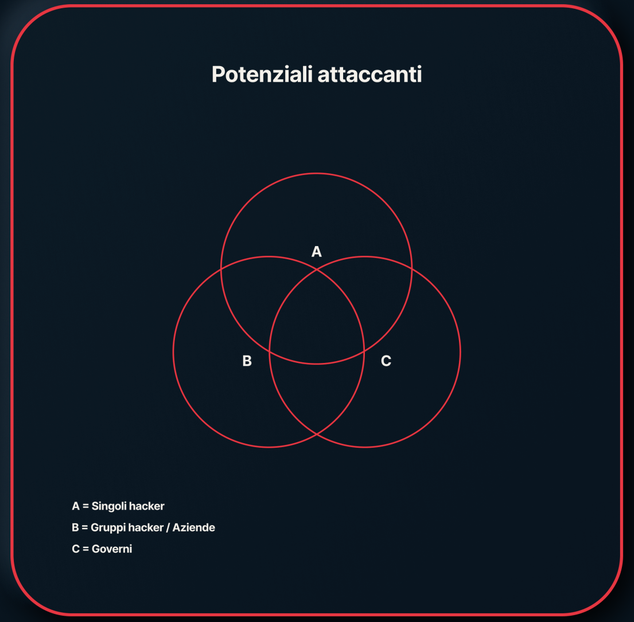


Figura 3.6 – Diagramma di Venn rappresentante potenziali stakeholder dai quali hanno origine i Cyber attacchi.

Potenziali attaccanti

Nonostante non sia possibile eseguire un'accurata stima di quanti effettivamente siano ad oggi gli utenti e le organizzazioni etichettabili come "criminali", è ragionevole ipotizzare che, in relazione al vasto numero di utenti regolari, esista un segmento minore ma significativo di hacker malintenzionati e gruppi che operano illegalmente. Questa frazione, seppur inferiore numericamente, rappresenta una minaccia costante, direttamente proporzionale all'ampiezza dell'ecosistema digitale, tale frangente viene descritto in Figura 3.2.4, dove si identificano tre categorie principali di attaccanti (speculari agli attori bersaglio), ognuno con le proprie motivazioni e metodi:

Singoli utenti (A)

I singoli hacker agiscono indipendentemente e possono avere una vasta gamma di competenze e risorse. Alcuni possono essere mossi da motivazioni ideologiche, altri dalla ricerca di guadagno economico o semplicemente dal desiderio di sfidare le loro abilità contro sistemi di sicurezza sofisticati.
La loro imprevedibilità e autonomia li rendono particolarmente difficili da tracciare e contrastare.

Aziende/organizzazioni (B)

In questa categoria si collocano gruppi, organizzazioni criminali, corporazioni che operano al di fuori delle normative, impegnate in attività come il furto di dati, la distruzione di infrastrutture digitali o la creazione e vendita di malware e lo spionaggio industriale, la loro esistenza dimostra che la capacità di attacco può essere organizzata e sostenuta da risorse significative.

L'intersezione tra queste categorie genera una complessa rete di potenziali collaborazioni tra differenti tipi di attaccanti, per esempio, potrebbero esserci casi in cui singoli hacker lavorino per conto di governi o gruppi organizzati, o aziende che si impegnano in attività di hacking sia autonomamente sia come parte di un'operazione più ampia sponsorizzata da un governo, la sostanziale differenza di questo diagramma se comparato con gli altri sta nel fatto che l'interezza delle azioni svolte dai gruppi sia A, che B che C non rientrano nello spettro della legalità, risultando quindi, caratterizzati da una preponderante indipendenza.

Governi (C)

Per quanto riguarda i sistemi paese, è globalmente risaputo come determinate nazioni poco inclini alla cooperazione internazionale adoperino armi informatiche ed esperti di settore nel tentativo di danneggiare aziende, dissidenti politici o nazioni rivali. La cronaca riporta svariati casi in cui attacchi e attaccanti vengono finanziati da democrature, regimi estremisti o totalitari presenti nel panorama globale contro entità nazionali (United States Department of Justice, 2018).

3.2.3 User personas

Lo User personas è uno strumento teorico dello UX Design e del Marketing creato per delineare un profilo dettagliato e realistico degli archetipi di utenza ai quali un prodotto od un servizio è destinato, attraverso questo processo, si esplorano e definiscono i bisogni e le aspettative degli utenti, basandosi su insight approfonditi dello scenario di riferimento. Definire uno User Personas significa elaborare un identikit credibile di un utente ideale, che rifletta fedelmente le caratteristiche e le motivazioni ricavate dall'analisi del contesto in cui il prodotto o il servizio verrà utilizzato.

A supporto del progetto conclusivo vengono definiti quattro profili accomunati dal contesto aziendale in cui sono inseriti, ciascuno rappresentativo di un ruolo distinto e fondamentale per l'organizzazione.

A questi quattro si aggiunge la figura emergente di un'esperta in cyber security, una hacker etica di giovane età. Questo mosaico di User Personas si rivela essenziale per delineare un'esperienza utente mirata e per sviluppare soluzioni che rispondano in modo efficace e personalizzato alle esigenze di ciascun ruolo all'interno dell'azienda.

Per aumentare ulteriormente il livello di profondità, sono state generate delle immagini attraverso l'uso dell'intelligenza artificiale per fornire ad ognuno dei personas un volto che rispecchiasse almeno in parte l'identikit sviluppato per ognuno di essi.

Luisella Pisano

Una Dirigente bancaria, il cui acume strategico e le capacità organizzative delineano una figura altamente qualificata, cauta e proattiva. Il percorso di Luisella riflette l'archetipo del dirigente che combina competenza tecnica con una visione strategica. Durante i suoi primi anni nel settore bancario, uniti all'esperienza e la continua formazione, hanno contribuito allo sviluppo di una leader determinata, capace di gestire la filiale e di guidare il suo team con mano ferma e intuizione, rendendola un punto di riferimento per i suoi collaboratori.

Marco Re

Chief Information Security Officer che con la sua esperienza decennale si occupa di tutelare l'azienda per la quale lavora dalle minacce digitali. Rinomato per la sua abilità di collaborare strettamente con le divisioni IT e business, Marco eccelle nell'integrare soluzioni di sicurezza che allineano gli obiettivi aziendali con la necessità di agilità e innovazione. La sua dedizione si estende oltre la sfera professionale, in quanto forte sostenitore della formazione e dell'incremento di consapevolezza sulla sicurezza informatica, di fatto, si impegna come volontario in progetti di educazione digitale nelle scuole, questa attitudine rispecchia non solo il suo interesse personale ma anche un metodo per superare la propria riservatezza.

Serena Giorgi

Addetta alle risorse umane, il cui impegno è rivolto verso il benessere dei dipendenti e l'ottimizzazione dei processi interni. Distintasi per le sue eccellenti capacità interpersonali, fondamentali nel suo ambito, affronta quotidianamente le sfide di un ruolo che comporta una pressione costante e numerose richieste da parte di colleghi e superiori, fattori che talvolta la portano a un inevitabile tensione. Questo stato di stress si manifesta con una minore partecipazione attiva e un crescente distacco emotivo con il personale, segnali di un carico di lavoro che inizia a pesare.

Angelico Carbone

Impiegato amministrativo privo di un background universitario, Angelico si distingue per la sua meticolosità e la notevole affidabilità, aspetti che lo rendono un professionista altamente apprezzato. Angelico è dotato di un'inclinazione innata per l'ordine, una competenza che lo fa risaltare nell'ambiente lavorativo, qui i suoi colleghi lo valutano positivamente non solo per le sue abilità professionali ma anche per il suo temperamento calmo e rassicurante, che contribuisce all'instaurazione di un contesto sereno e produttivo.

Luisella Pisano

"Dirigente"

- 38 anni
- Direttrice di filiale bancaria
- Laurea magistrale in Economia aziendale

Bio

Luisella è stata recentemente promossa al ruolo di Direttrice bancaria della filiale per cui ha lavorato sin dai primi anni post laurea, l'attuale posizione le ha richiesto una buona dose di gavetta, corsi di aggiornamento ed anche una serie di condizioni favorevoli alla promozione, uno dei suoi punti di forza è la sua grande determinazione e proattività, unite alle capacità organizzative acquisite con l'esperienza.

Le responsabilità di Luisella la condizionano anche al difuori del lavoro, nel suo tempo libero infatti si dedica spesso alla lettura o ad uscire con la sua compagnia di amici di vecchia data. Nonostante la sua scarsità di tempo, essendo madre single si vede parecchio partecipe anche nella vita sportiva e scolastica di suo figlio adolescente. Il senso di responsabilità nei confronti della sua famiglia la condiziona e sprona nella vita lavorativa a mantenere un'ambiente sicuro oltre che efficiente.

Personalità

Introverso/a — **Estroverso/a**

Analitico/a — **Creativo/a**

Molto impegnato/a — **Poco impegnato/a**

Disordinato — **Ordinato**

Independente — **Lavora di squadra**

Passivo/a — **Attivo/a**

Cauto — **Propenso al rischio**

Interessi

- Sviluppo di nuove strategie finanziarie innovative per la filiale bancaria (Tecnologie FinTech)
- Preservare e migliorare il rendimento della filiale
- Evitare incidenti inaspettati, soprattutto per la clientela

Influenze

- Tendenze economiche globali
- Clientela, colleghi, superiori e dipendenti
- Immagine e reputazione dell'azienda

Obiettivi

- Innovazione Servizi
- Rispettare le aspettative aziendali
- Efficientare e monitorare la filiale

Bisogni ed aspettative

- Sistemi di sicurezza affidabili ed avanzati
- Personale preparato e competente sia per le operazioni di quotidiana amministrazione che per la gestione di crisi
- Sistemi della filiale funzionanti e sicuri per le attività quotidiane

Motivazioni

- Leadership e Sviluppo del Team
- Crescita Professionale
- Senso di responsabilità

Pain points e frustrazioni

- Difficoltà nella comprensione della cyber security
- Tempistiche stringenti
- Regolamentazioni Stringenti
- Limitazione delle risorse

Marco Re

"Esperto in sicurezza informatica"

- 42 anni
- Chief Information Security Officer (CISO)
- Laurea magistrale in Sicurezza Informatica

Bio

Marco è CISO in una multinazionale di tecnologia con oltre 15 anni di esperienza nel campo della sicurezza informatica. Ha iniziato la sua carriera come analista di sicurezza, per poi crescere professionalmente e assumere ruoli di crescente responsabilità. È noto per la sua capacità di lavorare a stretto contatto con le divisioni IT e business per integrare soluzioni di sicurezza che supportino gli obiettivi aziendali senza compromettere l'agilità o l'innovazione. Ha una passione per la formazione e la sensibilizzazione alla sicurezza, si vede promotore di una cultura aziendale che metta la sicurezza al primo posto.

Fuori dal lavoro è volontario in iniziative di educazione digitale per le scuole, un pò per interesse personale ed un pò per contrastare la sua timidezza, contribuendo a diffondere la consapevolezza sulla sicurezza informatica tra i più giovani. La sera, non è raro trovarlo immerso nella costruzione di modellini di aerei, che rappresenta una sua passione di lunga data e un modo per esercitare la pazienza e la precisione che poi riporta al suo lavoro quotidiano.

Personalità

Introverso/a — Estroverso/a

Analitico/a — Creativo/a

Molto impegnato/a — Poco impegnato/a

Disordinato — Ordinato

Independente — Lavora di squadra

Passivo/a — Attivo/a

Cauto — Propenso al rischio

Interessi

- Sviluppo di strategie di sicurezza informatica efficaci
- Formazione continua per se e per gli altri
- Collaborare con i dipendenti per tenere sotto controllo lo stato di sicurezza

Influenze

- Nuove normative del settore
- News e report riguardanti la cyber security
- Community del suo settore e di quelli affini
- Contesto lavorativo

Obiettivi

- Ridurre il rischio di violazioni dei dati all'interno dell'azienda
- Sviluppare programmi di formazione efficaci per i dipendenti
- essere un punto di riferimento nel settore dalla sicurezza informatica

Bisogni ed aspettative

- Personale formato e consapevole
- Riconoscimento e supporto dell'azienda nelle iniziative di sicurezza
- Strumenti avanzati ed efficaci per la sicurezza in azienda

Motivazioni

- Incoraggiare una cultura aziendale riguardo la sicurezza
- Mantenere e migliorare la sua reputazione e credibilità
- Tutelare se stesso, il personale e l'azienda dalle minacce del web

Pain points e frustrazioni

- Su di lui viene scaricata anche la responsabilità diffusa di tutto il personale
- Mancanza di consapevolezza sulla sicurezza informatica tra i colleghi
- Limitazioni di budget che impediscono l'adozione di migliori soluzioni di sicurezza
- Difficoltà comunicative con i meno esperti
- Scarso interesse dalle altre sfere riguardo la prevenzione

Angelico Carbone

"Dipendente affidabile"

- 29 anni
- Impiegato amministrativo
- Diploma di scuola superiore in economia aziendale

Bio

Angelico Carbone è un addetto all'amministrazione in una compagnia di assicurazioni ben stabilita. Nonostante non abbia seguito un percorso universitario, è altamente considerato per la sua precisione e affidabilità. Nel suo ruolo, si occupa dell'elaborazione dei dati, della gestione documentale e del supporto nella comunicazione interna, sempre con grande attenzione e minuziosità. Angelico ha una naturale propensione per l'organizzazione e una predisposizione per il servizio al cliente, qualità che gli permettono di eccellere nel suo ambiente di lavoro, dove i processi amministrativi richiedono meticolosità e precisione. È apprezzato dai colleghi per la sua capacità di collaborare e per la sua personalità tranquilla e rassicurante.

Fuori dal lavoro, Angelico è una persona generalmente equilibrata, molto legato alle sue relazioni ed ai suoi hobbi che riguardano prevalentemente l'attività fisica ed il tracking.

Personalità

Introverso/a	Estroverso/a
Analitico/a	Creativo/a
Molto impegnato/a	Poco impegnato/a
Disordinato	Ordinato
Independente	Lavora di squadra
Passivo/a	Attivo/a
Cauto	Propenso al rischio

Interessi

- Apprendimento continuo
- Attività fisica e strumenti affini per la salute
- Relazioni interpersonali

Influenze

- Community di fitness e benessere
- Colleghi e professionisti del settore
- Esperti di produttività e business

Obiettivi

- Avanzamento di carriera
- Equilibrio tra lavoro e vita privata
- Migliorare le capacità tecniche

Bisogni ed aspettative

- Supporto alla decisione nel contesto lavorativo
- Interazione chiara con colleghi e superiori
- Strumenti affidabili

Motivazioni

- Crescita professionale
- Autonomia
- Salute e benessere personale

Pain points e frustrazioni

- Difficoltà nella comprensione della cyber security
- software aziendali obsoleti o inefficienti
- potrebbe sentirsi sopraffatto se si trova di fronte a un flusso costante di compiti urgenti

Serena Giorgi

"Impiegata in difficoltà"

- 34 anni
- Addetta alle risorse umane (HR)
- Diploma di Scuola Superiore con formazione professionale in gestione delle risorse umane

Bio

Serena è un'addetta alle risorse umane in un'azienda di produzione, un ruolo che richiede una notevole attenzione ai dettagli e capacità interpersonali. Nonostante sia competente e faccia bene il suo lavoro, Serena si trova spesso stressata a causa delle elevate richieste e della pressione costante, questo si riflette in una partecipazione meno attiva e in un distacco emotivo rispetto al suo ambiente di lavoro.

Fuori dall'ufficio, Serena cerca di trovare equilibrio e tranquillità, dedicandosi a hobby rilassanti come lo yoga ed i weekend fuori porta. Tuttavia, la sua vita personale è spesso influenzata dallo stress lavorativo, che limita il suo coinvolgimento in attività sociali o in passatempi più attivi. Serena è consapevole della necessità di trovare un migliore equilibrio vita-lavoro e sta cercando modi per ridurre lo stress e aumentare il suo benessere generale.

Personalità

Introverso/a	Estroverso/a
Analitico/a	Creativo/a
Molto impegnato/a	Poco impegnato/a
Disordinato	Ordinato
Independente	Lavora di squadra
Passivo/a	Attivo/a
Cauto	Propenso al rischio

Interessi

- Yoga e Attività Mindfulness
- Sviluppo Professionale
- Svaghi e relax

Influenze

- Influencers "Esperti" di Benessere
- Colleghi e Rete Professionale

Obiettivi

- Riduzione dello Stress
- Promozione o Ruolo Manageriale
- Sviluppare una Rete Professionale

Bisogni ed aspettative

- Equilibrio Lavoro-Vita Privata
- Ambiente di Lavoro Supportivo
- Strumenti di Gestione del Tempo a lavoro

Motivazioni

- Crescita Personale
- Benessere Psicofisico
- Riconoscimento Professionale

Pain points e frustrazioni

- Sovraccarico di Lavoro
- Difficoltà nella comprensione della cyber security
- Mancanza di Tempo per Sé
- Difficoltà nel Mantenere l'Equilibrio Vita-Lavoro

Eleonora Repetto

"Hacker white hat"

- 25 anni
- inoccupata
- Laurea magistrale in informatica e master in Cyber security

Bio

Eleonora Repetto è una giovane e brillante hacker white-hat che si sta da poco interfacciando al mondo del lavoro con l'ambizione di fare la differenza nel settore della sicurezza informatica. Con una formazione tecnica di alto livello completata, si dedica con passione alla ricerca di vulnerabilità per rendere il web un luogo più sicuro.

Attivista nel digitale, Eleonora si impegna in iniziative etiche e sociali legate al mondo tech, concentrando la sua attenzione sugli aspetti della sicurezza e della privacy online. La sua partecipazione attiva a conferenze e eventi del settore mostra il suo impegno verso la consapevolezza e la divulgazione delle buone pratiche in ambito di sicurezza informatica. Nonostante la giovane età, la sua visione matura e la sua etica professionale la rendono una figura rispettata tra i suoi pari, pronta ad entrare nel mondo del lavoro con l'obiettivo di apportare un contributo significativo e positivo.

Personalità

Introverso/a	Estroverso/a
Analitico/a	Creativo/a
Molto impegnato/a	Poco impegnato/a
Disordinato	Ordinato
Independente	Lavora di squadra
Passivo/a	Attivo/a
Cauto	Propenso al rischio

Interessi

- Sviluppo e Contributo a Software Open Source
- Advocacy per la Privacy Online
- Educazione alla Sicurezza Informatica

Influenze

- Figure di Spicco nella Sicurezza Informatica
- Eventi di Settore
- Comunità Hacker e Tech

Obiettivi

- democratizzare la sicurezza informatica rendendola accessibile e comprensibile a tutti
- influenzare positivamente la società attraverso il suo lavoro e attivismo
- Evoluzione Professionale

Bisogni ed aspettative

- Ambienti di Lavoro Collaborativi
- Rispetto per l'Etica e la Legalità
- Opportunità di Crescita Professionale

Motivazioni

- Fare la Differenza
- Riconoscimento come Professionista
- Contribuire a Soluzioni Innovative

Pain points e frustrazioni

- Mancanza di Consapevolezza sulla Sicurezza del pubblico
- Barriere all'Entrata nel Mercato del Lavoro

3.2.4 User journey di un caso di phishing

Una volta compresa l'entità delle dinamiche sorge spontaneo porsi la domanda sul come queste situazioni si sviluppino all'atto pratico in termini di "azioni distribuite nel tempo", l'obiettivo di questa fase di analisi di fatto è stato quello di fare maggiore chiarezza riguardo ai quesiti: cosa succede, in che modo e soprattutto quando?

Per introdurre le informazioni seguenti è importante fare alcune premesse, successivamente verranno mostrati due "flussi" che differiscono per quanto riguarda il soggetto preso in esame, uno è un ipotetico attaccante impersonato dai Personas Eleonora Repetto (hacker esperta) e Luisella Pisano (Direttrice di una filiale bancaria, competente ed affidabile) un bersaglio di attacco.

Dalla prospettiva di questi Personas sono stati ipotizzati dei flussi di azioni Questo tipo di modello è detto "Customer Journey" e permette di "raccontare" e visualizzare le azioni di un soggetto distribuite cronologicamente, ai fini del raggiungimento di un obiettivo specifico.

Simulazione di attacco

Lo user journey in Figura 1.7 schematizza le azioni che il Personas Eleonora (un bersaglio) potrebbe tipicamente svolgere in uno scenario di attacco. L'esercizio permette di identificare le modalità con cui un esperto può penetrare le difese del suo bersaglio. L'attacco è schematizzato qui in 4 fasi:

1) Preparazione

Eleonora comincia selezionando l'azienda o l'organizzazione da attaccare sulla base di obiettivi e motivazioni intrinseche (es. ideologia, attivismo, motivi personali) o estrinseche (es. interessi economici o di appartenenza). Essendo il bersaglio un'azienda, l'attaccante si concentra nella ricerca di molteplici figure all'interno dell'organizzazione (impiegati, responsabili o consulenti esterni). Una volta trovati Eleonora comincia a studiare i bersagli per carpire pattern comportamentali (azioni che i soggetti tendono a fare con una certa costanza), informazioni private e connessioni con altri dipendenti o utenti. Raggiunto un livello soddisfacente di informazioni comincia ad analizzare i sistemi (dispositivi aziendali, account o reti private) con cui avrà bisogno di interagire per concretizzare la minaccia, solo successivamente inizierà a ipotizzare scenari di attacco, progettati su misura della vittima in modo da garantire un più alto tasso di successo, consapevole di non poter lasciare nulla al caso.

2) Attacco

Conclusa la progettazione, Eleonora lancia l'attacco a più utenti nel momento e nella forma più opportuna per destare meno sospetti possibili e per massimizzare l'impatto, in questo caso si tratta di una mail fraudolenta destinata ai bersagli selezionati. Da questo punto in poi dovrà attendere l'esito e monitorare attentamente la situazione fino a successivi sviluppi.

3) Reazione

L'attacco trova un esito se, dopo aver ricevuto il messaggio malevolo, uno degli utenti bersagliati agisce. Per esempio, in caso di phishing, tipicamente il bersaglio non si accorge o non verifica l'indirizzo email del mittente, il contenuto e le caratteristiche degli allegati o dei link fraudolenti. Nel phishing, chi attacca predispone un sistema quanto più preciso fedele al servizio che si aspetta l'utente bersagliato.

Quando l'utente entra nel sistema fraudolento e compila dati nei form predisposti, l'hacker Eleonora riceve credenziali e dati sottratti, che le conferiscono il controllo dell'account del bersaglio e di tutti i dati a lui accessibili nella piattaforma.
Prima che qualcuno si accorga dell'incidente può passare diverso tempo, in base alle misure di sicurezza implementate dall'impresa. In questo periodo, l'hacker, Eleonora è libera di accedere, alterare e rubare i dati di suo interesse o persino tentare di infettare altri account di utenti più importanti associati a quello in suo possesso.

4) Conseguenze

Se l'attacco andrà a buon fine, l'hacker potrà intraprendere diverse azioni, in base agli obiettivi originari: rivendicare l'attacco o chiedere un riscatto per evitare l'ulteriore diffusione di materiale sensibile online.

Questa ricostruzione racchiude in maniera semplificata gli elementi focali che possono caratterizzare un attacco informatico, in questo caso, di phishing. Sicuramente la capacità di chi attacca nel costruire stimoli in grado di trarre in inganno il bersaglio è fondamentale. Queste condizioni necessitano d'altra parte di una situazione bersaglio favorevole, legata ai sistemi aziendali /o ai comportamenti degli utenti che per fretta, distrazione, mancanza di adeguate informazioni possono mettere in atto comportamenti pericolosi, come non verificare l'indirizzo email del mittente, l'indirizzo URL del link, il testo nel corpo della mail per identificare dettagli sospetti.

Simulazione di difesa

Quando un attacco basato su phishing si verifica, sono diversi gli scenari possibili con cui i bersagli possono reagire. Il Journey in Figura 1.8 ne descrive uno in cui, oltre a un'efficace applicazione delle best practice in fase di attacco. In questo contesto, la User Journey non si concentra su un singolo utente, bensì sull'esperienza collettiva dell'organico dell'azienda bersagliata. Questo approccio è motivato dalla natura degli attacchi informatici che, quando mirano a un'organizzazione, coinvolgono necessariamente più persone all'interno della stessa.

Come per l'attacco, anche la difesa viene schematizzata in 4 fasi specifiche volte alla protezione e messa in sicurezza della filiale, dei suoi clienti e dipendenti:

1) Preparazione

In un primo momento l'azienda grazie alle direttive di Luisella (difensore) e alla collaborazione con consulenti esterni, prepara e redige un'analisi dei rischi e un piano di contromisure. Tale piano prevede misure preventive come l'installazione di nuovi dispositivi e l'attivazione di servizi cloud per il monitoraggio e per la gestione delle operazioni bancarie, formazione per aggiornare il personale sulla protezione dell'ecosistema aziendale digitale, l'istituzione di un comitato di sicurezza per gestire la Cyber-security in ogni aspetto, non solo tecnologico, includendo figure e procedure dedicate.

2) Attacco

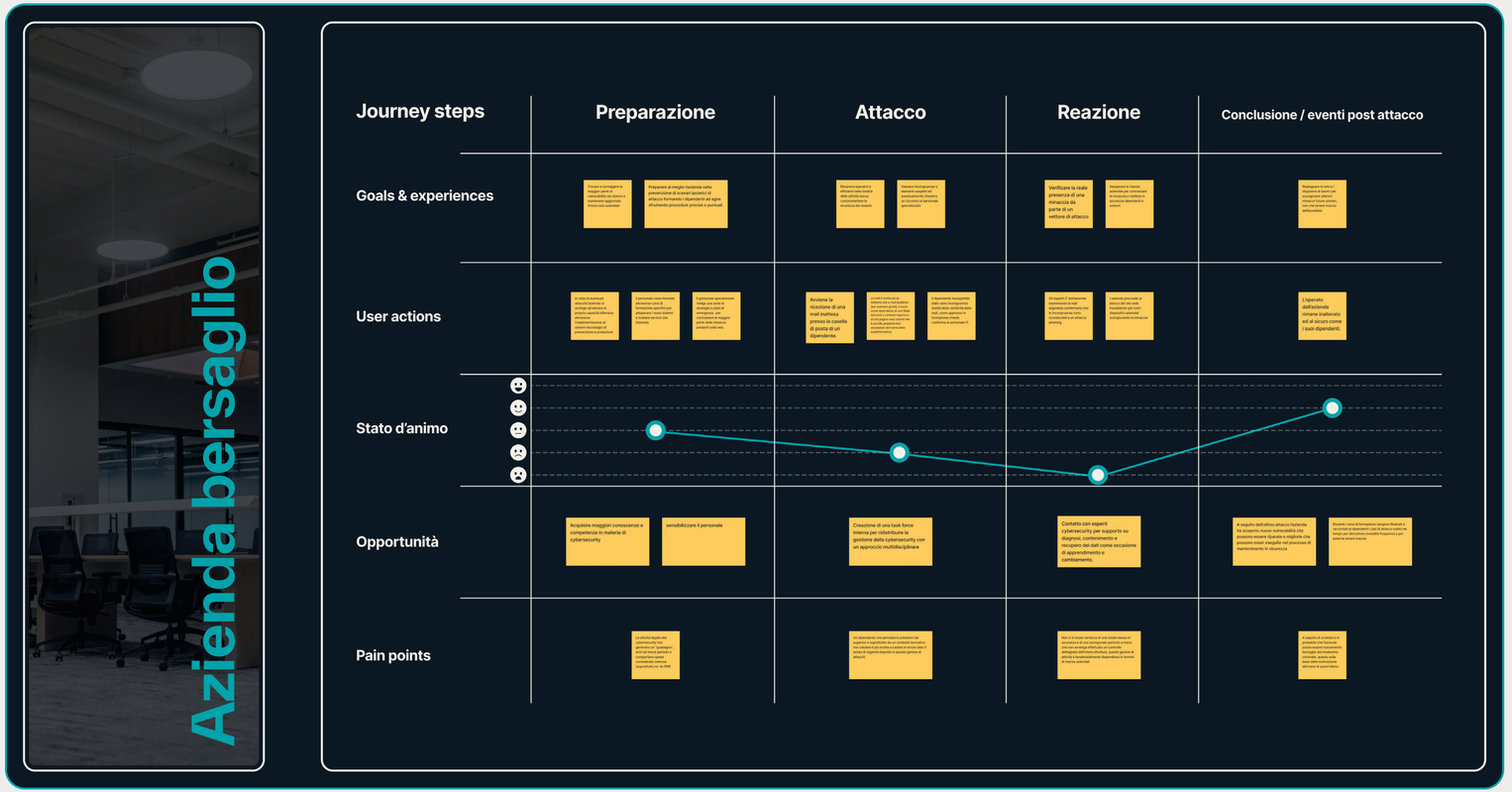
Un'operatore riceve nella sua casella di posta elettronica aziendale una mail contenente informazioni e richieste anomale: la grammatica del testo è errata solo in certi punti, il mittente non risulta noto all'operatore, e in allegato viene richiesta l'apertura di un URL particolarmente lungo. Grazie ai corsi di formazione l'utente identifica gli elementi sospetti della email e richiede l'assistenza di un responsabile per la Cyber-security al quale inoltra il messaggio.

3) Reazione

Il personale specializzato avvia una serie di rapidi accertamenti, mettendo in pratica le apposite best practice descritte nel piano di sicurezza aziendale: vengono impiegati software di sicurezza e conoscenze. Quando viene confermato il tentativo di attacco, il responsabile avvisa il personale tramite i sistemi di comunicazione interna, scongiurando il tentativo di phishing. In parallelo vengono avviate le procedure di messa in sicurezza e verifica dello stato dei sistemi.

4) Conseguenze

Successivamente all'avvenimento, l'azienda dovrà continuare a monitorare la situazione per scongiurare eventuali ulteriori tentativi di phishing e accertare che nessun ransomware sia riuscito a penetrare nei sistemi. Così facendo, l'azienda riesce a scongiurare perdite di dati ed economiche.



3.2.5 Octalys - attacco

Nella fase di ricerca, il modello Octalys ha avuto un ruolo fondamentale come strumento di analisi comportamentale, impiegato per valutare come specifici fattori esperienziali possano influenzare le persone in un'ipotesi di attacco.

Il modello Octalys dimostra come l'attività di hacking risulti particolarmente stimolante e coinvolgente al pari di un'esperienza di carattere ludico, entrano in gioco fattori motivazionali equilibrati fra intrinseci ed estrinseci ma, noti per contribuire fortemente all'instaurazione di uno stato di tensione "positiva" o flow. il criminale dedica meticolosamente le proprie risorse al raggiungimento dei propri obiettivi (accomplishment, social influence, empowerment, epic meaning).

Nell'ipotesi di attacco le attività pongono l'attaccante rapidamente in una posizione di dominio nei confronti degli stati d'animo del soggetto attaccato (accomplishment), permettendogli da subito di avanzare richieste o riscatti, questo solamente a patto che vi sia stata una chiarissima comprensione e preparazione precedente, in altri casi dove il difensore rimane ignaro dell'attaccante gli esiti sono quasi unicamente dipendenti dalle sue capacità nel preservare l'anonimato (avoidance), nelle primissime fasi possono presentarsi repentine e consistenti variazioni degli stati d'animo a seguito dei feedback ricevuti (unpredictability) cosa che però con il passare del tempo tende ad attenuarsi una volta stabilitosi un quadro generale più definito della situazione dove il criminale mantiene una posizione di controllo.

Molto importante è l'instaurazione e mantenimento di un rapporto di sottomissione duraturo, di fatto, trova più conveniente e vantaggioso non gravare in maniera schiacciante sulla vittima divenendo un "male minore" rispetto ad una presa di posizione, che comporterebbe il rallentamento se non il totale arresto del lavoro ed il coinvolgimento delle forze dell'ordine.

Figura 3.7 – Octalys attori di attacco.

Gli stati d'animo chiave sono:

- Eccitazione
- Ansia
- Concentrazione
- Curiosità

In conclusione, praticare un attacco informatico pare essere un'attività in grado di soddisfare diversi requisiti per il raggiungimento di un esperienza appagante.

Octalys - difesa

Contrariamente all'esperienza di attacco, le attività di prevenzione o di contenimento dei danni risultano ostiche e frustranti.

Nel caso della prevenzione le procedure non mostrando benefici nell'immediato futuro vengono trascurate per favorire attività differenti o non correlate alla sicurezza della struttura informatica dell'azienda (Epic meaning), il problema viene rimandato in un ipotetico secondo momento.

Nell'evenienza di un attacco, quando il bersaglio subisce un eventuale arresto della produzione od il processo viene pesantemente ostacolato (Ownership), i danni già subiti, sommati a quelli potenziali, definisco un periodo di grave stress per l'intero ecosistema sia in termini economici che organizzativi, l'unica soluzione a breve termine per la ripresa dei lavori diviene il pagamento del riscatto (Scarcity & impatience, Avoidance, Unpredictability) che rende l'intera struttura dipendente dalla volontà del cyber criminale, importante tenere conto anche delle tempistiche di interazione richieste dall'attaccante.
Un mancato pagamento nell'immediato può presto insorgere in un pesante danno reputazionale nel breve periodo, incrinando i rapporti di fiducia fra impresa, clienti, fornitori, e altri, non tenendo però conto dei ben peggiori danni a lungo termine ingenuamente sottovalutati o reputati come "rimediabili" (Social Influence).

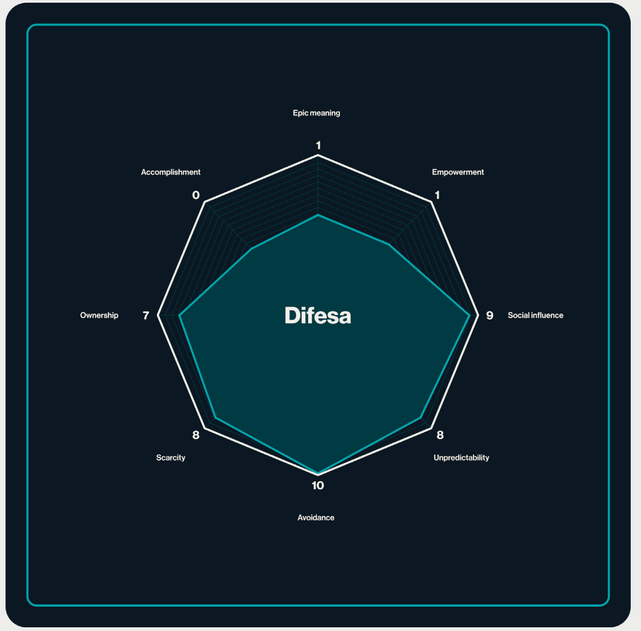


Figura 3.8 – Octalys attori bersaglio.

I provvedimenti richiesti non risultano coinvolgenti per l'azienda ma anzi, un piano di urgenza nella sola eventualità di un danno, gli stati d'animo chiave sono:

- Ansia
- Urgenza
- Sfiducia
- Timore

In questo caso il modello suggerisce che le attività di difesa e prevenzione, oltre a gli ovvi costi fisici (tempo e risorse) per la messa in atto, risultano essere attività complesse, cognitivamente dispendiose e sgradevoli a livello esperienziale.

3.3

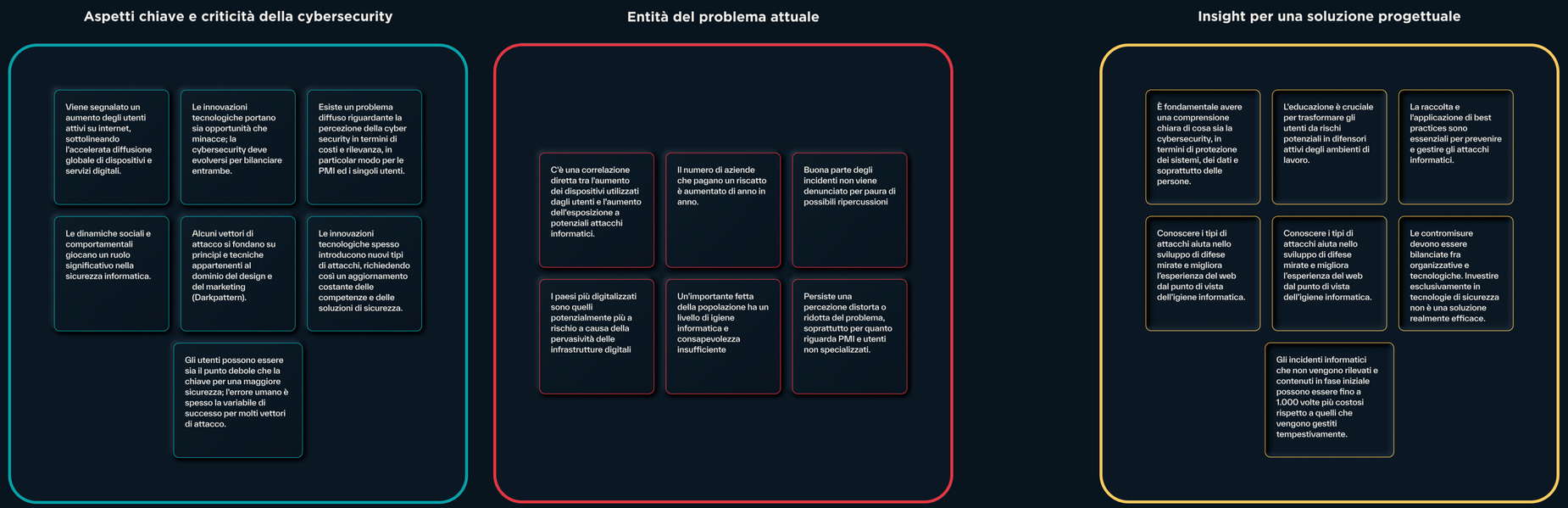
Fase 2) Il progetto

Di seguito verrà illustrata nel complesso il risultato delle ricerche condotte in precedenza, raccontando nello specifico tutti quegli aspetti che hanno permesso lo sviluppo del Touch Point sul quale verte l'intero elaborato di tesi.

In primo luogo si darà spazio alla definizione univoca del problema, al diagramma delle affinità e agli "How Might We", per circoscrivere vincoli ed obiettivi che guideranno il processo creativo, successivamente tradotti in un concept e in una ricerca visiva, mentre in ultima parte verranno esposti gli elaborati prodotti quali il prototipo interattivo dell'applicazione mobile FRACTAL ed i relativi mockup del materiale visual.

Definizione del problema

Tenendo conto della sempre più rapida e capillare interconnessione digitale a cui siamo quotidianamente esposti e la considerevole incidenza degli errori umani nel mantenimento della sicurezza informatica, di anno in anno lo scenario della Cyber-security rischia di complicarsi se non si interviene in maniera sistematica ed efficace sulla percezione, comprensione e preparazione che ogni utente possiede riguardo le crescenti minacce digitali.



3.3.1 Diagramma delle Affinità

Una volta ricavata una soddisfacente quantità di dati, per renderli più facilmente interpretabili ed analizzabili, sono stati organizzati e suddivisi in gruppi specifici, chiamati cluster. Questa metodologia (detta Diagramma delle affinità) permette il riconoscimento di pattern e la categorizzazione delle informazioni basata su somiglianze e differenze significative.

L'approccio non solo facilita una più rapida identificazione delle correlazioni e delle tendenze emergenti tra i dati, ma supporta anche la presa di decisioni informate e la generazione di ipotesi specifiche ottimali per un processo creativo attento ai bisogni dell'utente finale ed allo scenario do riferimento.

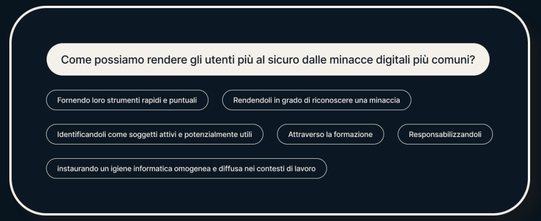
3.3.2 Sfida progettuale - How Might We

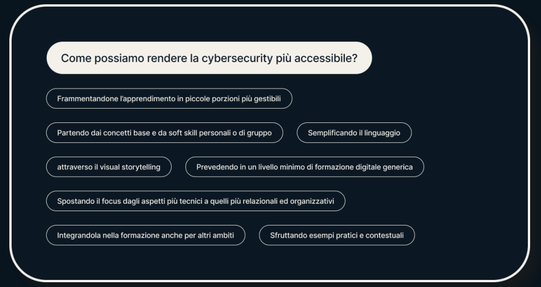
La tecnica “How Might We” (HMW), introdotta nell’ambito del Design Thinking, è impiegata nel processo di design per aiutare chi progetta a inquadrare sfide e problemi in modo aperto ed esplorativo.

Attraverso questa tecnica si arriva a definire il progetto come soluzione al problema, e a identificare diverse caratteristiche del prodotto digitale che si andrà a sviluppare.

Le domande formulate hanno portato l’attenzione su metodi innovativi per migliorare la sicurezza informatica attraverso l’educazione, l’empowerment degli utenti e la semplificazione del concetto di Cyber-security. Il primo passo è affrontare la necessità di proteggere gli utenti dalle minacce digitali più comuni, con strumenti rapidi e formazione mirata per aiutarli a riconoscere e gestire potenziali rischi.

Emerge inoltre un tema di responsabilizzazione, fondamentale per mantenere buoni livelli di sicurezza, da supportare attraverso pratiche di “igiene informatica” da offrire nei contesti lavorativi, dove le pratiche sicure dovrebbero essere parte integrante delle routine quotidiane.





3.3.3 Prodotti di riferimento

Prima di dare avvio alla fase in cui si sarebbe sviluppato il prototipo, sono stati presi in considerazione una serie di prodotti digitali di riferimento da cui trarre ispirazione per stabilire singole feature o caratteristiche potenzialmente utili nella strutturazione di un servizio al passo con gli attuali standard in termini di esperienza utente. L'analisi di questi software ha permesso di identificare elementi chiave che potrebbero essere adattati e incorporati nel progetto, la sfida è stata quella di amalgamare le migliori pratiche di questi sistemi innovativi, integrando aspetti di interattività, sicurezza o personalizzazione.

Learnn

Learnn

Emerge come una piattaforma di e-learning innovativa, offrendo formazione da remoto con contenuti modulari e accessibili. Questa struttura di apprendimento frammentato e flessibile di Learnn ha ispirato la creazione di moduli formativi personalizzabili nel nostro progetto. Ciò consente agli utenti di imparare a proprio ritmo, scegliendo argomenti e modalità di apprendimento in linea con le proprie esigenze, questo prodotto ha influenzato il nostro approccio portandoci ad enfatizzare la personalizzazione e l'accessibilità del contenuto formativo, rendendo l'apprendimento sulla cyber-security più user-friendly e adattabile.

Kahoot!

Scelto per l'apprendimento attraverso il gioco e un'interazione rapida e coinvolgente, specialmente in contesti formativi di gruppo. Questa piattaforma ha suggerito l'integrazione di elementi più informali nel progetto, allo scopo di rendere la formazione sulla cyber-security più interattiva e meno formale. L'approccio di Kahoot!, con il suo focus sull'engagement e sulla partecipazione attiva, ha influenzato significativamente il nostro design, conducendo ad un'esperienza di apprendimento che stimola la curiosità e facilita la memorizzazione dei concetti chiave.

3.3.4 Descrizione del Concept

La Cyber security di oggi non è più solo una necessità, ma una responsabilità condivisa. In risposta alle dinamiche discusse fino ad ora, nel corso delle precedenti analisi dello stato dell'arte, si desidera proporre un concept di applicativo mobile che miri a soddisfare questo bisogno critico di tutela dalle nuove o sempre più diffuse minacce della rete e al contempo capace di promuovere awareness sul complicato tema della sicurezza digitale.

Questo, vuole avvenire focalizzandosi sull'instaurazione di un contesto aziendale proattivo, consapevole e collaborativo, grazie ad una formazione personalizzata e attraverso l'acquisizione di strumenti accessibili per la prevenzione e per la messa in sicurezza di dati, sistemi e persone, seguendo modelli preesistenti di best practices già discusse ma non sempre facili da mettere in atto.

L'intero sistema si fonda su tre concetti chiave che delineano di conseguenza l'insieme di funzioni e possibilità offerte dall'app:

- Consapevolezza: educare in materia di sicurezza informatica.
- Attuazione: agevolare l'impiego di strumenti efficaci e best practices.
- Condivisione: evolvere e consolidare il servizio tramite la sua community di appartenenza.

Pensando a contesti di lavoro, le figure protagoniste del servizio sono individui che possono ricoprire diversi ruoli e funzioni, identificati nella user research come la parte più sensibilmente esposta ai rischi informatici; sono considerati anche gli Admin, soggetti nettamente più competenti e con un ruolo di responsabilità. Entrambi questi profili d'utenza possono interagire grazie all'app come avverrebbe in una classe di studio, dove il docente organizza un programma di apprendimento e fornisce materiale didattico, mentre lo studente si forma e mette alla prova le proprie competenze attraverso dei test valutati.

La realizzazione di questo concept si basa sull'integrazione di diversi elementi esperienziali, non solo digitali:

3.3.5 I Touchpoints

Benché l'intero progetto si focalizzi sulla realizzazione di un prototipo interattivo, parte della riflessione ha riguardato l'ecosistema in cui esso viene immerso, si tratta nello specifico di touchpoints finalizzati all'arricchimento e al supporto dell'esperienza fornita dall'applicativo mobile come mostrato in Figura 3.9.

Mobile App

FRACTAL è un'app per dispositivi mobili attorno alla quale ruota l'intero progetto di potenziamento degli utenti in termini di cyber-security grazie alla formazione e all'instaurazione di team di lavoro in grado di affrontare le minacce digitali con prontezza ed efficacia. Il fulcro di FRACTAL è facilitare la vita quotidiana degli utenti che devono o ricevere una formazione e aggiornamento sulla sicurezza informatica oppure far fronte a situazioni di rischio digitale nell'immediato, rendendo più intuitiva e semplice la comunicazione fra colleghi e la generale sicurezza dei dati/dei sistemi di un'impresa.

Canali social

Allo scopo di comunicare in maniera più approfondita il progetto, i canali social sono strutturati principalmente su 4 piattaforme quali:

- Linkedin: per entrare in contatto con aziende, enti ed organizzazioni tramite contenuti sponsorizzati e newsletter che si avvalgono di un tone-of-voice più professionale e di alto livello. Da qui partiranno inoltre i recruiting e gli inviti a gli eventi ufficiali (workshop, fiere, conferenze).
- Youtube: In questa piattaforma vengono caricati tutti quei contenuti utili all'onboarding dell'applicazione, video tutorial approfonditi sulle funzionalità ed infine le registrazioni dei workshop e degli eventi svolti oltre che all'advertising.
- X e Threads: sono impiegati per coinvolgere le community del settore tech e giornalistico (posizionamento nella cronaca relativa alla Cyber-security) e per condividere con il pubblico eventuali comunicati ufficiali, nuovi aggiornamenti del software e le novità relative all'ecosistema del progetto.

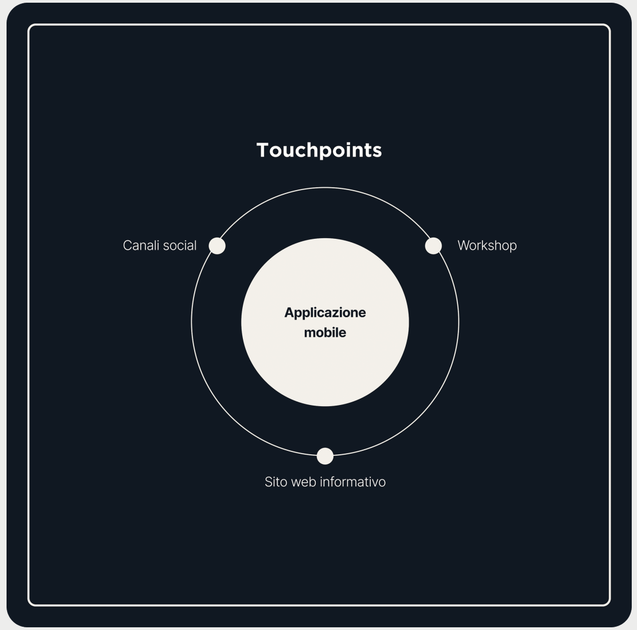


Figura 3.9 – Mappa dei Touchpoints.

Workshop

Occasionalmente verrebbero organizzati workshop ed eventi formativi allo scopo di favorire il networking tra professionisti, aziende, studenti o aspiranti esperti del settore. La pubblicizzazione del servizio diventa dunque un'opportunità per definire occasioni speciali di apprendimento e nuove conoscenze fra stakeholders.

Piattaforma web

Per la gestione delle sottoscrizioni e per il generico supporto al cliente (FAQ), viene messa a disposizione una piattaforma web dedicata, dove sarà possibile ricevere assistenza relativa al proprio account ed alla propria esperienza in app.

3.3.6 Fractal - UI

Qui di seguito viene approfondita la struttura dell'app Fractal, le principali funzionalità e l'interfaccia utente.

L'app è organizzata al suo interno in tre sezioni principali, differenziate visivamente da uno specifico colore:

- Formazione: sezione dell'app dedicata all'apprendimento teorico e allo sviluppo di competenze per la Cyber-sicurezza (contraddistinta dal colore Ciano).
- Minacce: una sezione dedicata ad assistere gli utenti nella prevenzione e prevenzione e risposta a eventuali attacchi informatici tramite strumenti di comunicazione interna (contraddistinta dal colore Ambra).
- Strumenti operativi: area che offre strumenti informativi aggiuntivi detti "risorse della community" che puntano ad ampliare l'esperienza dell'app attraverso nuove feature non disponibili nella versione base, questi possono permettere ad esempio l'esportazione dei dati presenti nello storico minacce in uno specifico tipo di file (XLM, PDF o altri) per permettere la generazione di report, oppure nuove funzioni che vanno ad aumentare le possibilità di formazione con lezioni interattive. (contraddistinta dal colore bianco e nero come in home screen).

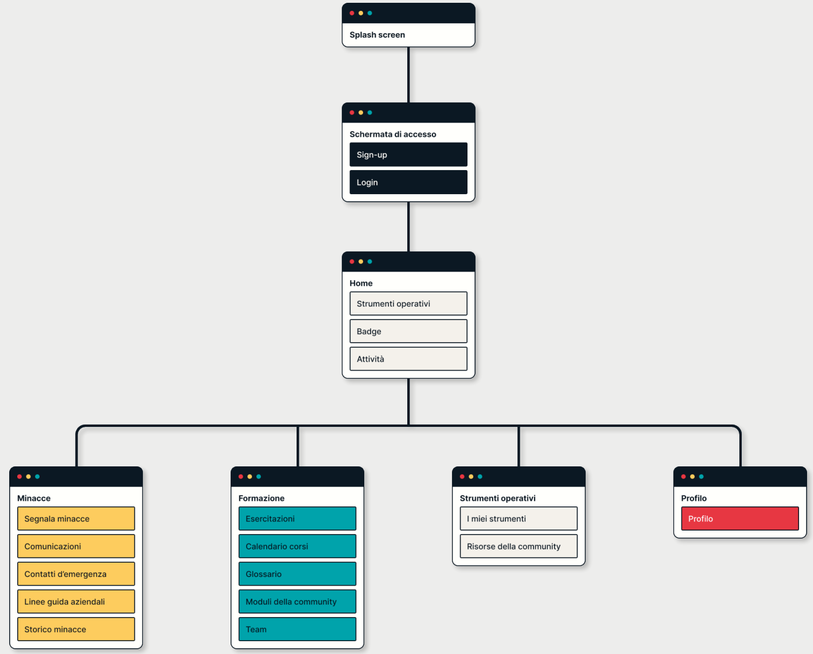
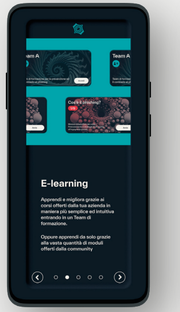


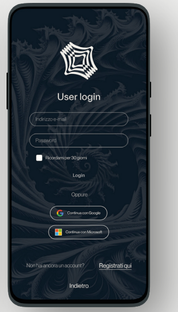
Figura 3.10 – Sitemap dell'applicazione mobile.

Onboarding

Alla prima apertura, l'app presenta tramite un carosello le funzioni e le caratteristiche principali, le sezioni e le funzionalità disponibili.

L'app offre alcune risorse informative generali accessibili anche senza registrazione, che invece è necessaria per accedere alle funzioni di partecipazione ai Team e segnalazione di attacchi. Una volta conclusa la prima introduzione all'applicativo, l'utente viene dunque reindirizzato alla pagina di accesso come guest o tramite login.





Home page

2.1 Un pulsante centrale dedicato alle eventuali segnalazioni legate a sospetti attacchi, pulsante presente anche nella sezione Minacce.

2.2 Un pulsante color ambra di piccole dimensioni provvisto di contatore rosso che notifica l'utente di eventuali comunicazioni inviate o dal proprio team o da un responsabile.

1.3 Il pulsante di accesso alla sezione Team, che raccoglie i gruppi nei quali l'utente è attualmente attivo e nella quale è possibile crearne di nuovi.

2.3 Nella parte bassa, un tasto che porta l'utente alla raccolta di contatti d'emergenza.

3.1 L'ultimo modulo di apprendimento in sospeso (se presente).

1.1 L'accesso ai Badge, ovvero riconoscimenti per gli obiettivi raggiunti, progettati in come meccanica di gamification.

1.2 Il pulsante Attività, che porta a: una sezione che raccoglie i parametri relativi all'operato dell'utente nel corso del tempo.

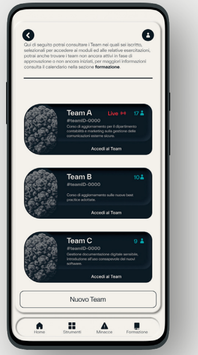
Raggiunta la home page si ha immediato accesso ad una serie di funzioni base poste in una cornice (come la barra di navigazione nella parte bassa dello schermo o il pulsante per raggiungere il profilo utente) dedicate allo spostamento da una sezione all'altra, questa pagina nello specifo funge da HUB centrale.

Pagina dei Badge

1.1

Pagina delle Attività

1.2



Pagina dei Team

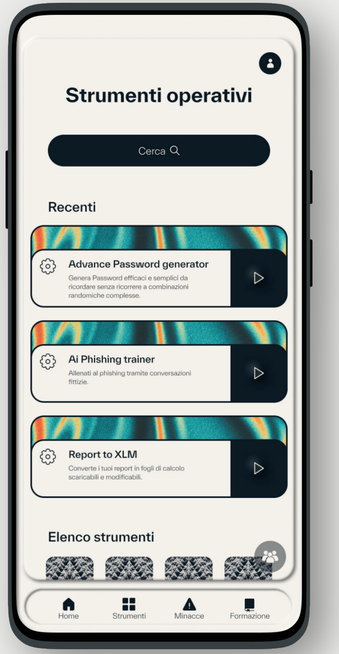
1.3

Centro Comunicazioni

2.2

Pagina dei Contatti

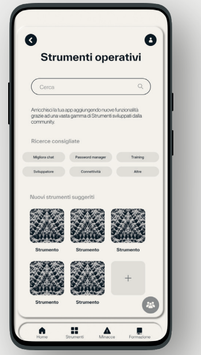
2.3



Strumenti

La sezione strumenti presenta una raccolta personale di funzioni aggiuntive installate dall'utente grazie a un apposito "store" nel quale è possibile cercare elementi aggiuntivi (add-on) da installare.

L'interfaccia viene suddivisa pertanto in una barra di ricerca per le nuove funzionalità posta in alto, una sezione centrale contenente gli ultimi strumenti utilizzati, mentre in basso l'insieme di strumenti già installati.



Formazione

3.2 Un'area posta in cima alla pagina che informa l'utente sullo stato di completamento delle eventuali esercitazioni e che permette un rapido accesso ad esse tramite gli appositi pulsanti posti subito a sinistra.

3.1 Una card che permette di riprendere rapidamente dall'ultimo corso in fase di completamento come in home page.

3.4 Una pagina dedicata al calendario per tenere traccia dei corsi programmati.

1.3 Un secondo pulsante che porta alla raccolta dei team.

La sezione Formazione dell'app raccoglie nella sua struttura tutte le funzioni dedicate alla didattica in generale, dando priorità per esempio alle raccolte di corsi, alle esercitazioni da svolgere ed alla gestione dei team di formazione tramite per esempio la feature calendario o il pulsante Team.

3.3 Un glossario che raggruppa una database di conoscenze basilari per la Cyber-security come terminologia specifica di settore e concetti chiave.

3.5 Un pulsante corsi che serve per accedere alla raccolta personale dell'utente, permettendo un facile recupero dei corsi a cui si è iscritti o che esso sta seguendo.

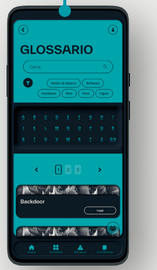
3.6 Una call-to-action che suggerisce all'utente di sperimentare nuovi corsi offerti dalla community.

Riprendi ultimo modulo

3.1

Esercitazioni

3.2



Glossario

3.3

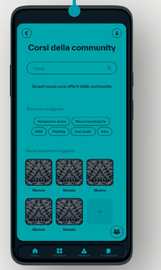
Ogni utente, anche non registrato, avrà a disposizione un archivio di conoscenza base consultabile attraverso un glossario per l'apprendimento della terminologia di settore, per partecipare a una community è necessario essere loggati.

Calendario corsi

3.4

Raccolta corsi

3.5



Corsi della ccommunity

3.6

Minacce

In quest'area viene enunciato l'attuale livello di rischio del proprio contesto lavorativo.

2.2 Un secondo pulsante che porta alla raccolta dei team.

2.3 Viene nuovamente proposto il pulsante per il centro comunicazioni, anche in questa sezione con pin di notifica quando arrivano nuove segnalazioni.

2.4 Call to action che reindirizza alla raccolta di linee guida fornite dall'azienda.

La sezione minacce racchiude le componenti dell'app che possono supportare le fasi di prevenzione e reazioni a eventuali attacchi informatici. Un indicazione sul corrente livello di sicurezza è presentata nella parte alta dello schermo, poi, attraverso gli strumenti di comunicazione, si fornisce il modo per segnalare eventuali problematiche o rapidamente consultare le linee guida per la messa in sicurezza, rendendo l'utente parte attiva della protezione informatica.

2.1 Pulsante prioritario che permette di effettuare segnalazioni al proprio network.

2.5 Sezione che racchiude l'insieme di dati relativi ad attacchi e segnalazioni relative alla propria organizzazione o Team.

Storico segnalazioni **2.5**

Linee guida aziendali **2.4**

Come mostrato nel riquadro **2.1**, l'utente avviando un processo di segnalazione andrà a compilare un breve questionario relativo alla presunta minaccia, che, una volta consegnato raggiungerà immediatamente gli esperti preposti alla sicurezza informatica della propria azienda e che a loro volta potranno informare il resto del (o dei) Team nel centro comunicazioni.

2.1

1 - Avvio segnalazione 2 - Compilazione 3 - Consegna

3.3.7 Ricerca visiva

Moodboard

Generate attraverso l'intelligenza artificiale proprietaria di OpenAI chiamata "DALL-E", questo processo non convenzionale ha permesso la creazione e valutazione di molteplici soluzioni a partire da uno stesso prompt di comandi, raffinato ed ottimizzato nel corso delle diverse generazioni.

Il processo non desidera rendere solo più immediata la creazione di una moodboard ma anche di permettere al progettista di fruire di una più vasta e personalizzata gamma di soluzioni e combinazioni che successivamente andranno necessariamente filtrate e definite, di fatto, il punto di forza dello strumento sta nella quantità di materiale generato poiché soffermandosi ad un singolo elaborato non è minimamente in grado di esprimere uno stile.

Molto importante anche la valutazione del prompt impiegato, nel processo di ricerca di un'immagine sempre più coerente è fondamentale la sua continua raffinazione piuttosto che una generazione randomica a partire dal medesimo testo, la lingua impiegata è stata quella inglese poiché essendo il progetto composto da una moltitudine di vocaboli di origine anglofona si è preferito uniformarsi su di un'unica lingua per evitare interpretazioni fallaci, indesiderate od incoerenti.

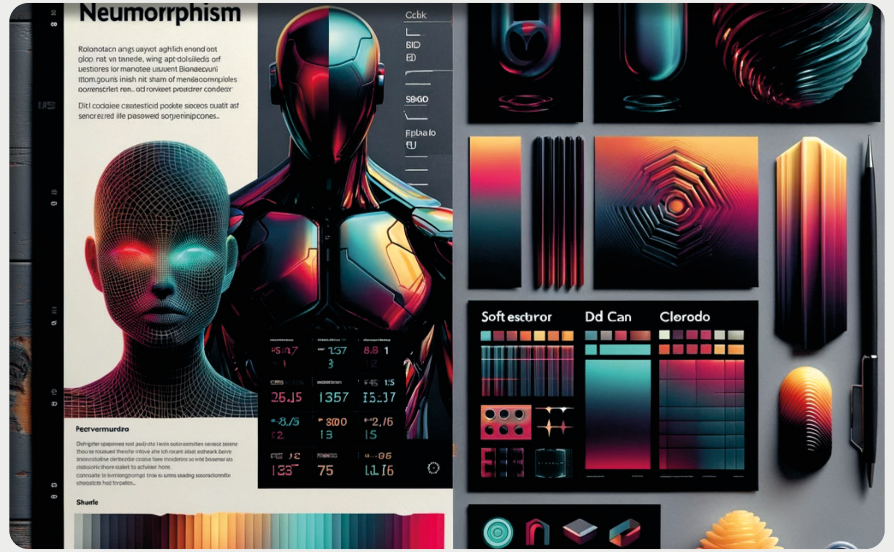
Il suddetto prompt ha come scopo la descrizione dettagliata e chiara dell'immagine da noi ipotizzata e ricercata, per una generazione "a tentativi" dunque è preferibile un testo molto articolato e dettagliato che andrà via via modificandosi od accorciandosi o piuttosto che uno generico o vago, maggiori saranno i dettagli corretti specificati nel prompt e meglio prenderà vita la nostra idea.

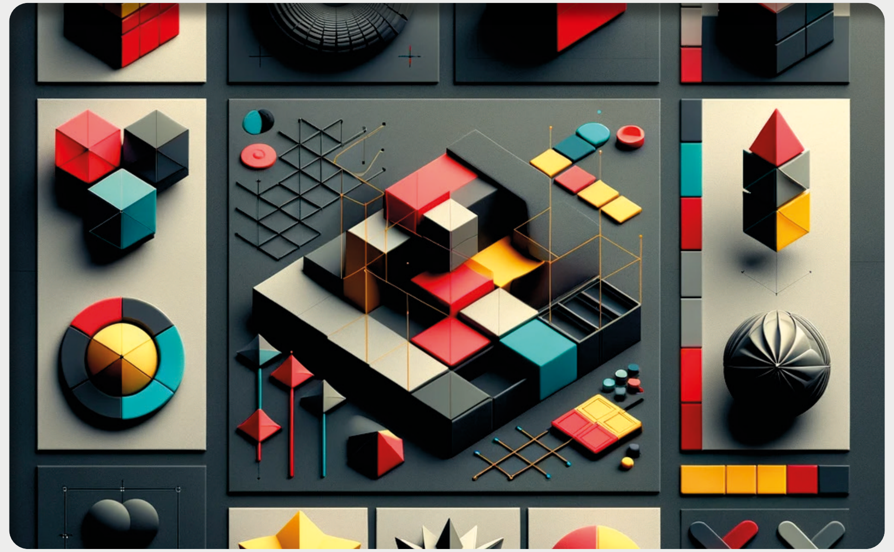
Evitare i Bias e le contraddizioni, quando specifichiamo una serie di caratteristiche per far sì che la generazione abbia una sua coerenza anche logica è preferibile definire una serie di parametri univoci evitando di ripeterli ed evitando soprattutto di inserirne due versioni non congruenti o fallaci nella logica di generazione (non è conveniente richiedere un cerchio ad angoli retti, un palette di colori freddi che vada dal rosso all'arancione), una generazione attraverso prompt sconnessi o comunque errati può contribuire alla generazione di qualsivoglia tipo di aberrazioni all'interno dell'immagine.

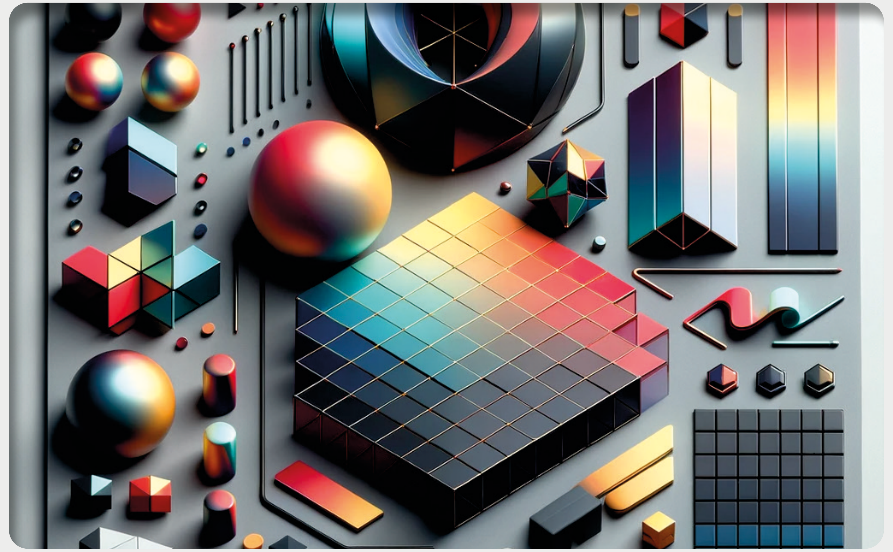
Le moodboard riscontrate generalmente nel web portavano sempre ai medesimi risultati, intuitivi ma ripetitivi e giustificati da una banale distinzione "bene e male" degli attori con palette colori contenenti per lo più tinte piatte come il blu quando si parla di Cyber security, il rosso per gli hacker od il verde quando si parla delle aziende e dei sistemi da salvaguardare, una retorica sicuramente coerente e funzionante ma limitata ad un ristretto spettro di significati.

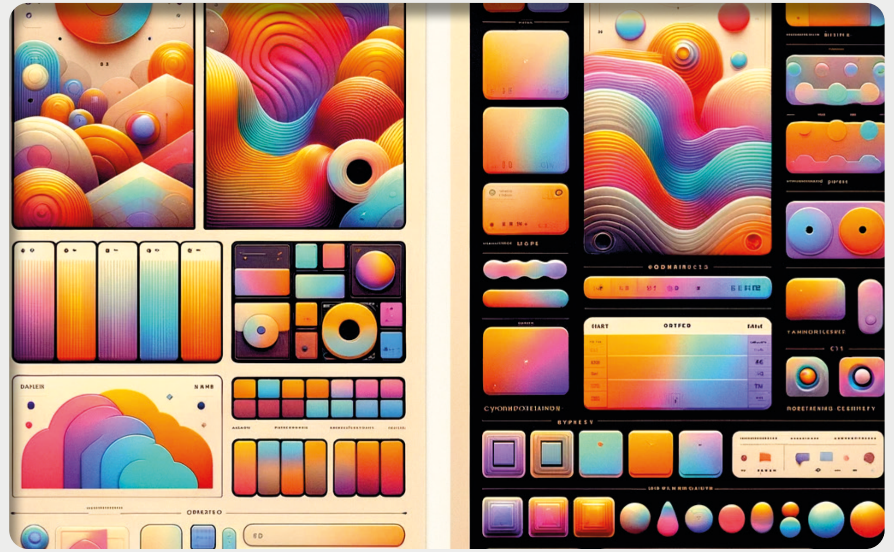
La semiotica iconica del settore pone al centro quasi sempre lucchetti, scudi, segnali di allerta ed allarme, nonostante queste forme siano sicuramente caratteristiche e riconducibili al tema sarebbe opportuno fornire un punto di vista più approfondito e ricerca della simbologia alla base.

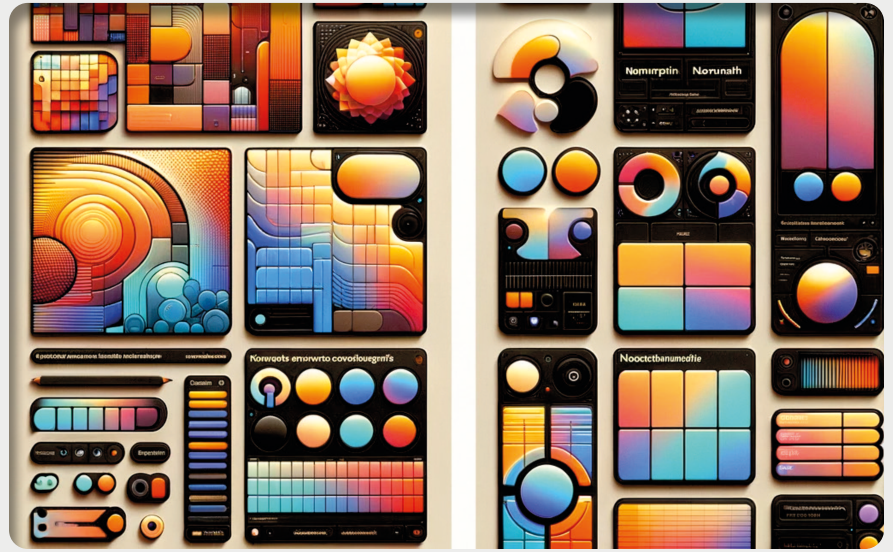
Attraverso DALL-E vengono ricercate nuove suggestioni in grado di ampliare il discorso da un punto di vista sensoriale di tipo ottico andando a delineare nuovi scenari progettuali stravolgendo le palette con il rigore di esprimere specifiche emozioni quando necessario, non cercherà di essere dunque una ricerca stilistica prettamente estetica e determinata dal gusto personale ma bensì un'evoluzione ponderata, evitando il più possibile di ricadere negli stereotipi e nella banalità che caratterizzano anche la percezione del settore da parte del grande pubblico.


Neumorrphism







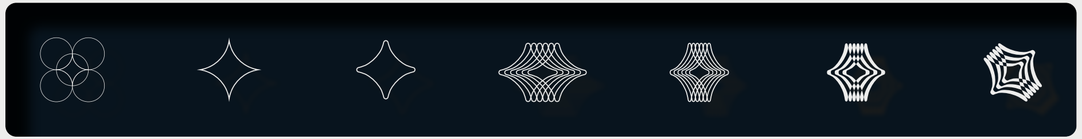


Identità visiva

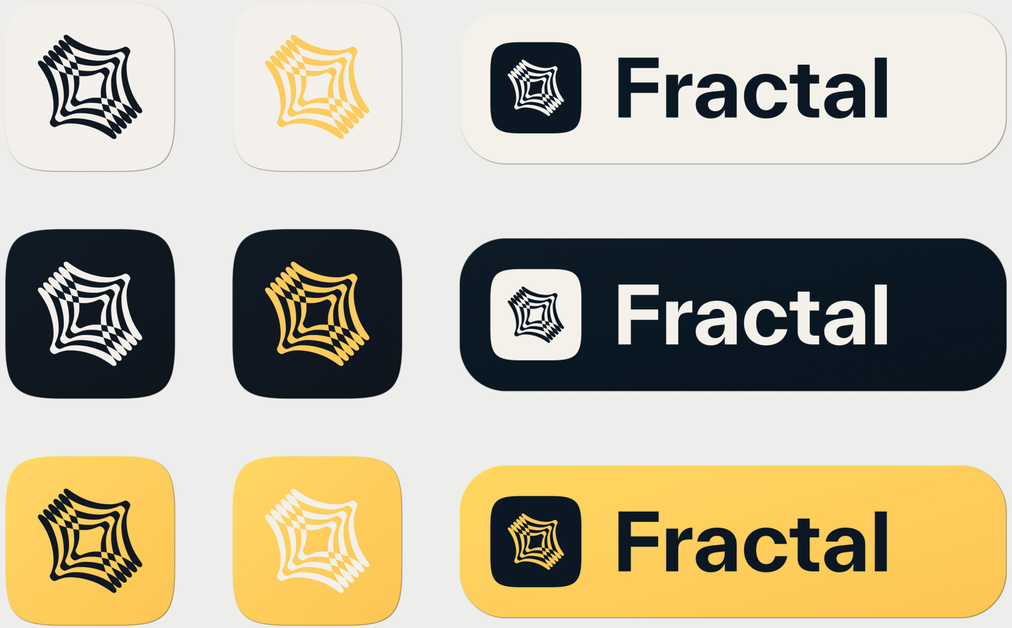
Come i frattali, il cui design è determinato da semplici formule ripetute su diverse scale, così la sicurezza informatica richiede attenzione nei dettagli a ogni livello. Il logo, ad essi ispirato, è stato progettato per rappresentare visivamente questo concetto. La sua struttura vuole comunicare ripetizione e interdipendenza, l'uso del colore invece desidera raccontare la stratificazione dell'apprendimento promossa dall'app attraverso appunto il micro learning.

Il carattere tipografico scelto, il TWK Everett, riflette la modernità e la natura digitale del campo della cybersecurity. Con le sue linee pulite e la connessione distintiva tra le aste di molte lettere, il font evoca un senso di interconnessione e tecnologia avanzata, che sono fondamentali per un'applicazione che si propone di essere all'avanguardia nel campo della formazione e della prevenzione della sicurezza informatica.

L'intero materiale visual esplora il contrasto generato da complesse ed articolate composizioni di frattali tridimensionali, in scala di grigi, alternate a layout e grafica in stile neobrutalista e neumorfista che comportano invece elementi ariosi e minimalisti.



Fractal



TWK Everett Regular

ABCČDEFGHIJKLMNOPQRSŠTUVWXYZŽ
abcčdefghijklmnopqrsštuvwxyzž
#$%^&*0123456789_.;.:

Aa Aa Aa Aa

TWK Everett Bold

ABCČDEFGHIJKLMNOPQRSŠTUVWXYZŽ
abcčdefghijklmnopqrsštuvwxyzž
#$%^&*0123456789_.;.:

Aa Aa Aa Aa

PANTONE 433 C
#1d252d

PLATINO
#E5E4E2

PANTONE 135 C
#FFC658

PANTONE 032 C
#EF3340

PANTONE 320 C
#009CA6

Fractal

4

Conclusioni e prospettive

La presente tesi ha evidenziato come lo User Experience Design e la comunicazione svolgano un ruolo fondamentale nell'ambito della cybersecurity, rimarcando l'importanza di strategie umano-centriche per migliorare la consapevolezza e la resilienza di organizzazioni e privati cittadini di fronte alle minacce informatiche.

Le ricerche suggeriscono che la progettazione di esperienze digitali sicure non sia semplicemente una questione tecnica, ma richieda anzi una profonda comprensione delle dinamiche umane e degli aspetti psicologici legati all'utente. La collaborazione interdisciplinare tra i campi della cybersecurity, del Design e della psicologia emerge come una possibile strategia vincente nel contrasto alle nuove minacce digitali.

Questo lavoro in conclusione, sottolinea l'urgenza di riconsiderare l'approccio tradizionale alla sicurezza informatica, proponendo un modello più inclusivo e partecipativo, incoraggiando l'adozione di pratiche di design centrato sull'utente, possiamo non solo contrastare più efficacemente le minacce cyber, ma anche promuovere una cultura digitale più consapevole e responsabile.

Ringraziamenti

Molto sentito è l'affetto a chi mi ha supportato lungo tutto il percorso, sia dentro che fuori dall'università nonostante gli ostacoli, alcuni più evidenti, altri meno.

Ringrazio dunque mia nonna Lucia, mia Madre Rosangela e gli amici Simone, Gianmarco, Michele, Luigi, Marco.

Ringrazio sinceramente la professoressa Frisiello per avermi guidato con grande pazienza e gentilezza in questo ultimo progetto qui al politecnico.

In fine ringrazio Asia che fra tutti per prima, ha creduto in me.

Riferimenti - Bibliografia

Bottà Debora, User eXperience Design, Hoepli, 2018.

Buiatti Eleonora, Forma mentis. Neuroergonomia sensoriale applicata alla progettazione, Franco Angeli, 2016.

Bureau of Investigation and Analysis of Industrial Risks (BEA-RI), Investigation report On the fire in the OVH data, Ministère de la Transition écologique, 2022.

ENISA, Good practice guide on vulnerability disclosure, 2015.

ENISA, Threat Landscape 2022, 2023.

Floridi, Luciano (ed.) The Onlife Manifesto. Being Human in a Hyperconnected Era. Springer, 2014.

International Electrotechnical Commision (IEC), IEC-GUIDE-120-2023, 2023.

Kahneman Daniel, Pensieri lenti e veloci, Mondadori, 2011.

Mazzini Federico, Hackers, Storia e pratiche di una cultura, Laterza, 2023.

NIST (National Institute of Standard and Technology), Computer Security Incident Handling Guide, Gaithersburg, 2012.

Norman Donald Arthur, La caffettiera del masochista. Il design degli oggetti quotidiani, Giunti Psicologia, 2019.

Rizzo, A. Ergonomia cognitiva. Il Mulino, 2020.

Schneier Bruce, Secrets and Lies: Digital Security in a Networked World, Wiley, 2004.

Riferimenti - Sitografia

Atomic Design - Brad Frost, "Atomic Design Methodology":
atomicdesign.bradfrost.com/chapter-2/ (ottobre 2023)

Allianz, "Detection and response tools increasingly important as cyber claims surge":
commercial.allianz.com/news-and-insights/news/cyber-security-trends-2023-press.html (giugno 2023)

Bitdefender, "Triout - Spyware Framework for Android with Extensive Surveillance Capabilities":
www.bitdefender.com/blog/labs/triout-spyware-framework-for-android-with-extensive-surveillance-capabilities/

Cisco, Meraki Blog (MDM), "Gestione dei dispositivi mobili: su larga scala per i team IT più piccoli":
meraki.cisco.com/blog/2022/11/mobile-device-management-big-scale-for-smaller-it-teams/

Cybernews, "How to create good and strong passwords":
cybernews.com/best-password-managers/how-to-create-a-strong-password/

DCD, "OVHcloud's data center fire: One year on, what do we know?":
www.datacenterdynamics.com/en/opinions/ovhclouds-data-center-fire-one-year-on-what-do-we-know/ (agosto 2023)

Deceptive Patterns:
www.deceptive.design (settembre 2023)

Digital Guardian, Resources and documentation:
www.digitalguardian.com/dskb/cyber-security (marzo 2023)

Enciclopedia Treccani online:
www.treccani.it

ENISA (Agenzia dell'Unione Europea per la Cyber-sicurezza):
www.enisa.europa.eu/publications#c3=2013&c3=2023&c3=false&c5=publicationDate&reversed=on&b_start=0 (agosto 2023)

Focus, "Troppe possibilità di scelta, nessuna decisione: così il cervello va in sovraccarico":
www.focus.it/comportamento/psicologia/cervello-choice-overload-scelte (ottobre 2023)

Fullstory, "What is user friction? How to avoid the mistakes and optimize your UX":
www.fullstory.com/user-friction (ottobre 2023)

Guerre di rete, "Cosa è rimasto dell'eredità di Aaron Swartz, oggi":
www.guerredirete.it/cosa-e-rimasto-delleredita-di-aaron-swartz-oggi/

Guerre di rete, "Sulla storia dell'hacking c'è ancora molto da raccontare":
www.guerredirete.it/storia-hacking-ancora-molto-da-raccontare/ (aprile 2023)

HP official website, Security Resources:
www.hp.com/us-en/solutions/computer-security-resource.html (aprile 2023)

Kaspersky Resource Center, "Buone abitudini di igiene informatica per stare al sicuro quando si è online?":
www.kaspersky.it/resource-center/preemptive-safety/cyber-hygiene-habits (marzo 2023)

Kaspersky Resource Center, "The Virus Encyclopedia":
encyclopedia.kaspersky.it/knowledge/years-1970s/ (marzo 2023)

Kaspersky Resource Center, "Tips for Generating Strong and Unique Passwords":
www.kaspersky.com/resource-center/threats/how-to-create-a-strong-password (marzo 2023)

Kaspersky Resource Center, "What is Social Engineering?":
www.kaspersky.com/resource-center/definitions/what-is-social-engineering (marzo 2023)

Microsoft, "Active Directory (AD) Domain Services Overview":
learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (marzo 2023)

Riferimenti - Sitografia

Neurexplore, “Quali sono gli effetti dei Bias sulla percezione della comunicazione?”:
www.neurexplore.com/it/ Bias-cognitivi-comunicazione (Novembre 2023)

New York Times, “Cyberattack Forces a Shutdown of a Top U.S. Pipeline”:
www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html (agosto 2023)

Oracle, “Cos’è il machine learning?”:
www.oracle.com/it/artificial-intelligence/machine-learning/what-is-machine-learning/ (13/10/2023)

Repubblica, “Attacco hacker a Colonial Pipeline: pressione su gas e benzina negli USA”:
finanza.repubblica.it/News/2021/05/10/attacco_hacker_a_colonial_pipeline_pressione_su_gas_e_benzina_negli_usa-29/ (agosto 2023)

Repubblica, “Cybersecurity, in Italia servono almeno 100mila esperti in più”:
www.repubblica.it/dossier/economia/innova-italia/2022/07/05/news/Cybersecurity_in_italia_servono_piu_esperti_almeno_100mila-356695711/
(agosto 2023)

The Register, “OVHcloud datacenter ‘lacked’ automatic fire extinguishers, electrical cutoff”:
www.theregister.com/2022/03/22/ovhcloud_fire_datacenter_report (agosto 2023)

TSW (THE SIXTH W), “ Bias cognitivi: le scorciatoie mentali che influenzano le nostre scelte”:
www.tsw.it/journal/ricerca/ Bias-cognitivi-scorciatoie-mentali-influenzano-nostre-scelte/ (novembre 2023)

The United States Department of Justice, “North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions”:
www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (agosto 2023)

Washington Post, “One year ago, Colonial Pipeline changed the cyber landscape forever”:
www.washingtonpost.com/politics/2022/05/06/one-year-ago-colonial-pipeline-changed-cyber-landscape-forever/ (agosto 2023)

We Are Social, “Digital 2023 – I dati globali”:
wearesocial.com/it/blog/2023/01/digital-2023-i-dati-globali/ (agosto 2023)

Wired, “Chi è Kevin Mitnick, il più celebre degli hacker”:
www.wired.it/article/kevin-mitnick-famoso-hacker/ (marzo 2023)

Wired, “Cosa sappiamo dell’attacco ransomware a Ferrovie”:
www.wired.it/article/ferrovie-attacco-ransomware/ (luglio 2023)

Wired, “Il premio Turing ai pionieri della crittografia a chiave pubblica”:
www.wired.it/attualita/tech/2016/03/02/premio-turing-crittografia-chiave-pubblica/ (ottobre 2023)

Wired, “L’invisibile cyber guerra della Russia per piegare l’Ucraina”,:
www.wired.it/article/ucraina-russia-guerra-attacchi-informatici-malware-ddos-energia/ (febbraio 2023)

Wired, “Trenitalia assaltata dagli hacker di Hive Group: timori per i dati personali dei viaggiatori”:
www.repubblica.it/tecnologia/2022/03/24/news/trenitalia_assaltata_dagli_hacker_di_hive_group_vogliono_5_milioni_di_dollari-342626658/
(agosto 2023)

Wired, “Un pezzo di internet è andato a fuoco, letteralmente”:
www.wired.it/internet/web/2021/03/10/incendio-data-center-ovh-strasburgo/ (agosto 2023)

Riferimenti - Videografia

FILIPPO LUBRANO | TEDxVerbania - “Storia della Cybersecurity: dalla guerra fredda ai ransomware”:
www.ted.com/talks/filippo_lubrano_storia_della_Cybersecurity_dalla_guerra_fredda_ai_ransomware

Tomorrow unlocked - “Why Would Cybercriminals Hack a Fridge?”:
www.youtube.com/watch?v=w74tiaGfzfM&ab_channel=TomorrowUnlocked

MARK T. HOFFMAN | TED - “The Psychology of Cybercrime”:
www.ted.com/talks/mark_t_hoffmann_profiling_hackers_the_psychology_of_cybercrime

ALESSIO PENNASILICO | TED - “Perché dovresti preoccuparti di Cybersecurity”:
www.ted.com/talks/alessio_pennasilico_perche_dovresti_preoccuparti_di_Cybersecurity

CORRADO GIUSTOZZI | TEDxTalks - “Il lato oscuro dell'internet delle cose”:
www.youtube.com/watch?v=IrauF74kGv0&ab_channel=TEDxTalks

RSA Conference 2012 - “Human Hacking Exposed - 6. Preventative Tips That Can Save Your Company”:
www.youtube.com/watch?v=p40fZFAUz6U&ab_channel=SocialEngineerOrg