Università degli Studi di Camerino

Scuola di Scienze e Tecnologie

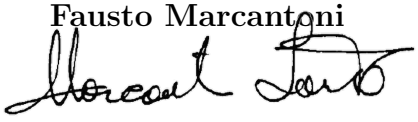
Corso di Laurea in Informatica (Classe L-31)

Studio del Phishing, dei tool e simulazione di una campagna di Phishing

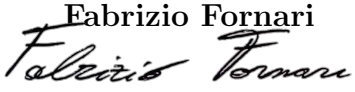
Laureando
Davide Nappo

Matricola 110157

Relatore
Fausto Marcantoni



Correlatore
Fabrizio Fornari



A.A. 2022/2023

Contents

1 Introduzione **13**
- 1.1 Motivazione . . . 13
- 1.2 Obiettivi . . . 13
- 1.3 Struttura della Tesi . . . 14

2 Spazio Cibernetico e Cyber Risk **15**
- 2.1 Definizione di Spazio Cibernetico . . . 15
- 2.2 Attori . . . 16
- 2.3 Tipologie di minacce . . . 16
- 2.4 Cyber Risk . . . 17
- 2.5 Falsi miti . . . 17
- 2.6 Rischi più diffusi . . . 17
- 2.7 Danni causati dal Cyber Risk . . . 18
- 2.8 Gestione del rischio . . . 18

3 Cybersecurity **21**
- 3.1 Definizione di Cybersecurity . . . 21
- 3.2 I 3 componenti della cyber security . . . 21
- 3.3 Storia della cybersecurity . . . 22
- 3.4 Caratteristiche principali della cybersecurity . . . 22
- 3.5 L'importanza della cybersecurity . . . 23
- 3.6 Dati sulla cybersecurity . . . 23
- 3.7 Tipologie di attacchi . . . 25

4 Ingegneria Sociale **27**
- 4.1 Definizione di Ingegneria sociale . . . 27
- 4.2 Meccanismi psicologici alla base dell'ingegneria sociale . . . 27
- 4.3 Tattiche e attacchi di ingegneria sociale . . . 28

5 Phishing **33**
- 5.1 Definizione di Phishing . . . 33
- 5.2 Storia del phishing . . . 34
  - 5.2.1 Le origini . . . 34
  - 5.2.2 L'affermazione e i social media . . . 34
  - 5.2.3 Gli attacchi più famosi . . . 35

5.3 Tipologie di phishing 39
5.4 Attaccanti e vittime 45
5.5 Perchè e quanto il phishing ha successo 47
5.6 Strategie di difesa 49
5.6.1 Strategie generali 49
5.6.2 Strategie specifiche 50

6 Tool Di Phishing **53**
6.1 Elenco dei principali tool di Phishing 53
6.1.1 Gophish 57
6.1.2 PyPhisher 65
6.1.3 PhishInsight 70
6.1.4 Zphisher 81
6.2 Tunneling 85
6.2.1 Cloudflare 87
6.2.2 Ngrok 87
6.2.3 LocalXpose 89

7 Esperimento di Phishing **91**
7.1 Fasi di un esperimento di Phishing 91
7.2 Esempio di un esperimento di phishing 92

8 Conclusioni e Sviluppi Futuri **97**

Listings

List of Figures

2.1 Rappresentazione insiemistica del cyberspazio. [12] 15

3.1 Grafico Clusit della distribuzione delle tecniche di attacco nel 2022 [14] . 23
3.2 Grafico Clusit tecniche di attacco in Italia nel 2022 [14] 24
3.3 Grafico Clusit delle vittime in Italia nel 2022 [14] 24
3.4 Grafico Clusit tipologie e distribuzione attaccanti 2022 [14] 25

5.1 Esempio di email di phishing inviata durante la FifaWorldCup2018. Esempio di messaggi con biglietti e viaggi omaggio [38] 38
5.2 Esempio di email di phishing inviata durante la FifaWorldCup2018. Esempio di notificazione fake con allegati.[38] 38
5.3 Esempio di email molto generica di phishing, creata attraverso un tool. . 40
5.4 Esempio di phishing generico via email. Da notare come l'indirizzo email sospetto di ritorno, non abbia nulla a che fare con Netflix.[23] 40
5.5 Esempio di Spear Phishing. Sono evidenziate l'indirizzo email utilizzato, il link malevolo e la frase comune finale usata per far apparire il messaggio come leggittimo.[63] 41
5.6 Immagine che riassume brevemente le differenze tra Phishing, SpearPhishing e Whaling.[34] 43
5.7 Esempio di Smishing basato su una presunta attività inusuale nell'account Apple. [1] 45

6.1 Uno screen del codice sorgente di Gophish. 57
6.2 Pagina di Login di Gophish 58
6.3 Home Page di Gophish 58
6.4 Creazione del profilo con cui verranno inviate le email di phishing su Gophish. 59
6.5 Esempio di email di test generata da Gophish 60
6.7 Template Reference di Gophish 60
6.6 Schermata di modifica di un' email su Gophish 61
6.8 Schermata di modifica di una landing page su Gophish 62
6.9 Campi da compilare per aggiungere utenti e gruppi su Gophish. 63
6.10 Campi da compilare per creare una nuova campagna di Gophish. 64
6.11 Dashboard di Gophish in cui è possibile vedere l'andamento della campagna di phishing ed eventuali dati sulle vittime. 64
6.12 Schermata di avvio di PyPhisher 66

6.13 Schermata di esecuzione del tool. 66
6.14 Schermata di esecuzione del tool. In questa immagine è possibile vedere la creazione del link della pagina di phishing 67
6.15 Pagina di phishing con template basato sulla login page di Instagram. . 68
6.16 Pagina di phishing con template basato sulla pagina dell'autenticazione a 2 fattori di Instagram. 68
6.17 Pagina reale di Instagram su cui viene reindirizzata la vittima. 68
6.18 Credenziali catturate. Nella foto vengono censurati alcuni dati della vittima. 69
6.19 File di testo su cui vengono salvate le credenziali e il codice OTP. 69
6.20 Lista degli email template presenti su PhishInsight con testo in inglese. 70
6.21 Lista degli email template presenti su PhishInsight con testo in italiano. 71
6.22 Email template di tentato accesso all'account Facebook. 71
6.23 Schermata di modifica di un template email su PhishInsight. 72
6.24 Landing page di Facebook. 72
6.25 Dati da compilare per aggiungere un utente alla user list su PhishInsight. 73
6.26 Dati da compilare per creare un nuovo gruppo ed aggiungervi uno user su PhishInsight. 73
6.27 Prima parte dei dati da inserire per avviare una campagna con PishInsight. 74
6.28 Seconda parte dei dati da inserire per avviare una campagna con PishInsight. 75
6.29 Email di pishing della campagna avviata, presente come template in PishInsight. 75
6.30 Landing page di Facebook della campagna avviata, presente come template in PishInsight. La vittima arriva qui dopo aver clickato il link presente nell'email. 76
6.31 Messaggio a cui l'utente viene reindirizzato dopo essere caduto vittima della simulazione di phishing. 76
6.32 Dashboard di PhishInsight che mostra i dati sulla campagna di phishing avviata. 77
6.33 Alcuni dei moduli di allenamento presenti su PhishInsight. 78
6.34 Esempio di modulo di allenamento sul phishing presente su PhishInsight. 79
6.35 Esempio di modulo di allenamento sul phishing presente su PhishInsight. Attraverso la gamification è possibile spronare i dipendenti all'apprendimento. 80
6.36 Moduli di allenamento di PhishInsight in italiano sul phishing. 80
6.37 Installazione di Zphisher su una macchina virtuale con sistema operativo Kali Linux. 82
6.38 Schermata di avvio di Zphisher. 82
6.39 Zphisher in esecuzione. In questa Figura viene chiesto all'utente come esso desideri far apparire la pagina fake scelta in precedenza, in locale o su rete internet globale. 83
6.40 Esempio del servizio di tunneling offerto da Zphisher. Il tool inizializza un server PHP sul localhost:8080 e lo rende visibile su rete internet globale. 84
6.41 Esempio di "customizzazione" dell'url con Zphisher. 84
6.42 Template di una pagina di login fake di Paypal fornita da Zphisher. . . 85

6.43 Esempio di funzionamento del tunneling [17]. 86
6.44 Esempio di funzionamento di ngrok [41]. 89
6.45 Esempio di funzionamento di LocalXpose[36]. 90

7.1 Esempio di email realizzata per la campagna di phishing. 93
7.2 Esempio di landing page realizzata per la campagna di phishing. 94
7.3 Esempio della dashboard intuitiva di Gophish in cui sono contenute le varie informazioni riguardanti la Campagna effettuata. 94

List of Tables

6.1 Tabella riassuntiva di alcuni dei principali tool di phishing. 56

1. Introduzione

La tecnologia ha cambiato radicalmente il modo in cui viviamo e lavoriamo, introducendo una vasta gamma di vantaggi senza precedenti, ma anche una serie di rischi sempre più complessi e pericolosi. In particolare, la crescente dipendenza dalle tecnologie digitali ha portato ad un aumento dei cosiddetti "cyber risk", ovvero i rischi derivanti dall'utilizzo di sistemi informatici e di telecomunicazione e, in questo contesto, la cybersecurity si presenta come una delle principali sfide del nostro tempo, rappresentando una questione di importanza critica per le imprese, le istituzioni e i cittadini di tutto il mondo. Il cyber spazio, ovvero l'ambiente digitale in cui avvengono le attività online, è diventato un luogo dove si concentrano numerose minacce e vulnerabilità, che, possono causare danni ingenti a livello economico, politico e sociale. Tra i vari pericoli spicca il phishing, che, nell'era digitale in cui viviamo, rappresenta una minaccia sempre più diffusa e pericolosa che sfrutta l'inganno per ottenere informazioni sensibili, come password, dati finanziari e personali.
Nel Capitolo 1 saranno illustrate prima le motivazioni che hanno spinto a perseguire l'obiettivo descritto e quindi la struttura della tesi.

1.1 Motivazione

La lotta contro il phishing richiede uno sforzo collettivo, coinvolgendo utenti consapevoli, aziende attente e legislazioni adeguate. La presente tesi si propone di contribuire a questa causa, sensibilizzando sul tema, promuovendo la consapevolezza e offrendo strumenti per contrastare con successo questa minaccia sempre crescente nella società digitale odierna.

1.2 Obiettivi

La lotta contro il phishing richiede uno sforzo collettivo, coinvolgendo utenti consapevoli, aziende attente e legislazioni adeguate. La presente tesi si propone di contribuire a questa causa, sensibilizzando sul tema, promuovendo la consapevolezza, analizzando e testando i principali tool di phishing in commercio utilizzati dagli attaccanti, fornendo consigli e un esempio di realizzazione di una campagna di phishing e offrendo strumenti per contrastare con successo questa minaccia sempre crescente nella società digitale odierna.

1.3 Struttura della Tesi

Inizialmente nei Capitoli 2, 3 e 4 verranno fornite alcune nozioni base indispensabili su argomenti quali cyberrisk, cyberspazio, cybersecurity e ingegneria sociale per comprendere appieno la tipologia di attacco protagonista di questa tesi. Attraverso una ricerca approfondita e l'analisi di casi studio, nel Capitolo 5, dopo aver dato una definizione del fenomeno, verranno poi esplorate le diverse tipologie di phishing, tra cui phishing via email, spear phishing, whaling, vishing e pharming. Saranno presi in considerazione anche gli sviluppi recenti nel campo del phishing, come il phishing mobile. Un aspetto importante affrontato in questa tesi riguarda, inoltre, le strategie di prevenzione e le contromisure che possono essere adottate per contrastare efficacemente gli attacchi di phishing. Saranno esaminate le best practice di sicurezza informatica, le politiche di consapevolezza degli utenti e l'implementazione di soluzioni tecnologiche per rilevare e mitigare il phishing. Nel Capitolo 6 il focus sarà invece sull'analisi e il test di alcuni tool di phishing, fino a porre le basi per la realizzazione di una campagna di phishing effettuata nel Capitolo 7. Infine, nel Capitolo 8 saranno fornite alcune considerazioni riguardanti le conclusioni e gli sviluppi futuri.

2. Spazio Cibernetico e Cyber Risk

Prima di addentrarsi nel mondo del phishing è fondamentale spendere qualche parola per capire il contesto e alcune nozioni base. L'obiettivo di questo capitolo, in particolare, è fornire un background su spazio cibernetico e cyber risk, mentre nei Capitoli 3 e 4 l'attenzione sarà su cybersecurity e ingegneria sociale.

2.1 Definizione di Spazio Cibernetico

Si definisce spazio cibernetico "l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi" (decreto del presidente del Consiglio dei ministri 24 Gennaio 2013) [40] . Lo spazio cibernetico, come mostrato in Figura 2.1 rappresenta un nuovo dominio che si colloca trasversalmente agli altri 4 domini già conosciuti: terrestre, aereo, marittimo, spaziale. Esso è un ambiente creato dall'uomo, virtuale, senza confini, caratterizzato da uno spazio indefinito ed in continua evoluzione. Tale spazio è però caratterizzato da criticità e vulnerabilità che possono essere sfruttate da vari attori e con diversi tipi di approcci e minacce.

Figure 2.1: Rappresentazione insiemistica del cyberspazio. [12]

2.2 Attori

Alcuni attori generalmente coinvolti nello sfruttamento di criticità e vulnerabilità sono[7]:

- **HACKTIVIST.**
  Si tratta di individui o gruppi che utilizzano le proprie abilità informatiche per sostenere una causa politica o sociale. Gli hacktivist spesso attuano attacchi informatici a siti web e reti informatiche di organizzazioni o governi che ritengono violino i diritti umani o l'etica.

- **INSIDER.**
  Sono individui che hanno accesso autorizzato ai sistemi informatici e possono commettere atti illeciti all'interno dell'organizzazione. Gli insider possono essere dipendenti, ex dipendenti o fornitori di servizi esterni che hanno accesso alle reti informatiche dell'organizzazione.

- **BOTNET OPERATOR.**
  Si tratta di individui che controllano una rete di computer infetti (botnet) e la utilizzano per attacchi informatici, come ad esempio il lancio di attacchi DDoS per sovraccaricare i siti web.

- H**ACKER GOVERNATIVI.**
  Sono individui che lavorano per un governo e utilizzano le loro abilità informatiche per condurre attività di spionaggio informatico o per effettuare attacchi informatici contro obiettivi specifici di interesse nazionale.

2.3 Tipologie di minacce

Alcune tipologie di minacce che vedono coinvolti gli attori precedentemente descritti sono[5]:

- **GUERRA CIBERNETICA (CYBER – WARFARE).**
  La guerra cibernetica consiste nell'utilizzo di tecnologie informatiche per condurre operazioni militari e di intelligence durante conflitti armati.

- **SPIONAGGIO CIBERNETICO (CYBER-ESPIONAGE).**
  Lo spionaggio cibernetico è l'attività che sfrutta le potenzialità della rete per rubare segreti industriali, con l'obiettivo di ottenere un vantaggio competitivo nel mercato dei brevetti civili o di acquisire una superiorità strategica attraverso la sottrazione di disegni e apparecchiature militari o dual-use.

- **CRIMINALITA' CIBERNETICA (CYBER –CRIME).**
  Operazioni illegali che avvengono nello spazio cibernetico, come truffe, frodi telematiche, furto d'identità, sottrazione indebita di informazioni, pornografia infantile e altro ancora.

- **TERRORISMO CIBERNETICO (CYBER-TERRORISM).**
  Il terrorismo cibernetico rappresenta l'utilizzo della rete da parte di gruppi terroristici per effettuare attacchi informatici, ideologicamente motivati, con l'obiettivo di colpire target sensibili come il settore creditizio, le infrastrutture militari, i sistemi di controllo dei servizi di pubblica utilità e i mezzi di informazione. È importante sottolineare che il concetto di cyberspazio è strettamente legato a

quello di cyber risk e cybersecurity, poiché le minacce descritte possono avere conseguenze estremamente gravi per la sicurezza e la stabilità degli Stati, delle organizzazioni e delle persone.

2.4 Cyber Risk

Il cyber risk o rischio informatico, secondo l'Institute of Risk Management (IRM), rappresenta[47]: "qualsiasi rischio di perdita finanziaria, distruzione o danno alla reputazione di un'organizzazione dovuto a un malfunzionamento del sistema informativo". La gestione della sicurezza dei dati di un'impresa, di un privato o di una pubblica amministrazione è fondamentale per garantire la protezione del proprio patrimonio informativo e dei dati aziendali, diventando quindi una priorità per qualsiasi imprenditore o start-up che voglia competere nel mercato di internet. Solo attraverso una pianificazione preventiva, con l'aiuto di professionisti esperti, è possibile proteggere i dati, le informazioni, le transazioni finanziarie, l'utilizzo di app e sistemi informatici da eventuali attacchi informatici. Il tema del cyber risk è di cruciale importanza nel processo di analisi e riduzione dei rischi aziendali, specialmente in un contesto dove sempre più tecnologie e modelli di business sono basati sulla rete, che rende la gestione del cyber risk management essenziale per garantire la sopravvivenza stessa dell'impresa.

2.5 Falsi miti

In Italia esiste il falso mito secondo il quale il nostro paese sia uno dei più sicuri in materia di Cyber Risk. Tuttavia, la realtà è che il nostro Paese è uno dei più a rischio secondo i rapporti del Clusit (Associazione Italiana per la sicurezza informatica), e le perdite economiche dovute a eventi Cyber sono in continua crescita[8]. Inoltre, non è vero che solo le grandi aziende sono a rischio. In realtà, le piccole imprese sono le più colpite, poiché spesso gestiscono il rischio in modo approssimativo e con budget limitati. Questo le rende più vulnerabili e sempre più soggette ad attacchi massivi rispetto agli attacchi mirati alle grandi imprese. Non bisogna pensare che la propria azienda sia al sicuro dal Cyber Risk, in quanto anche le imprese più preparate possono essere colpite da errori umani, come dimostrato dalla diffusione del Cryptolocker (malware che blocca i documenti presenti nel computer, criptandoli con una password e rendendo impossibile aprire i file). Molti pensano che basti un backup giornaliero dei dati per proteggere la propria azienda, ma purtroppo i danni causati da fermo attività e le spese per la ricostruzione delle banche dati possono essere molto rilevanti. Non bisogna sottovalutare i danni causati dal Cyber Risk. Se dovesse verificarsi una perdita di informazioni importanti o una divulgazione di dati riservati, ci sarebbero interruzioni dell'attività, richieste di risarcimento da parte di terzi e danni reputazionali difficilmente quantificabili.

2.6 Rischi più diffusi

Ci sono diversi tipi di minacce in ambito Cyber Risk che possono danneggiare un'azienda [10]. Tra questi, i rischi più diffusi sono:

- **Errore umano:** spesso i dipendenti commettono errori involontari come l'apertura

di e-mail o il download di file infetti, che possono aprire la strada a virus e malware.

- **Eventi accidentali:** sbalzi di tensione o problemi all'impianto di climatizzazione della sala server possono compromettere il sistema informatico.
- **Azione dolosa di terzi:** hacker, dipendenti malintenzionati o attacchi di ransomware possono causare danni significativi alla sicurezza informatica dell'azienda.

In generale, ogni dispositivo che l'azienda utilizza, come PC, server e dispositivi mobili, può rappresentare una potenziale porta d'accesso per le minacce informatiche. È importante che le aziende adottino le giuste misure di sicurezza e formazione dei dipendenti per prevenire e mitigare il Cyber Risk.

2.7 Danni causati dal Cyber Risk

I danni causati dal Cyber Risk possono essere diretti e materiali ai sistemi elettronici e informatici, ma anche da interruzione di attività, richieste di risarcimento danni da parte di terzi, danno reputazionale e perdita di clienti e fornitori, e costi emergenti per servizi professionali[18]. Per questo motivo, è importante che le aziende adottino politiche di sicurezza informatica adeguate e formino i propri dipendenti per gestire il Cyber Risk in modo efficace. Solo così si potrà minimizzare il rischio e proteggere l'attività aziendale.

2.8 Gestione del rischio

La prevenzione, la protezione, la formazione e l'assicurazione sono componenti importanti nella gestione dei rischi informatici[6].

- **Prevenzione:** La prevenzione è un aspetto cruciale per evitare le minacce informatiche. Ciò include l'implementazione di misure di sicurezza tecniche, come firewall, sistemi di rilevamento delle intrusioni e crittografia dei dati. Inoltre, è importante mantenere aggiornati i sistemi e il software con le ultime patch di sicurezza e adottare politiche di accesso e autenticazione robuste.
- **Protezione:** La protezione dei sistemi e dei dati sensibili è fondamentale per mitigare i rischi informatici. Ciò implica l'adozione di controlli di sicurezza adeguati, come l'uso di password complesse, la gestione dei privilegi di accesso, l'uso di crittografia e la sicurezza fisica dei dispositivi. È inoltre consigliabile implementare soluzioni di backup regolari per proteggere i dati da perdite o danni.
- **Formazione:** La formazione è essenziale per sensibilizzare e responsabilizzare le persone riguardo alla sicurezza informatica. I dipendenti devono essere informati sulle minacce comuni, come il phishing e le frodi informatiche, e istruiti su come riconoscerle ed evitarle. La formazione dovrebbe includere anche le migliori pratiche per la gestione delle password, l'utilizzo sicuro dei dispositivi e l'adozione di comportamenti sicuri online.
- **Assicurazione:** L'assicurazione contro i rischi informatici è diventata sempre più importante per le organizzazioni. Le polizze di assicurazione cibernetica offrono

una copertura finanziaria in caso di violazione dei dati, attacchi informatici o interruzioni del servizio. Queste polizze possono coprire i costi di risposta agli incidenti, ripristino dei dati, responsabilità civile e perdite finanziarie. L'assicurazione cibernetica può essere considerata come un complemento alle altre misure di prevenzione e protezione.

In sintesi, la prevenzione, la protezione, la formazione e l'assicurazione sono elementi chiave per gestire i rischi informatici in modo efficace. Implementare misure di sicurezza tecniche, educare il personale sulla sicurezza informatica, adottare politiche e procedure solide e valutare la copertura assicurativa possono contribuire a ridurre l'impatto dei rischi informatici e garantire la continuità operativa dell'organizzazione.

3. Cybersecurity

Questo capitolo si concentra sulla cybersecurity e sul ruolo critico che essa gioca nella protezione delle informazioni digitali. Qui ne viene data una definizione e ne vengono spiegate le caratteristiche, i dati e le principali minacce che costituiscono una sfida per la sicurezza informatica e per tutti gli esperti del settore. Conoscere la cybersecurity aumenta anche la consapevolezza nei confronti del fenomeno del phishing.

3.1 Definizione di Cybersecurity

Il termine "cybersecurity" o "sicurezza informatica" fa riferimento alla combinazione di strumenti, principi e processi finalizzati alla tutela delle risorse informatiche, come le reti e i dati degli utenti, da possibili minacce[20]. Affinché sia efficace, la cybersecurity richiede l'adozione di misure di sicurezza basate su tre elementi fondamentali: le persone, i processi e la tecnologia. Questo approccio tripartito consente alle organizzazioni di proteggersi da attacchi specializzati, nonché da minacce interne comuni, come la violazione accidentale di dati o gli errori umani.

3.2 I 3 componenti della cyber security

- **Persone.**
  Le persone sono un componente essenziale della cybersecurity e ogni dipendente dell'organizzazione deve essere consapevole del proprio ruolo nella prevenzione e riduzione delle minacce informatiche. Inoltre, il personale tecnico specializzato nella sicurezza informatica deve essere costantemente aggiornato per essere in grado di rispondere agli attacchi informatici di ultima generazione.

- **Processi.**
  I processi sono altrettanto importanti nella cybersecurity poiché definiscono come le attività, i ruoli e i documenti dell'organizzazione sono interconnessi tra loro, con l'obiettivo finale di mitigare i rischi della sicurezza delle informazioni. I processi devono essere costantemente rivisti e aggiornati per potersi adattare e adeguare alle minacce informatiche in costante evoluzione.

- **Tecnologia.**
  Infine, la tecnologia rappresenta un altro componente essenziale della cybersecurity. L'analisi dei rischi informatici che l'organizzazione corre è il punto di partenza per determinare i controlli e le misure di sicurezza da implementare per proteggere l'azienda. Le tecnologie possono essere utilizzate per prevenire o ridurre l'impatto di tali rischi, tenendo conto delle conclusioni tratte dalla valutazione dei rischi aziendali e del livello accettabile di rischio.

3.3 Storia della cybersecurity

Nel settore si tende a far coincidere la nascita dei primi strumenti di sicurezza informatica con la comparsa dei primi virus e delle prime minacce. Il primo virus in assoluto, Creeper, fu creato nel 1971 per funzionare su ARPANET, il progenitore di Internet, ma era un codice completamente innocuo. Il primo virus che ha fatto danni seri è stato il trojan PC-Write nel 1986, anno in cui è stato anche scoperto Marcus Hess, l'hacker tedesco che rubava dati dalle reti americane per rivenderli al KGB[32].

Per questo motivo, possiamo dire che la cybersecurity è nata nel 1986, in risposta alle prime minacce globali che i governi di allora non potevano più ignorare (una delle prime misure di sicurezza fu la creazione di un honeypot,che in inglese significa letteralmente "barattolo di miele", termine che viene utilizzato metaforicamente per indicare i sistemi informatici progettati per attirare i cybercriminali, così come un vasetto di miele attirerebbe un orso goloso[56]).

3.4 Caratteristiche principali della cybersecurity

La triade CIA (Confidentiality, Integrity, Availability) rappresenta i principi che reggono tutte le attività di cybersecurity, ovvero riservatezza, integrità e disponibilità dei dati e dei sistemi informatici[27]. Questi sono i principi alla base di tutte le attività di cybersecurity, perché l'obiettivo finale è garantire che dati e sistemi siano sempre:

- **Accessibili** solo alle persone autorizzate.
- **Completi**, ovvero che non ne vengano perse o distrutte porzioni.
- **Disponibili**, ovvero utilizzabili in qualsiasi momento.

Inoltre, il NIST (National Institute of Standards and Technology) nel 2018 ha definito delle linee guida[27] con l'obiettivo di creare un riferimento standardizzato e comune a livello globale per la gestione della sicurezza informatica che si basano su 5 funzioni principali:

- **Identificare:** comprendere l'ambiente informatico, i processi, i dati e gli asset coinvolti e suscettibili ad attacchi.
- **Proteggere:** implementare misure di protezione come la crittografia, il controllo degli accessi, le policy di sicurezza, i firewall e altri strumenti di sicurezza.
- **Rilevare:** implementare sistemi di rilevamento delle intrusioni, delle infezioni e altre attività illecite, per identificare eventuali violazioni di sicurezza in modo tempestivo e poter rispondere prontamente.
- **Rispondere:** sviluppare piani d'azione, procedure e processi per rispondere agli eventi critici di sicurezza, come gli attacchi informatici, per minimizzare i danni e ripristinare la sicurezza dell'ambiente informatico.
- **Ripristinare:** definire strategie e strumenti per il ripristino efficiente ed efficace dell'operatività del sistema e dei dati in generale dopo un evento critico.

3.5 L'importanza della cybersecurity

La protezione dei dati e dei sistemi informatici è di estrema importanza per garantire la privacy e la sicurezza delle informazioni sensibili degli utenti, come dati personali e finanziari, informazioni commerciali e proprietarie, e così via. In caso di violazione di queste informazioni, le conseguenze possono essere devastanti per l'organizzazione e per i suoi clienti, con potenziali danni finanziari, reputazionali e legali. Infine, avere una forte sicurezza informatica può aiutare a mantenere la fiducia dei clienti e degli utenti, che sono sempre più consapevoli dei rischi legati alla sicurezza informatica e scelgono di fare affari solo con organizzazioni che dimostrano di proteggere adeguatamente i loro dati e le loro informazioni[59].

3.6 Dati sulla cybersecurity

La cybersecurity è diventata un tema di crescente importanza a livello globale e nazionale. La digitalizzazione delle attività quotidiane e degli affari ha portato a un aumento delle minacce online, creando la necessità di adeguati protocolli di sicurezza informatica. Secondo il "Global Risks Report 2021" del World Economic Forum [31], il rischio di attacchi informatici e di frodi online è in costante aumento. Il rapporto sottolinea inoltre come il COVID-19 abbia accelerato la digitalizzazione di molte attività, aumentando la necessità di rafforzare la sicurezza informatica. Il Clusit (Associazione Italiana per la Sicurezza Informatica) è una delle principali organizzazioni italiane che si occupano di sicurezza informatica. Clusit pubblica regolarmente rapporti, studi e analisi sulle minacce informatiche, le tendenze e le best practice in materia di sicurezza. Il rapporto Clusit del 2023 [8] evidenzia un peggioramento nel trend di attacchi mondiali specificando che dai 1554 attacchi gravi censiti nel 2018 si è passati ai 2489 del 2022 con un aumento del 60% e che l'Italia è stata bersaglio del 7,6% di questi attacchi mondiali guadagnando un triste +168% rispetto al 2021 e al 2022.

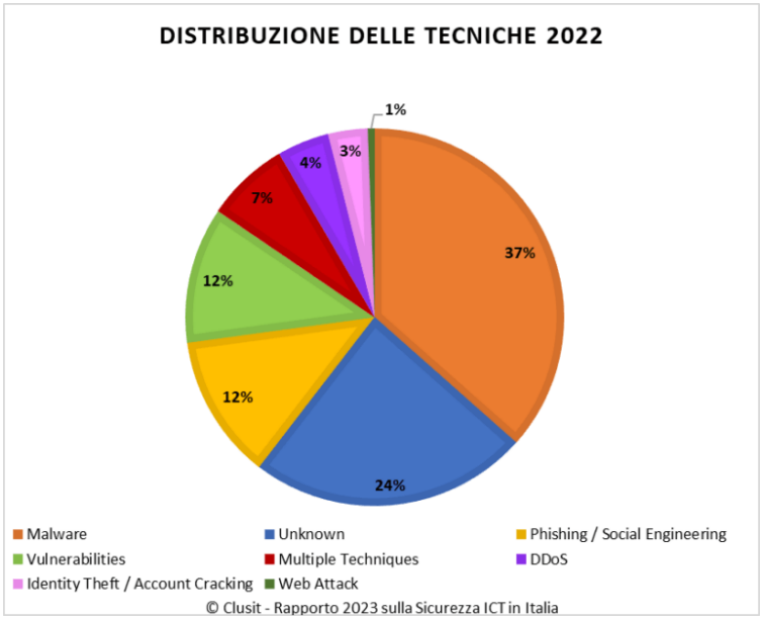


Figure 3.1: Grafico Clusit della distribuzione delle tecniche di attacco nel 2022 [14]

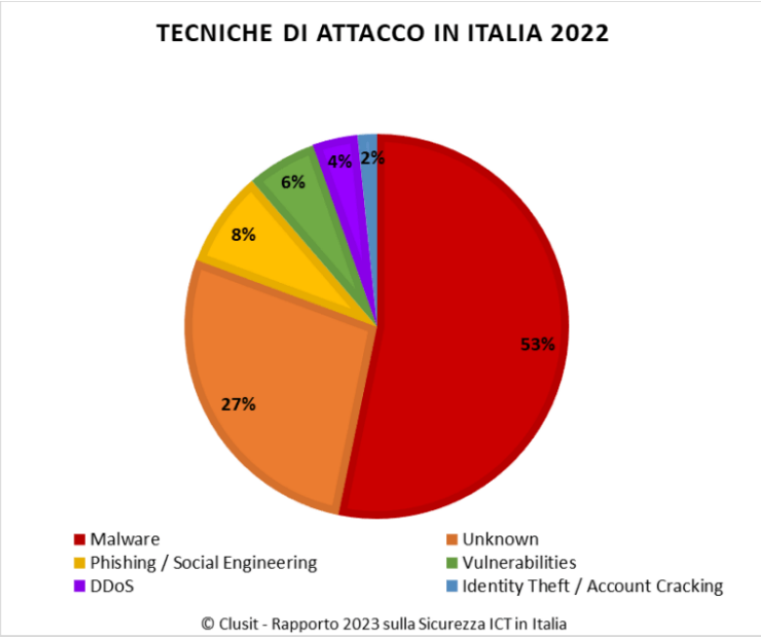


Figure 3.2: Grafico Clusit tecniche di attacco in Italia nel 2022 [14]

Analizzando i due grafici contenuti nelle Figure 3.1, e 3.2 possiamo notare quali siano le minacce più comuni in Italia e nel mondo: Malware, l'uso di tecniche ancora sconosciute, l'ingegneria sociale e il phishing.

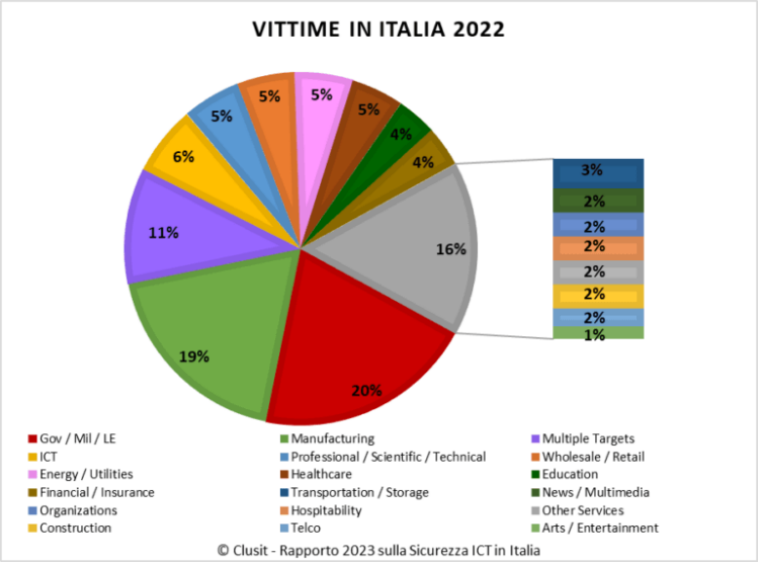


Figure 3.3: Grafico Clusit delle vittime in Italia nel 2022 [14]

Nel grafico in Figura 3.3 vengono evidenziati i tipi di azienda più colpiti in Italia nel 2022, mostrando come le aziende governative e il settore manifatturiero risultino i più bersagliati da attacchi informatici.

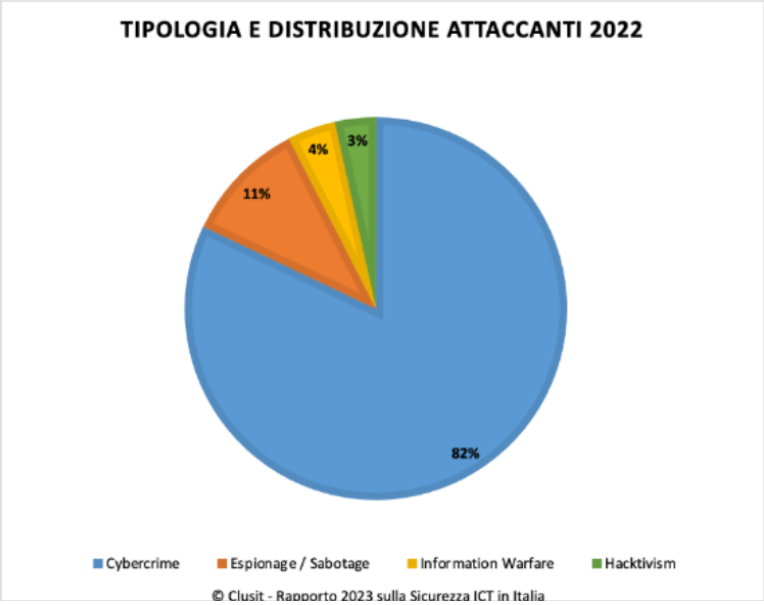


Figure 3.4: Grafico Clusit tipologie e distribuzione attaccanti 2022 [14]

In quest'ultimo grafico, contenuto nella Figura 3.4 vengono evidenziati invece la distribuzione e la tipologia di attaccanti. Questo grafico mette in luce come la tipologia di attacco più comune sia quella della cybercrime, volta a estorcere denaro e informazioni ai malcapitati.
Da tutti questi dati si evince come la cybersecurity rappresenti un tema di crescente importanza a livello internazionale e nazionale, con una crescente consapevolezza della necessità di adeguati protocolli di sicurezza informatica. La digitalizzazione delle attività quotidiane e degli affari ha portato a un aumento delle minacce online, rendendo necessaria una costante attenzione e investimenti nella protezione delle informazioni online.

3.7 Tipologie di attacchi

In questo paragrafo, saranno descritte alcune delle tipologie di attacchi più diffuse[60], fino ad arrivare all'ingegneria sociale, alla quale è dedicato un capitolo a parte, il 4, poiché alla base del phishing, l'argomento di questa tesi.

- **Malware.**
  La definizione di malware deriva dalla combinazione di due parole: malicious (malevolo) + software = malware. Il malware è un software progettato per agire contro gli interessi del proprietario di un sistema o un dispositivo, e, una volta penetrato, si installa eseguendo il proprio codice. Esistono varie tipologie di malware e gli effetti causati sono più o meno gravi. Virus, worm e trojan sono categorie di malware che prendono il nome da come si diffondono. Altri malware invece prendono il nome da quello che fanno: spyware, adware, keylogger, backdoor, ransomware, rootkit, dialer. Alcuni dei più famosi sono:

  – **Virus** Il virus è un programma scritto per introdursi e riprodursi nel pc del malcapitato, alterare e modificare i dati presenti. Vari tipi di virus sono[43]:

    - **Virus dei file:** infetta solitamente i file di programma con estensioni come .exe, .com e .bat. Una volta attivo, si diffonde rapidamente a tutti i programmi caricati.
    - **Virus delle macro:** Un altro tipo di virus è quello delle macro, che si insinua nei file di dati di programmi come Word, Excel, PowerPoint e Access, rendendoli estremamente difficili da riparare.
    - **virus MBR (Master Boot Record):** sono una categoria di virus che si insediano in memoria e si replicano nel primo settore di un dispositivo di archiviazione, dove sono memorizzate le tabelle di partizione e i programmi di avvio del sistema operativo[9]. Questo tipo di virus infetta l'area di avvio del dispositivo di archiviazione anziché i normali file. La rimozione del virus MBR può essere effettuata eliminando l'intera area di memoria in cui si è insediato il virus, ovvero l'area MBR.

- **Adware** Software malevoli che, una volta installati, causano un eccesso di pop-up e annunci pubblicitari rallentando vistosamente il dispositivo del malcapitato. Gli sviluppatori degli adware guadagnano mediante la visualizzazione automatica di pubblicità online nell'interfaccia utente del software o su una schermata che compare durante il processo di installazione. L'adware inoltre può anche tenere traccia delle attività dell'utente, spiandolo, in modo da fornire il tipo di pubblicità più appropriata. I primi adware risalgono al 1995 circa, inseriti all'interno di spyware, ma, gli anni di proliferazione maggiore furono quelli a cavallo tra il 2005 e il 2008. Per reprimere il fenomeno molti browser hanno poi iniziato ad introdurre adblocker e plugin adblock provocando però in alcuni casi anche una perdita per quei siti web che fanno uso di pubblicità legittime. Per difendersi dagli adware è utile avere un antivirus installato sul proprio dispositivo con cui eseguire scansioni quotidiane e evitare di lasciarsi prendere dalla curiosità andando su siti potenzialmente pericolosi.
- **Ransomware** Si tratta di una tipologia di malware molto pericolosa ma dal funzionamento piuttosto semplice, limita l'accesso al dispositivo infettato richiedendo un pagamento (spesso in Bitcoin) per poter essere rimosso. Il primo caso di ransomware fu il trojan Aids scritto dal biologo Joseph Popp, risalente al 1989, il quale seguiva un payload e mostrava una schermata all'utente in cui compariva un messaggio di scadenza di un software installato, criptava i file dell'hard disk e poteva essere rimosso solo con il pagamento di un riscatto di 189 dollari da parte dell'utente, i soldi furono poi devoluti da Popp alla ricerca per la cura all'Aids. Ci sono due tipi principali di ransomware:
    - **Cryptor:** criptano i file contenuti nel dispositivo rendendoli inaccessibili.
    - **Blocker:** bloccano l'accesso al dispositivo infettato [44].

Queste sono solo alcune delle tipologie di attacchi più comuni presenti sulla rete. Nel capitolo successivo viene approfondita l'ingegneria sociale, metodologia alla base di svariati tipi di attacchi, tra cui il Phishing, l'argomento principale di questa tesi.

4. Ingegneria Sociale

In questo capitolo finale, tra quelli riguardanti alcune nozioni fondamentali, l'attenzione è rivolta sull'ingegneria sociale, meccanismo alla base del phishing.

4.1 Definizione di Ingegneria sociale

L'ingegneria sociale viene anche definita "hacking umano" e consiste nell'attuazione di tecniche di persuasione ai danni di una vittima per indurla con l'inganno a condividere informazioni sensibili. È una pratica allettante per tutti i criminali informatici in quanto consente loro di risparmiare tempo ed evitare un lavoro tecnico complesso per aggirare ad esempio eventuali misure di sicurezza informatica. La formazione del personale sui rischi risulta dunque fondamentale nel contesto di attacchi di questo tipo. "L'ingegneria sociale è ogni atto tendente a influenzare una persona, per spingerla ad intraprendere un'azione che non necessariamente è nel suo miglior interesse" [22].

4.2 Meccanismi psicologici alla base dell'ingegneria sociale

I meccanismi psicologici utilizzati dagli attaccanti nel contesto dell'ingegneria sociale sono molteplici e pericolosi[50], alcuni sono:

- **Scarsità:** Molte cose sono considerate valevoli quando sono rare o disponibili per un tempo limitato. L'attaccante può affermare che un'offerta è disponibile solo per un periodo limitato o che una risorsa desiderata sta per esaurirsi per indurre le persone a fornire informazioni o a compiere azioni rapide, inducendo un senso di urgenza.

- **Unità:** Un meccanismo psicologico attraverso il quale la vittima condivide la propria identità con l'attaccante, si instaura un rapporto di unità, di condivisione.

- **Reciprocità:** Spacciare un'azione malevola come un atto di generosità in modo da instaurare fiducia nella vittima. Ad esempio informare la vittima che c'è stato un accesso malevolo al proprio account e deve dunque cambiare le proprie credenziali.

- **Autorità:** Gli attaccanti cercano di presentarsi come figure di autorità o professionisti affidabili per convincere le persone a fare ciò che desiderano. Possono utilizzare uniformi, titoli professionali, nomi di organizzazioni rispettabili o utilizzare il nome di figure di alto profilo per ottenere fiducia e indurre alla cooperazione.

- **Consistenza:** Fare leva sul desiderio delle persone di rimanere coerenti alle proprie parole, credenze e azioni; per esempio, ricordare alla vittima che deve rinnovare la password come già fatto altre volte in passato.

- **Empatia:** Gli attaccanti possono cercare di creare un senso di connessione o comprensione emotiva con le loro vittime. Sfruttando l'empatia, possono generare un ambiente di fiducia e convincere le persone a fornire informazioni sensibili o ad aderire alle loro richieste. Ad esempio, un attaccante potrebbe utilizzare una storia emotiva o una situazione difficile per suscitare compassione o simpatia. Possono cercare di instaurare un rapporto di fiducia facendo leva sull'empatia, dimostrando comprensione e supporto per i problemi o le preoccupazioni delle vittime.

4.3 Tattiche e attacchi di ingegneria sociale

In questa sezione vengono riportate le tattiche e gli attacchi di ingegneria sociale[24], cioè strategie generali utilizzate per convincere le vittime a compiere azioni indesiderate e a fornire informazioni sensibili.

- **Impersonation:** consiste nell'utilizzare una falsa identità per ingannare la vittima e ottenere l'accesso ad aree riservate, a informazioni sull'azienda ecc...

- **Piggybacking o Tailgating:** (in italiano noto come "scroccare" o "infilarsi di straforo") è una tecnica di ingegneria sociale in cui un individuo non autorizzato segue da vicino una persona autorizzata per accedere a un'area sicura o a un sistema informatico protetto. Ad esempio, se un dipendente si sta preparando ad entrare in un'area sicura protetta da un badge di accesso, un piggybacker potrebbe avvicinarsi all'impiegato e chiedere di passare con lui attraverso la porta, fingendo di aver dimenticato il proprio badge. In questo modo, il piggybacker riesce ad accedere all'area protetta senza avere l'autorizzazione. Questa tecnica è particolarmente pericolosa perché consente a individui non autorizzati di accedere a sistemi e dati sensibili senza dover utilizzare alcuna tecnica di hacking. Inoltre, una volta dentro, il piggybacker potrebbe rubare informazioni riservate o danneggiare il sistema. Per prevenire l'accesso non autorizzato alle aree sicure, le organizzazioni dovrebbero adottare misure di sicurezza come la videosorveglianza, l'accesso con badge, l'autenticazione a più fattori e la sensibilizzazione dei dipendenti sui rischi del piggybacking. Inoltre, i dipendenti dovrebbero essere istruiti a non permettere l'accesso a persone sconosciute o non autorizzate e a segnalare eventuali comportamenti sospetti al personale di sicurezza.

- **Shoulder surfing:** in questo tipo di tecnica, il malintenzionato osserva l'utente mentre digita password o altre informazioni riservate. Questo tipo di attacco può essere eseguito da vicino o da lontano, utilizzando teleobiettivi o telecamere nascoste. Ad esempio, un malintenzionato potrebbe posizionarsi dietro un individuo in fila alla cassa di un supermercato e guardare la sua carta di credito mentre viene digitata la password. Per proteggersi dallo shoulder surfing, gli utenti possono adottare alcune misure di sicurezza come coprire la tastiera con le mani durante la digitazione di password, utilizzare filtri privacy per i monitor, evitare di lasciare informazioni su documenti lasciati sulle scrivanie, su post-it o altri fogli, evitare di inserire password in luoghi pubblici o affollati e posizionare i

monitor del computer in modo da limitare la visibilità ad altre persone. Le organizzazioni possono inoltre adottare misure di sicurezza come la sensibilizzazione dei dipendenti sui rischi dello shoulder surfing, l'adozione di politiche di sicurezza per la scelta delle password e l'implementazione di controlli di sicurezza fisica come telecamere di sorveglianza e schermi protettivi per i monitor dei computer.

- **Eavesdropping:** L'eavesdropping è una tecnica di attacco informatico che consiste nell'intercettare e ascoltare le comunicazioni tra due o più parti senza il loro consenso per raccogliere informazioni riservate. L' eavesdropping può essere eseguito utilizzando vari metodi, come l'installazione di software di monitoraggio sui dispositivi di comunicazione delle vittime, l'installazione di dispositivi di intercettazione sulle linee di comunicazione o la creazione di reti Wi-Fi o cellulari fasulle per intercettare le comunicazioni. Per proteggersi dall'eavesdropping, gli utenti possono adottare alcune misure di sicurezza, come utilizzare la crittografia end-to-end per proteggere le comunicazioni, utilizzare connessioni VPN per proteggere le comunicazioni su reti pubbliche, utilizzare protocolli di sicurezza robusti come SSL/TLS, e verificare la presenza di eventuali dispositivi di intercettazione.

- **Dumpster diving:** è una tattica di attacco di ingegneria sociale che consiste nel cercare informazioni sensibili o riservate tra i rifiuti di un'organizzazione o di un individuo. Nella spazzatura si possono trovare una vasta gamma di informazioni sensibili o personali, come ad esempio:

  - Documenti cartacei contenenti informazioni finanziarie o personali, come rapporti bancari, dichiarazioni fiscali, lettere commerciali, moduli di iscrizione, contratti, ecc.
  - Password scritte su carta, dispositivi di archiviazione, o note scritte.
  - Supporti di memorizzazione, come dischi rigidi, unità USB o schede di memoria, che possono contenere dati sensibili o informazioni riservate.
  - Etichette di spedizione o ricevute che possono rivelare informazioni sulle attività dell'organizzazione o sulle abitudini di acquisto dei clienti.
  - Prodotti scaduti o obsoleti, che possono rivelare informazioni sulle strategie di marketing o sugli schemi di produzione dell'organizzazione.
  - Strumenti o apparecchiature obsolete, che possono essere utilizzati per accedere ai dati o alle reti dell'organizzazione.

  Gli attaccanti possono eseguire questa tecnica cercando informazioni tra i rifiuti di un'organizzazione o di un individuo, oppure cercando informazioni nei cassonetti vicino alle sedi dell'organizzazione o alle case degli individui. Possono anche cercare informazioni attraverso il furto di documenti o computer. Per proteggersi dal dumpster diving, le organizzazioni possono adottare alcune misure di sicurezza come la distruzione sicura di documenti e dati sensibili, l'adozione di politiche di sicurezza per la gestione dei rifiuti, l'installazione di videocamere di sorveglianza e il controllo dell'accesso alle aree sensibili. È importante tenere presente che il dumpster diving è spesso considerato una tecnica di attacco illegale e può essere punito dalla legge.

- **Reverse Social Engineering (RSE):** è una tecnica di attacco di ingegneria sociale che inverte il tradizionale flusso dell'attacco. Invece di un attaccante che tenta di convincere un utente a fare qualcosa, un utente può essere convinto

di fare qualcosa senza rendersene conto, causando potenzialmente gravi danni alla sicurezza dell'organizzazione. Nella maggior parte degli attacchi di ingegneria sociale tradizionali, l'attaccante inizia il contatto con la vittima e cerca di convincerla a fornire informazioni o ad eseguire un'azione specifica. Con l'RSE, invece, l'attaccante si finge un dipendente, un rappresentante di un'azienda o un tecnico del supporto IT e contatta la vittima fingendo di aver bisogno di aiuto o informazioni. L'obiettivo dell'RSE è di convincere la vittima a fornire informazioni o eseguire un'azione, senza rendersi conto che sta collaborando con un attaccante. Questo tipo di attacco può essere particolarmente pericoloso perché la vittima potrebbe essere meno attenta o diffidente, poiché crede di parlare con un legittimo rappresentante dell'organizzazione. Gli utenti possono proteggersi dall'RSE adottando alcune misure di sicurezza come l'identificazione dei segnali di allarme e la verifica dell'identità di chi richiede l'accesso o l'informazione prima di fornirla. In generale, l'RSE dimostra l'importanza di educare gli utenti sulla sicurezza informatica e sulle tecniche di attacco di ingegneria sociale, in modo da renderli più consapevoli e attenti alle minacce potenziali.

- **Watering Hole:** L'attacco watering hole è una tattica sofisticata utilizzata dai criminali informatici per compromettere i sistemi informatici di un determinato gruppo di utenti mirati. Questo tipo di attacco prende il nome dal comportamento degli animali selvatici che si radunano presso un punto di abbeveraggio comune, diventando vulnerabili a potenziali predatori. L'attacco watering hole può essere considerato una forma di attacco di ingegneria sociale, infatti, sfrutta la fiducia degli utenti nel visitare siti web legittimi e di fiducia per comprometterli e iniettare codici malevoli e malware. I criminali informatici sfruttano la familiarità degli utenti con i siti web frequentati per far loro abbassare la guardia e interagire con contenuti malevoli o eseguire azioni indesiderate. In questo modo, gli attaccanti sfruttano la componente umana dell'equazione di sicurezza informatica, manipolando le persone anziché attaccare direttamente le vulnerabilità tecnologiche.

- **Quid pro quo:** Il "quid pro quo" è un termine latino che significa "qualcosa in cambio di qualcos'altro". In contesto di sicurezza informatica, il quid pro quo è una forma di attacco di ingegneria sociale in cui un aggressore offre qualcosa di valore o un favore in cambio di informazioni o accesso non autorizzato. Un esempio comune di attacco quid pro quo è quando un aggressore si fa passare per un tecnico informatico o un addetto al supporto e contatta una potenziale vittima, offrendo assistenza o soluzione a un problema apparente. In cambio, l'aggressore chiede all'utente di fornire le proprie credenziali di accesso o consentire l'accesso remoto al proprio sistema. L'attacco quid pro quo sfrutta la tendenza delle persone a fidarsi di individui che sembrano offrire aiuto o vantaggi. Tuttavia, dietro l'offerta c'è l'intenzione di ottenere informazioni sensibili o accesso ai sistemi dell'utente per scopi malevoli. Per proteggersi dagli attacchi quid pro quo, è importante adottare alcune misure di sicurezza, come verificare l'identità delle persone che richiedono accesso o richiedono informazioni sensibili. In caso di dubbi, è consigliabile contattare direttamente l'organizzazione o il servizio coinvolto per verificare l'autenticità della richiesta. Inoltre, è importante educare gli utenti sulle possibili minacce e sensibilizzarli sulla pratica di condividere informazioni solo con fonti attendibili e verificate.

E dopo aver fornito un background solido su CyberSpazio, CyberRisk, Cybersecurity,

gli attacchi informatici più comuni e l'ingegneria sociale possiamo finalmente concentrarci su una tipologia di attacco estremamente famosa e basata proprio sull'ingegneria sociale, il Phishing, il vero protagonista di questa tesi.

5. Phishing

5.1 Definizione di Phishing

Prima di addentrarci nel mondo del phishing è opportuno cercare di dare una definizione di phishing come già provato a fare da Elmer Lastdrager nell'articolo: "Achieving a consensual definition of phishing based on a systematic review of the literature". [33]

Prendiamo in considerazione diverse definizioni date dalla letteratura scientifica e informatica: La parola "phishing" ha avuto origine nel 1996. Il termine fu coniato sulla base dell'analogia che i truffatori utilizzavano la posta elettronica come amo da pesca per "pescare" nomi utente, password e altre informazioni sensibili. Si ritiene che l'uso delle lettere "ph" derivi dalla parola "phreaking" [2] ovvero un termine gergale inglese che indica l'attività di chi studia, sperimenta o sfrutta i telefoni, le compagnie e i sistemi telefonici per divertimento, vantaggio personale o curiosità, ricercando falle all'interno della tecnologia che permettano usi non previsti dal sistema.[66]

Secondo l' Oxford University Press (2014), UK [46] il phishing è: "La pratica fraudolenta di inviare e-mail che si presume provengano da aziende rispettabili al fine di indurre le persone a rivelare informazioni personali, come password e numeri di carte di credito, online". Secondo l' Anti-Phishing Working Group(2013)[4] invece, gli attacchi di phishing comportano la distribuzione di massa di messaggi di posta elettronica contraffatti con indirizzi di ritorno, collegamenti e branding che sembrano provenire da banche, agenzie assicurative, rivenditori o società di carte di credito. Questi messaggi fraudolenti sono progettati per indurre i destinatari a divulgare dati di autenticazione personali come nomi utente di account e password, numeri di carte di credito, numeri di previdenza sociale, PIN di carte bancomat, ecc. Poiché queste e-mail sembrano "ufficiali" e i destinatari si fidano del marchio, spesso rispondono a loro, con conseguenti perdite finanziarie, furto di identità e altri atti fraudolenti. Recentemente il termine phishing è entrato a far parte anche del dizionario Treccani, il quale ci fornisce le seguenti definizioni :

- Probabile variante ortografica della parola inglese fishing (pescare), con cui si indica una frode informatica finalizzata all'ottenimento di dati personali sensibili (password, numero di carta di credito ecc.) e perpetrata attraverso l'invio di un messaggio di posta elettronica a nome di istituti di credito, finanziarie, agenzie assicurative, in cui si invita l'utente, generalmente al fine di derubarlo, a comunicare tali informazioni riservate.[57]

- ⟨fišiṅ⟩ s. ingl. [da fishing ≪pesca≫, con sostituz. di ph a f originatasi nell'ambiente della pirateria informatica], usato in ital. al masch. – Nel linguaggio di Internet, il tentativo di impadronirsi illegalmente dei dati personali di un utente, e di altre utili informazioni (numeri di conto corrente e di carta di credito, codici di sicurezza per l'accesso a banche dati, ecc.), generalm. al fine di derubarlo;

> il meccanismo di frode consiste nell'inviare messaggi fasulli di posta elettronica, a nome di istituti di credito, finanziarie, agenzie assicurative, ecc., che invitano l'utente a comunicare i dati e le informazioni in questione.[58]

In generale possiamo affermare che il phishing è una tecnica di ingegneria sociale combinata a competenze più tecniche e utilizzata dagli hacker per rubare informazioni personali, finanziarie o di login, tramite l'uso di messaggi di posta elettronica fraudolenti, siti web contraffatti, sms, chiamate vocali e/o altri mezzi.

5.2 Storia del phishing

In questo paragrafo saranno trattati velocemente la storia del phishing, la nascita del fenomeno e gli attacchi più famosi avvenuti con questa tecnica.

5.2.1 Le origini

La prima esplorazione del concetto di phishing si è verificata nel 1987, durante la conferenza Interex dove Jerry Felix e Chris Hauck presentarono un articolo intitolato "System Security: A Hacker's Perspective"[28], in cui discussero di un metodo utilizzabile da una terza parte per imitare un servizio affidabile. La prima testimonianza di "phishing" su internet risale al 2 gennaio 1996. Negli anni '90, quando l'accesso a Internet era principalmente tramite connessione dial-up a pagamento, AOL (un internet service provider) offriva una prova gratuita di trenta giorni tramite un floppy disk e alcune persone cercavano modi per evitare di pagare. Alcuni individui, per continuare ad accedere gratuitamente a Internet dopo la scadenza della prova, crearono nomi utente simili a quelli degli amministratori di AOL. Utilizzando questi nomi utente falsi, cercavano di ottenere le credenziali di accesso delle persone. Con l'aumento della popolarità di Internet, i truffatori adattarono queste tattiche per fingersi amministratori di un provider di servizi Internet (ISP) e inviare email agli utenti al fine di ottenere le credenziali di accesso degli utenti. Una volta falsificata l'identità di qualcuno, gli hacker potevano accedere a Internet utilizzando l'account della vittima e inviare spam dall'indirizzo email della vittima. L'aver ottenuto le credenziali degli account di AOL permise agli hackers di capire le potenzialità di questo tipo di attacco e come potessero essere attuabili attacchi simili anche verso sistemi di pagamento.

L'11 settembre 2001 segna una data importante per la storia americana, ma anche una data importante nella storia del phishing. Nell'immediato dopo gli attacchi alle Torri Gemelle, furono inviate diverse richieste di verifica dell'identità degli utenti, rivelatesi poi fraudolente, e con l'unico scopo di raccogliere i dati delle inconsapevoli vittime dal sistema di digital currency E-Gold. Questo fu il secondo attacco avvenuto contro la piattaforma di digital currency americana. Il primo fu un tentativo simile avvenuto nel giugno di quell'anno.Entrambi gli attacchi sono stati inizialmente considerati fallimenti, ma hanno contribuito a mettere il phishing saldamente sul radar di molte organizzazioni criminali.

5.2.2 L'affermazione e i social media

Nel 2004, il phishing si era consolidato come una forma diffusa di cybercriminalità. Nel periodo tra maggio 2004 e maggio 2005, si stima che circa 929 milioni di dollari statunitensi siano stati persi a causa delle truffe di phishing. [45]

La diffusione a partire del 2004 fu possibile anche grazie all'azione del gruppo criminale Rock Phish che prendeva il nome dalle caratteristiche degli URL che utilizzavano, in cui potevano comparire stringhe come "rock" o "r". Si stima che RockPhish fu responsabile del 50% o più degli attacchi di phishing mondiali e della creazione di una sofisticata rete di frodi automatizzate che coinvolgevano lo spam e il phishing a fini criminali.[62] Un'altra pietra miliare nella storia del phishing, così come nella storia di internet e di tutti noi, è stata la nascita e diffusione dei social media, in particolare nella metà degli anni 2000. I social media hanno introdotto nuovi vettori di attacco, consentendo agli aggressori di ingannare le persone e rubare le loro informazioni personali o credenziali di accesso. Alcune delle dinamiche che hanno contribuito alla diffusione del phishing attraverso i social media includono:

- Falsi profili e messaggi: Gli aggressori creano falsi profili o utilizzano account compromessi per inviare messaggi ingannevoli agli utenti dei social media.Questi messaggi possono contenere link malevoli che portano a pagine di phishing progettate per rubare informazioni personali.
- Phishing tramite applicazioni e giochi: Alcune applicazioni o giochi sui social media possono essere utilizzati come strumenti per condurre attacchi di phishing. Gli utenti potrebbero essere ingannati a fornire informazioni sensibili o a consentire l'accesso alle loro credenziali di accesso attraverso queste applicazioni o giochi compromessi.
- Phishing tramite messaggi di posta elettronica collegati ai social media: Gli aggressori inviano email ingannevoli che sembrano provenire dai social media, ad esempio notifiche di messaggi o aggiornamenti di stato. Queste email possono contenere link malevoli che portano a pagine di phishing.
- Phishing tramite annunci sponsorizzati: Gli aggressori possono utilizzare annunci sponsorizzati su piattaforme di social media per diffondere link malevoli o ingannevoli. Questi annunci possono apparire come promozioni legittime, ma in realtà conducono a pagine di phishing.

La scelta di utilizzare il tempo verbale presente per descrivere queste dinamiche non è casuale, è importante notare infatti che il phishing attraverso i social media è un problema ancora attuale e in continua evoluzione, poiché gli aggressori si adattano costantemente alle nuove tecnologie e alle abitudini degli utenti.

5.2.3 Gli attacchi più famosi

Con l'affermazione del phishing sono proliferati gli attacchi verso privati, aziende e istituzioni. Di seguito vengono trattati alcuni degli attacchi più famosi avvenuti nel mondo e in Italia:

- **L'incidente della Nordea Bank:** Nel 2007, la banca svedese Nordea perse oltre 7 milioni di corone quando i truffatori riuscirono a inviare email fraudolente ai clienti della banca, attirandoli ad installare il trojan "haxdoor" mascherato da software anti-spam. Chiamato "il più grande colpo di banca online di sempre" dalla società di sicurezza digitale McAfee, i clienti di Nordea furono colpiti da email di phishing contenenti virus trojan che hanno installato un keylogger nei computer delle vittime e le hanno indirizzate verso un falso sito web della banca, dove gli hacker hanno intercettato le credenziali di accesso.

- **Operazione Phish Phry:** Nel 2009 ci fu uno degli arresti di sicurezza informatica più grandi da parte dell'FBI. La maggior parte degli arrestati erano stati protagonisti di diverse frodi bancarie online che permisero loro di rubare circa 1,5 milioni di dollari. Da qui si capì ancora di più che la fama del phishing stava per aumentare.

- **RSA:** Nel 2011 la società di sicurezza RSA fu vittima di spear phishing a causa di una vulnerabilità di Adobe Flash. Vennero inviate email in cui si chiedeva una revisione di un file, di aprirlo e visualizzarlo. Un utente cadde nella trappola e ciò permise ai truffatori di ottenere un accesso backdoor al desktop della vittima e di rubare i dati aziendali.

- **Phishing Dyre:** Nel 2014 il gruppo di hacker russo Dyre convinse migliaia di vittime a scaricare file eseguibili fingendosi dei consulenti fiscali. Quando la vittima non inseriva le proprie credenziali nel falso sito di phishing, gli hacker chiamavano la vittima tramite Skype fingendo di essere agenti di polizia e impiegati bancari per incoraggiare il trasferimento. Tutto ciò causò la perdita di milioni di dollari.[15]

- **Lo "scam di Facebook e Google":** In questo classico caso di business email compromise (BEC), un uomo lituano di nome Evaldas Rimasauskas rubò oltre 100 milioni di dollari a Facebook e Google. Rimasauskas e i suoi complici crearono account email fake abbastanza convincenti di Quanta Computer, con sede a Taiwan, che effettivamente intratteneva rapporti commerciali con Facebook e Google. Inviarono email di phishing accuratamente studiate con false fatture, contratti e lettere a dipendenti di entrambe le aziende, fatturando loro in modo fraudolento milioni di dollari nel corso di due anni, dal 2013 al 2015. I dipendenti di Facebook e Google hanno pagato oltre 100 milioni di dollari sui conti bancari della finta azienda di Rimasauskas, che ha poi riciclato attraverso banche in Lettonia, Cipro, Slovacchia, Lituania, Ungheria e Hong Kong.

- **Attacco alla rete elettrica ucraina:** Nel dicembre 2015, l'azienda di distribuzione di energia ucraina Kyivoblenergo diventò il primo fornitore di rete elettrica al mondo ad essere colpito da un attacco informatico. Gli hacker furono in grado di attaccare l'azienda elettrica ucraina attraverso una email di phishing che consentì loro di accedere alla rete di Kyivoblenergo. Utilizzando il malware noto come BlackEnergy, i perpetratori furono in grado di attaccare i computer e i sistemi SCADA dell'azienda, disconnettendo 30 sottostazioni per tre ore. Questo attacco provocò un black-out, durante il quale fino a 230.000 clienti hanno perso l'energia elettrica, quasi la metà delle abitazioni nella regione di Ivano-Frankivsk, in Ucraina, che conta circa 1,4 milioni di abitanti.

- **Attacco whaling di Ubiquity Network:** In un altro caso di truffa BEC, l'azienda tecnologica con sede a San Jose, Ubiquity Network, fu vittima di un attacco di "whaling" il 5 giugno 2015. Gli aggressori finsero di essere un membro di alto livello dell'azienda e inviarono una email a un dipendente del dipartimento finanziario delle sussidiarie dell'azienda con sede a Hong Kong, che cadde nella trappola degli aggressori. I truffatori impersonarono il CEO e l'avvocato dell'azienda e istruirono il responsabile contabile a effettuare una serie di trasferimenti per chiudere un'acquisizione segreta. Nel corso di 17 giorni, l'azienda effettuò 14 trasferimenti bancari su conti in Russia, Ungheria, Cina e Polonia.

L'azienda segnalò trasferimenti di fondi per un totale stimato di 46,7 milioni di dollari che erano detenuti dalla sussidiaria dell'azienda incorporata a Hong Kong verso altri conti esteri. Il piano venne alla luce solo dopo che il Federal Bureau of Investigation (FBI) degli Stati Uniti contattò Ubiquity per informarli che l'agenzia sospettava che l'azienda fosse stata vittima di frodi.

- **Attacco BEC a FACC:** Il produttore austriaco di componenti aerospaziali e società di ingegneria FACC fu vittima di uno degli attacchi BEC più dannosi dal punto di vista finanziario della storia nel 2016. In questo incidente, un dipendente di FACC ricevette un' email apparentemente routinaria in cui i malintenzionati si fingevano il CEO dell'azienda e chiedevano all'organizzazione di trasferire circa 50 milioni di dollari su un altro conto come parte di un "progetto di acquisizione". Il messaggio sembrava provenire dal CEO di FACC, Walter Stephan, e il dipendente cadde nella trappola, trasferendo i soldi. L'azienda riuscì a impedire che circa 10 milioni di dollari fossero trasferiti all'ultimo minuto, ma il danno è stato grave e il CEO di FACC ha perso il lavoro a causa dell'accaduto.[55]

- **Attacco alla Crelan Bank:** Un mese dopo l'incidente di FACC la vittima di un simile scam fu la banca belga Crelan Bank. Un attaccante si spacciò per il CEO dell'organizzazione e inviò un'email a un dipendente in cui chiedeva di trasferire una somma di denaro in un account controllato dall'attaccante. L' incidente danneggiò la banca per 75,6 milioni di dollari, inclusi i costi per rimediare all'attacco.

- **Attacco a Sony Pictures:** Nel novembre 2014, il gruppo criminale hacking "Guardians of Peace" rilasciò circa 100 terabyte di dati rubati dallo studio cinematografico Sony Pictures. Gli attaccanti usarono email di phishing per ingannare dirigenti di alto livello di Sony, facendo credere che provenissero da Apple e chiedendo informazioni di verifica dell'identità. Le vittime furono indirizzate a un sito falso dove le loro credenziali di accesso furono catturate. Questo permise agli aggressori di ottenere una vasta quantità di dati sensibili, inclusi dettagli sugli impiegati e corrispondenze private. Inoltre, usarono un malware distruttivo per tentare di cancellare l'infrastruttura informatica di Sony. Gli aggressori chiesero poi a Sony di ritirare il film "The Interview", una commedia sulla trama per assassinare il leader nordcoreano Kim Jong-un, minacciando attacchi terroristici nei cinema che proiettavano il film. I danni stimati furono di circa 100 milioni di dollari, pari a circa 80 milioni di euro.

- **Attacco a Colonial Pipeline:** Nel maggio 2021 il fornitore di carburante Colonial Pipeline fu vittima di uno degli attacchi informatici più grande di tutti i tempi. I danni furono causati da un ransomware che costrinse l'organizzazione a interrompere le operazioni dopo che la sua rete aziendale e il sistema di fatturazione furono compromessi. L'installazione del ransomware fu possibile grazie a un precedente attacco di phishing via email che permise agli attaccanti di ottenere la password di un dipendente.L'organizzazione, che forniva quasi la metà delle forniture di petrolio alla costa orientale degli Stati Uniti, fu chiusa per una settimana, il che comportò la mancata consegna di circa 20 miliardi di galloni di petrolio, che valeva circa 3,4 miliardi di euro al momento e i prezzi della benzina schizzarono alle stelle, con ripercussioni economiche pesanti anche sui cittadini americani. Gli aggressori guadagnarono circa 3,75 milioni di euro grazie alla vendita della chiave di decrittazione a Colonial Pipeline.[25]

- **Fifa World Cup 2018:** Durante il mondiale del 2018 in Russia sono state perpetrate diverse truffe di phishing con milioni di dollari rubati. La truffa più comune era quella in cui si affermava che la vittima aveva vinto dei biglietti per un match della Coppa del mondo tramite una lotteria e la invitava a inserire le proprie informazioni personali per ottenere il premio. [38]

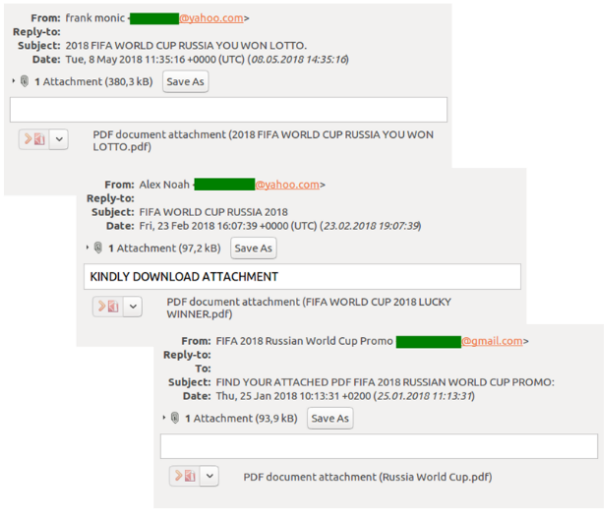


Figure 5.1: Esempio di email di phishing inviata durante la FifaWorldCup2018. Esempio di messaggi con biglietti e viaggi omaggio [38]

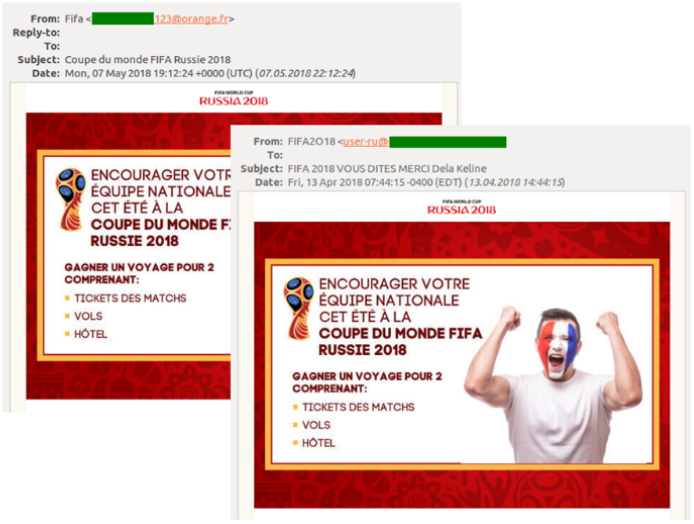


Figure 5.2: Esempio di email di phishing inviata durante la FifaWorldCup2018. Esempio di notificazione fake con allegati.[38]

- **Tecnimont Spa:** Un'azienda italiana attiva nel settore dell'ingegneria, costruzioni e procurement, chiamata Tecnimont Spa è stata vittima di una truffa di 18,6 milioni di dollari attraverso un sofisticato schema di frode BEC (Business Email

Compromise). In questo attacco di phishing, i truffatori hanno inviato email agli esecutivi dell'azienda in India, fingendo di organizzare chiamate false per discutere di un'acquisizione confidenziale in Cina. Questo ingannevole stratagemma ha portato alla sottrazione di una somma considerevole di denaro, causando gravi danni finanziari all'azienda.

- **The Scoular Company:** Una società di trading di commodities, The Scoular Company, è stata vittima di una sofisticata frode di spear phishing, durante la quale i truffatori hanno sottratto oltre 17 milioni di dollari. I malintenzionati si sono spacciati per il CEO dell'azienda e hanno inviato email a un dipendente, istruendolo su come trasferire fondi utilizzando il nome della vera società di contabilità dell'azienda. Tuttavia, le informazioni fornite erano fasulle, poiché l'indirizzo email proveniva da un server russo e il numero di telefono Skype era registrato con un indirizzo IP in Israele. Questa ingannevole operazione ha causato gravi danni finanziari all'azienda, evidenziando l'importanza di adottare misure di sicurezza robuste per proteggersi dalle frodi di spear phishing.

Questi sono solo alcuni degli innumerevoli e più grandi attacchi di phishing avvenuti su larga scala, per descrivere gli attacchi che avvengono ogni giorno, purtroppo, non basterebbero pagine e pagine di questa tesi. Dalle descrizioni degli attacchi è possibile notare come il phishing non sia solo quello via email, oggi infatti esistono diverse tipologie di phishing.[54]

5.3 Tipologie di phishing

Contrariamente all'opinione generale, il phishing non è solo caratterizzato da email e siti web fasulli, con il tempo si è evoluto sempre di più e ad oggi possiamo individuare phishing di diversi tipi con caratteristiche particolari:

- **Phishing generico via e-mail:** l'hacker invia un'e-mail fraudolenta che sembra provenire da un'organizzazione legittima, come una banca o un'azienda, e chiede alla vittima di fornire informazioni personali o di cliccare su un link che porta ad un sito web contraffatto. Di solito questo tipo di attacchi vengono fatti su larga scala focalizzandosi sulla quantità piuttosto che sulla qualità, come è possibile vedere nelle Figure 5.3 e 5.4.

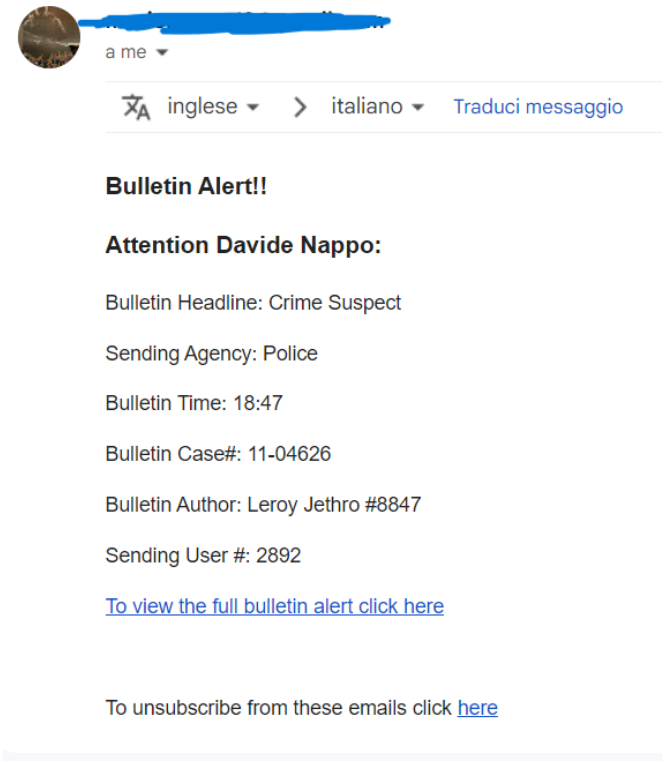


Figure 5.3: Esempio di email molto generica di phishing, creata attraverso un tool.

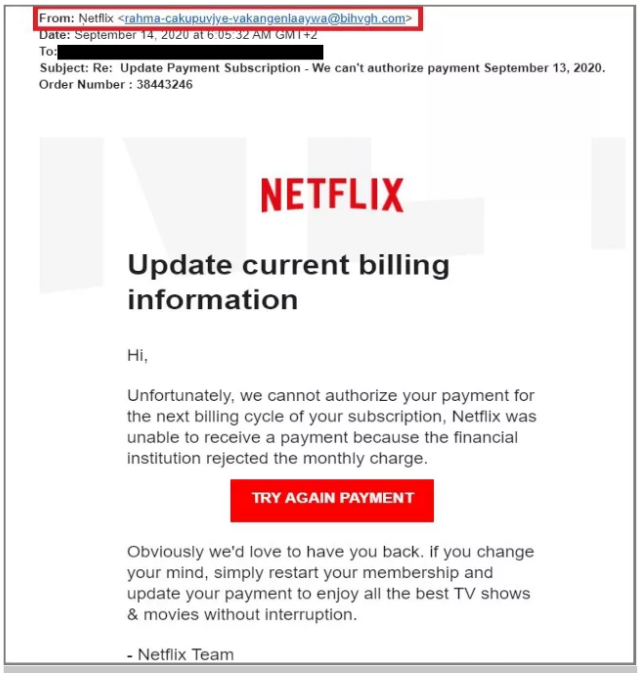


Figure 5.4: Esempio di phishing generico via email. Da notare come l'indirizzo email sospetto di ritorno, non abbia nulla a che fare con Netflix.[23]

- **Spear phishing:** questo tipo di phishing è rivolto a un individuo specifico o a un gruppo di individui, come dipendenti di un'azienda. L'hacker utilizza informazioni

personali o pubbliche per creare un messaggio di posta elettronica personalizzato e convincere la vittima a fornire informazioni o cliccare su un link malevolo. A differenza del più generico phishing, lo spear phishing è fortemente più mirato. Gli attaccanti si servono di informazioni personali e pubbliche quali dati presi dai social network,nome, cognome, ruolo svolto nell'azienda per cui lavora, hobby, informazioni fiscali e così via. Tali dettagli, essendo molto specifici, inducono la vittima ad abbassare la guardia. Mentre il phishing generico dà priorità alla quantità attaccando molteplici utenti su larga scala, lo spear phishing prioritizza la qualità. Un esempio di un'email di spear phishing è fornito nell'immagine 5.5.

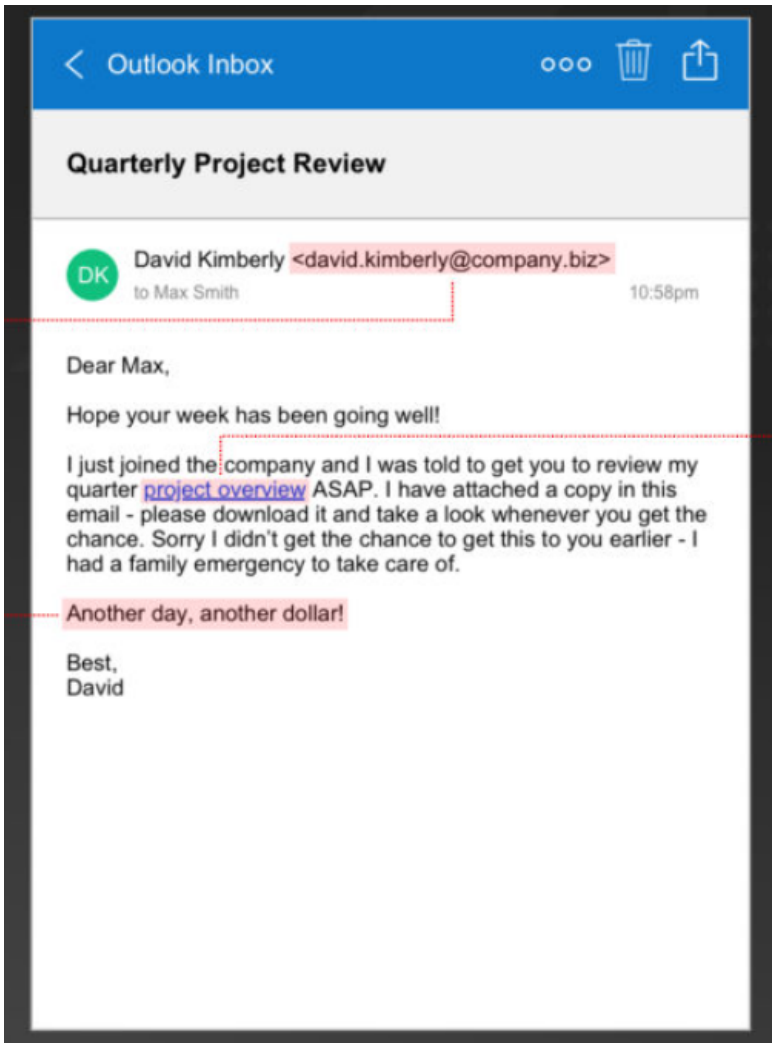


Figure 5.5: Esempio di Spear Phishing. Sono evidenziate l'indirizzo email utilizzato, il link malevolo e la frase comune finale usata per far apparire il messaggio come leggittimo.[63]

Da notare come nell'esempio appena visto nella Figura 5.5, il truffatore personalizzi l'email in base agli interessi e alla personalità della vittima. Questo è ciò che contraddistingue lo spear phishing dal comune phishing, ed è ciò che lo rende così efficace, anche se al tempo stesso costoso in termini di tempo e fatica per i truffatori. Dal punto di vista della resa economica questa tipologia di phishing risulta essere più remunerativa rispetto a quella generica poichè vengono prese di

mira figure più elevate all'interno delle aziende e ingannate attraverso l'utilizzo di informazioni dettagliate ottenute con una precedente fase di ricerca e studio. Non è infrequente che le vittime di attacchi mirati di spear phishing finiscano per effettuare bonifici di ingenti somme su conti bancari offshore controllati dai criminali informatici o addirittura divulghino le credenziali di accesso alla rete aziendale, il che può avere conseguenze ancora più devastanti rispetto alla semplice perdita economica causata da una transazione non autorizzata. I malintenzionati spesso utilizzano anche altre tecniche per rubare dati sensibili, come l'installazione di malware sulle reti aziendali o l'utilizzo di credenziali rubate per sottrarre dati. Una volta ottenute le credenziali di accesso, i criminali possono permanere nella rete delle vittime per mesi, passando inosservati. Nel frattempo, enormi quantità di dati possono essere sottratte senza che nessuno ne abbia consapevolezza. Quando alla fine viene scoperta la compromissione, l'azienda deve agire prontamente per contenere la minaccia e risolvere le vulnerabilità. Nello spear phishing, i truffatori utilizzano diverse strategie per ingannare le vittime:

  - Fingendosi un cliente insoddisfatto, inviano un link ad un sito malevolo simile a quello aziendale, chiedendo all'obiettivo di inserire le proprie credenziali di accesso.
  - Inviano messaggi di testo o email che avvisano della compromissione del conto in banca e includono un link per l'autenticazione delle credenziali.
  - Si spacciano per fornitori aziendali, minacciando la disattivazione dell'account e spingendo la vittima a cliccare su un link fraudolento per autenticarsi.
  - Richiedono donazioni o trasferimenti di denaro a un gruppo o ente specifico per ingannare le vittime.
  - Utilizzano nomi di fornitori reali con partite IVA false per creare fatture false e convincere le vittime a effettuare pagamenti non dovuti.

  Queste sono solo alcune delle astute strategie usate dai truffatori nel campo dello spear phishing, dimostrando la loro capacità di ingannare e trarre vantaggio da persone e organizzazioni vulnerabili. Questa tipologia di phishing sta diventando sempre più comune, basti pensare che rappresenta il quarto tipo più comune di truffa in Canada secondo un articolo un articolo del 2023 della Royal Canadian Mounted Police (RCMP).[29]

- **Whaling:** il whaling (detto anche ≪Compromissione della posta elettronica aziendale≫ o Business email compromise)[68] è una forma avanzata di spear phishing mirata a individui di alto profilo all'interno di un'organizzazione, come dirigenti, alti funzionari o personaggi famosi. Il termine "whale"fa riferimento ai "big fish" o "balene" nel mondo del phishing, indicando le personalità importanti e di alto valore che sono l'obiettivo di questi attacchi. La dinamica del whaling è quasi identica a quella dello spear phishing: Gli attacchi di whaling si distinguono per la loro mira precisa e la sofisticatezza rispetto al phishing tradizionale. I truffatori si concentrano su vittime di alto profilo, utilizzando informazioni personali e aziendali specifiche per rendere l'attacco più credibile. Questi messaggi di phishing possono apparire estremamente autentici e ingannare le vittime convincendo a condividere informazioni sensibili, come credenziali di accesso, password, dati finanziari o persino per effettuare trasferimenti bancari a qualcuno che credono sia il CEO o CFO dell'azienda. [61] Gli obiettivi di un attacco di whaling possono essere sottoposti a estorsione finanziaria, furto di proprietà intellettuale,

accesso non autorizzato a dati sensibili o danneggiamento dell'immagine e della reputazione personale o aziendale coinvolta. Poiché gli attacchi di whaling mirano a figure di spicco, le conseguenze possono essere gravi sia dal punto di vista finanziario che emotivo per le vittime coinvolte, rappresentando quindi una minaccia significativa per la sicurezza delle organizzazioni. Inoltre, questo tipo di phishing risulta molto pericoloso e difficilmente rilevabile poichè spesso non utilizzano URL maligni o allegati dannosi. Nella Figura 5.6 viene fornito un breve riassunto delle differenze tra phishing generico, spear phishing e whaling.

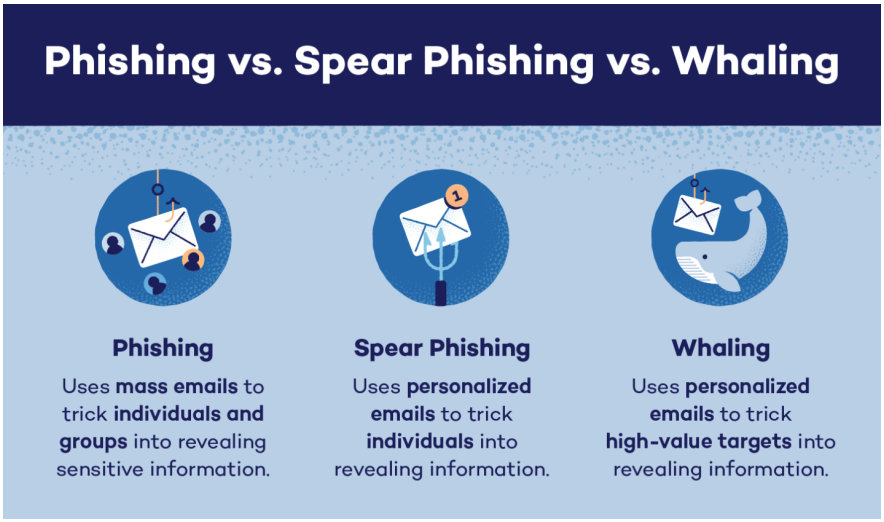


Figure 5.6: Immagine che riassume brevemente le differenze tra Phishing, SpearPhishing e Whaling.[34]

- **Pharming:** Il termine "Pharming" è un neologismo che deriva dalla combinazione delle parole "farming" (coltivazione) e "phishing". Il pharming è considerato un tipo di phishing che si differenzia dal phishing tradizionale per il modo in cui viene eseguito e con il quale si attrae la vittima. Mentre nel phishing classico gli attaccanti inviano email fraudolente o messaggi di testo mirati agli utenti per indurli a rivelare informazioni personali o finanziarie, nel pharming, gli aggressori utilizzano tecniche più sofisticate per dirottare il traffico di rete degli utenti verso siti web contraffatti. Nel pharming, i criminali mirano a manipolare il sistema di risoluzione dei nomi di dominio (DNS) o il server di risoluzione dei nomi di dominio (DNS) dell'utente. Questo può essere fatto attraverso attacchi di tipo DNS cache poisoning o modificando le impostazioni del router di rete. In questo modo, quando gli utenti cercano di visitare un sito web legittimo, vengono dirottati automaticamente verso un sito web falso che è sotto il controllo degli aggressori. Gli utenti potrebbero non accorgersi del cambiamento e potrebbero inserire informazioni sensibili su queste pagine false, che vengono poi raccolte dai criminali. Il pharming è detto il "phishing senza esca" ed è particolarmente pericoloso perché non richiede l'interazione diretta con l'utente, come avviene nel phishing tradizionale, rendendolo più difficile da individuare. Gli utenti potrebbero finire su pagine contraffatte anche digitando manualmente l'URL del sito legittimo nella barra degli indirizzi del browser e l'azione di antivirus potrebbe essere inutile. Nel settembre 2004, è stato registrato il primo attacco di pharming in Germania, mentre, nel gennaio 2005, a New York, anche l'ISP Panix.com

fu oggetto di un attacco di pharming. Nel corso degli anni, diverse istituzioni finanziarie in tutto il mondo sono state colpite da attacchi di questa tipologia, causando frodi e furti di identità. È stato riscontrato un notevole aumento dei casi negli ultimi anni, con migliaia di segnalazioni di attacchi. Sia pharming che phishing tradizionale sfruttano tecniche di ingegneria sociale per ottenere informazioni personali, ma con modalità diverse.[13]

- **Vishing:** Il Vishing è una forma di attacco informatico che combina le tecniche del phishing con l'uso del telefono. Il termine "Vishing" è una contrazione delle parole "Voice" e "Phishing". In questo tipo di attacco, gli hacker utilizzano chiamate telefoniche automatizzate o interazioni vocali per ingannare le vittime e ottenere informazioni personali o finanziarie. Durante un attacco di Vishing, le vittime possono ricevere una chiamata che sembra provenire da un'organizzazione legittima, come una banca, un'azienda o un'istituzione governativa. L'hacker può fingere di essere un rappresentante del servizio clienti o di sicurezza, cercando di convincere la vittima a fornire dati sensibili, come numeri di conto bancario, password o altre informazioni personali. Le chiamate di Vishing possono essere altamente sofisticate e convincere le vittime di essere autentiche, utilizzando anche tecniche di spoofing per falsificare l'identificatore di chiamata e farlo sembrare proveniente da un numero legittimo. Per proteggersi dagli attacchi di Vishing, è importante essere cauti quando si rispondono a chiamate da fonti sconosciute o sospette. Se qualcuno richiede informazioni personali o finanziarie, è meglio sospendere la chiamata e contattare direttamente l'organizzazione utilizzando informazioni di contatto verificate. Inoltre, è consigliabile installare applicazioni di blocco delle chiamate o usare servizi che rilevano e segnalano le chiamate di spam o phishing [53].

- **Smishing:** Lo "smishing" è una forma di truffa informatica che sfrutta gli SMS (Short Message Service) per ingannare le vittime e ottenere informazioni personali o sensibili. Il termine "smishing" è una fusione delle parole "SMS" e "phishing", poiché l'attacco combina le tattiche del phishing con l'utilizzo degli SMS come mezzo di comunicazione.

  Nello smishing, gli aggressori inviano messaggi di testo fraudolenti o ingannevoli alle vittime, spacciandosi per organizzazioni o servizi legittimi. Questi messaggi spesso contengono link malevoli o istruzioni per rispondere con informazioni personali, come password, numeri di carte di credito o altre informazioni sensibili.

  Gli smishing sono particolarmente pericolosi perché gli SMS sono considerati da molte persone come una forma di comunicazione sicura e affidabile. Le vittime possono cadere nella trappola senza sospettare nulla, rischiando di fornire dati sensibili agli aggressori.

  Per proteggersi dagli smishing, è essenziale essere cauti riguardo ai messaggi di testo provenienti da mittenti sconosciuti o che richiedono informazioni personali. In caso di dubbio, è sempre meglio verificare direttamente con l'organizzazione o il servizio che sembra aver inviato il messaggio prima di rispondere o cliccare su link sospetti. Inoltre, l'utilizzo di software di sicurezza per dispositivi mobili può aiutare a rilevare e bloccare messaggi smishing potenzialmente pericolosi [39]. Un esempio di smishing è fornito alla Figura 5.7.

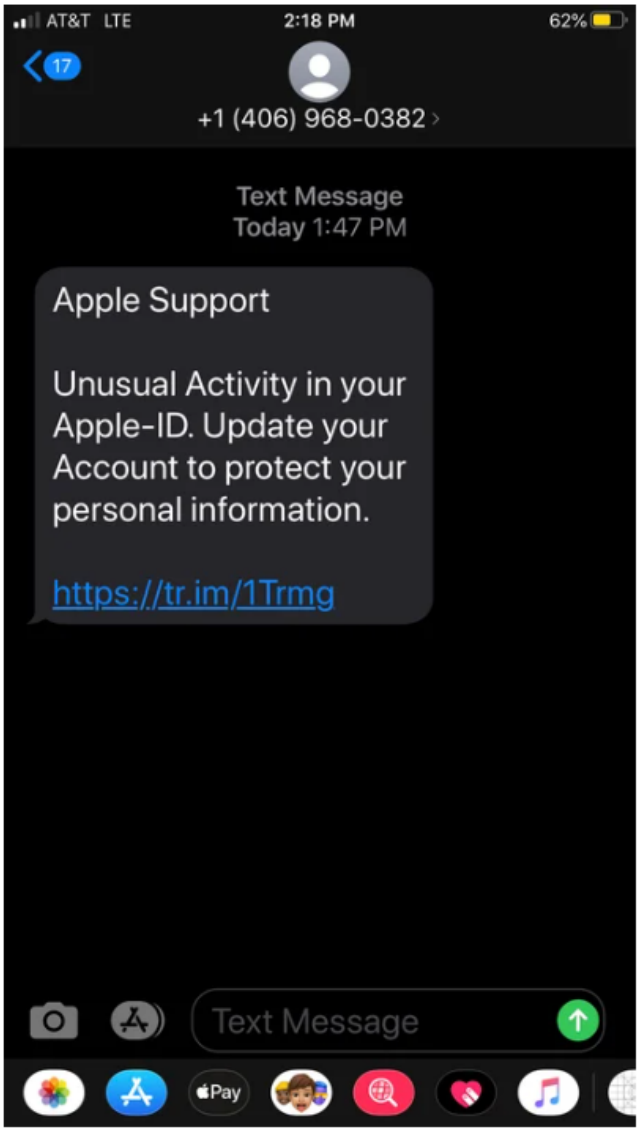


Figure 5.7: Esempio di Smishing basato su una presunta attività inusuale nell'account Apple. [1]

5.4 Attaccanti e vittime

Per comprendere appieno le dinamiche dei pericolosi attacchi di phishing, è essenziale delineare il profilo tipo dell'attaccante e della vittima. Nelle prossime righe saranno esplorate le caratteristiche di entrambi.

Profilo tipo di un attaccante di phishing:

- Nome: L'attaccante di phishing può operare in modo anonimo o sotto vari pseudonimi online. Il suo vero nome è generalmente sconosciuto.
- Età: L'età può variare notevolmente, ma molti attaccanti di phishing sono giovani adulti con competenze tecniche.
- Formazione: L'attaccante di phishing può avere una formazione informatica o di

sicurezza informatica, ma non è sempre il caso. Alcuni possono apprendere le abilità necessarie tramite risorse online.

- Motivazioni:
  - Finanziarie: Molti attaccanti di phishing sono motivati dal profitto. Vogliono rubare dati finanziari, come numeri di carte di credito o account bancari, per guadagnare denaro.
  - Distruttive: Alcuni attaccanti di phishing possono essere motivati dalla volontà di danneggiare o sabotare un'organizzazione o una persona.
  - Spionaggio: In alcuni casi, gli attaccanti di phishing possono essere governi o gruppi di spionaggio che cercano di ottenere informazioni sensibili da individui o organizzazioni. Razzia d'identità: Altri possono cercare di rubare identità per vari scopi, inclusi reati come frode o accesso a risorse riservate.
- Metodi: Gli attaccanti di phishing utilizzano una varietà di metodi, inclusi l'invio di email di phishing, la creazione di siti web falsi, la manipolazione di URL o l'utilizzo di social engineering per ingannare le vittime.
- Strumenti: Gli attaccanti di phishing utilizzano spesso strumenti informatici come kit di phishing, software di email spoofing, malware e botnet per automatizzare e scalare i loro attacchi.
- Livello di competenza: Il livello di competenza varia, ma molti attaccanti di phishing hanno una conoscenza tecnica delle reti, dei sistemi informatici e delle tecniche di ingegneria sociale.

Profilo tipo di una vittima:

- Nome: Il nome della vittima è variabile ed è generalmente sconosciuto agli attaccanti.
- Età: Le vittime del phishing possono appartenere a qualsiasi gruppo demografico, ma le persone anziane e i giovani meno esperti sono spesso bersagli comuni.
- Formazione: La formazione delle vittime può variare notevolmente. Alcune persone possono avere una conoscenza limitata della sicurezza informatica, mentre altre possono essere esperte.
- Motivazioni: Le vittime sono spesso motivate a rispondere agli attacchi di phishing per diverse ragioni:
  - Inganno: Le vittime possono cadere nell'inganno a causa dell'apparente autenticità dell'attacco.
  - Distrazione: In alcuni casi, le vittime possono essere distolte o non attente e fare clic su link o fornire informazioni senza pensarci.
  - Urgenza: Gli attacchi di phishing spesso cercano di creare un senso di urgenza per indurre le vittime a agire rapidamente senza riflettere.
  - Mancanza di consapevolezza: Alcune vittime potrebbero non essere consapevoli dei pericoli del phishing o delle tattiche utilizzate dagli attaccanti.

- Comportamento di risposta: Le vittime possono rispondere in modi diversi, inclusi cliccare su link, fornire informazioni personali o finanziarie, ignorare l'attacco o segnalare il tentativo di phishing alle autorità competenti o all'organizzazione coinvolta.
- Conseguenze: Le conseguenze per le vittime possono variare da danni finanziari a furti d'identità, perdita di dati sensibili o accesso non autorizzato a account online. La gravità dipende dall'efficacia dell'attacco e dalla tempestività della risposta.

5.5 Perchè e quanto il phishing ha successo

Dopo aver individuato le caratteristiche tipiche degli attaccanti e delle vittime può venire spontaneo domandarsi quanto gli attacchi di phishing abbiano successo e perchè questo accada. Gli ultimi dati internazionali [21] evidenziano alcune curiosità e ci donano alcuni spunti:

- Blocchi di Google: Google blocca circa 100 milioni di email di phishing al giorno.
- Marche più imitate: Nel primo trimestre del 2022, LinkedIn è stata la marca più imitata nei tentativi di phishing a livello globale, seguita da DHL, Google, Microsoft e FedEx.
- Settori più colpiti: Nel 2021, il settore energetico è stato il più colpito dagli attacchi di phishing (60%), seguito da servizi finanziari (46%) e produzione (40%).
- Perdite finanziarie: Nel 2022, gli attacchi di Business Email Compromise (BEC) hanno causato perdite finanziarie di oltre 2,7 miliardi di dollari negli Stati Uniti.
- Aumento durante la pandemia: Tra il 2020 e il 2021, i crimini informatici sono aumentati del 168% nella regione Asia-Pacifico, compresi gli attacchi di phishing.
- Tipo di attacco più comune nelle organizzazioni: Nel 2021, phishing è stato il tipo di attacco più comune nelle organizzazioni asiatiche (43%), europee (42%), nordamericane (47%) e latinoamericane (47%).
- Target demografico: I millennial e la Generazione Z (18-40 anni) sono più propensi a cadere vittima di attacchi di phishing rispetto alla Generazione X (41-55 anni).
- Phishing via messaggi: Il 90% degli attacchi di phishing inviati tramite app di messaggistica sono stati condotti attraverso WhatsApp, seguito da Telegram con il 5,04%.
- Kit di phishing: Nel 2021, sono stati rilevati 469 diversi "kit di phishing", strumenti utilizzati per condurre attacchi di phishing.
- Creazione di siti di phishing: In media, vengono creati 1,4 milioni di siti di phishing ogni mese.
- Attacchi alle aziende: Tra il 2022 e il 2023, il 79% delle aziende nel Regno Unito colpite da un attacco informatico ha identificato il phishing come il tipo di attacco.

  Da questi dati si evince che il phishing è uno degli attacchi informatici più frequenti ed ha successo in svariati casi per diversi motivi[51], principalmente legati

all'efficacia delle tattiche utilizzate dagli attaccanti e alle vulnerabilità umane nell'affrontare queste minacce:

- **Inganno convincente:** Gli attaccanti investono tempo ed energie per creare messaggi di phishing che sembrano autentici e provenire da fonti attendibili. Questi messaggi possono utilizzare loghi aziendali, nomi noti o informazioni personali per convincere le vittime della loro autenticità.
- **Urgenza e paura:** Molti attacchi di phishing cercano di creare un senso di urgenza o paura nelle vittime. Ad esempio, un'email potrebbe minacciare la chiusura di un account o affermare che un problema di sicurezza richiede un'azione immediata. Questo spinge le persone a compiere decisioni affrettate senza pensarci troppo.
- **Manipolazione emotiva:** Gli attaccanti sfruttano le emozioni umane, come la paura, la curiosità o la preoccupazione, per indurre le vittime a compiere determinate azioni. Ad esempio, un messaggio potrebbe promettere una ricompensa o minacciare conseguenze negative se l'utente non segue le istruzioni.
- **Mancanza di consapevolezza:** Molte persone non sono ben informate sulle minacce informatiche e sulla prevenzione degli attacchi di phishing. Questa mancanza di consapevolezza può rendere le persone più suscettibili di cadere nelle trappole degli attaccanti.
- **Facilità di esecuzione:** Il phishing richiede relativamente poco sforzo da parte degli attaccanti. Possono inviare migliaia di messaggi in modo automatizzato e aspettarsi che anche solo una piccola percentuale delle vittime cada nella trappola.
- **Vulnerabilità umane:** Alla base del successo del phishing ci sono le vulnerabilità umane. Anche le persone più attente possono essere ingannate quando ricevono un messaggio convincente che sembra provenire da una fonte fidata.
- **Sicurezza informatica inefficace:** In alcuni casi, le misure di sicurezza informatica possono non essere abbastanza solide da proteggere contro gli attacchi di phishing. Ad esempio, le soluzioni di filtraggio delle email potrebbero non riconoscere tutti i messaggi di phishing.
- **Aumento della sofisticazione:** Nel corso degli anni, gli attacchi di phishing sono diventati sempre più sofisticati, utilizzando URL contraffatti, siti Web clonati e tecniche di ingegneria sociale avanzate. Questo ha reso più difficile per le vittime riconoscere gli attacchi.
- **Mancanza di tutela legale:** In molte giurisdizioni, esistono poche protezioni legali specifiche contro il phishing. Le vittime spesso hanno poche possibilità di tutela legale, il che rende difficile perseguire la giustizia quando le loro informazioni personali vengono rubate.
- **Percezione di sicurezza:** Nonostante la consapevolezza dei potenziali rischi, le persone spesso percepiscono alcune azioni come sicure, come l'apertura di email o il clic su link. Questa falsa sensazione di sicurezza è esattamente ciò che i truffatori sfruttano.

5.6 Strategie di difesa

In questo paragrafo verranno mostrate e indagate alcune tecniche e strategie di difesa generali per il phishing generico e specifiche per le varie tipologie di phishing.

5.6.1 Strategie generali

Esistono accorgimenti e strategie di difesa comuni[48] contro tutti i tipi di phishing, quali:

- **Sensibilizzazione degli utenti:** L'educazione e la sensibilizzazione degli utenti sono fondamentali. Gli utenti devono essere istruiti su come riconoscere segnali di phishing, come messaggi con errori grammaticali, richieste insolite di informazioni personali o link sospetti.
- **Verifica dell'URL:** Prima di cliccare su un link in un'email o in un messaggio, è importante passare sopra il link con il cursore del mouse per visualizzare l'URL completo. Verificare se l'URL sembra legittimo e se corrisponde al sito web reale.
- **Uso di software di sicurezza:** Installare software di sicurezza, come programmi antivirus e antimalware, che possono rilevare e bloccare siti web malevoli o messaggi di phishing.
- **Filtraggio delle email:** Utilizzare filtri antispam per bloccare l'arrivo di email di phishing nella casella di posta in arrivo.
- **Autenticazione a due fattori:** Attivare l'autenticazione a due fattori (2FA) su tutti gli account online che lo supportano. Questa tecnica richiede un secondo passaggio di verifica, oltre alla password, per accedere a un account.
- **Verifica delle fonti:** Verificare sempre la fonte di un'email o di un messaggio prima di fornire informazioni personali. Ad esempio, contattare direttamente l'organizzazione tramite canali ufficiali per confermare se la richiesta è legittima.
- **Aggiornamenti regolari:** Mantenere il sistema operativo, i programmi e le applicazioni aggiornati con le ultime patch di sicurezza. Gli aggiornamenti spesso correggono le vulnerabilità note che potrebbero essere sfruttate dai truffatori.
- **Utilizzo di browser sicuri:** Utilizzare browser web che offrono funzionalità di sicurezza avanzate, come il rilevamento dei siti web malevoli o il blocco dei contenuti dannosi.
- **Monitoraggio delle transazioni:** Monitorare regolarmente i conti finanziari per individuare attività sospette o non autorizzate.
- **Non rispondere alle richieste:** Se si riceve una richiesta di informazioni sensibili tramite email, SMS o messaggi di social media, evitare di rispondere direttamente. Invece, contattare l'organizzazione o la persona attraverso canali ufficiali per verificare l'autenticità della richiesta.
- **Evitare l'uso di link:** Invece di cliccare sui link in un messaggio di phishing, è preferibile digitare manualmente l'URL del sito web nella barra degli indirizzi del browser.

- **Cautela con i download:** Evitare di scaricare allegati o file da fonti non verificate, poiché potrebbero contenere malware.
- **Segnalazione dei tentativi:** Se si riceve un tentativo di phishing, segnalarlo alle autorità competenti, all'organizzazione coinvolta o a fornitori di servizi online per bloccare ulteriori tentativi.
- **Utilizzo di servizi di posta sicura:** Utilizzare servizi di posta elettronica sicura che offrono protezione avanzata contro il phishing e i malware.
- **Backup dei dati:** Mantenere regolari copie di backup dei dati importanti per proteggersi da eventuali perdite di dati causate da attacchi di phishing.

  Adottando queste strategie di difesa e seguendo pratiche di sicurezza informatica, è possibile ridurre significativamente il rischio di cadere vittima di tentativi di phishing di vario tipo.

5.6.2 Strategie specifiche

In questa sottosezione vengono elencate strategie e accorgimenti specifici per evitare le tipologie di phishing descritte precedentemente nella Sezione 5.3:

- **Spear Phishing:**
  - **Autenticazione a due fattori avanzata:** Utilizzare metodi di autenticazione a due fattori avanzati che richiedono, ad esempio, l'uso di token hardware o app mobili per ulteriori verifiche.
  - **Controllo delle email esterne:** Implementare controlli per verificare l'autenticità delle email provenienti dall'esterno, ad esempio utilizzando indicatori di autenticità come il Domain-based Message Authentication, Reporting, and Conformance (DMARC).
  - **Formazione specifica:** Fornire formazione ai dipendenti sui rischi dello spear phishing e su come riconoscere e affrontare i messaggi sospetti.
  - **Verifica delle richieste di pagamento:** Per le richieste di pagamento o trasferimenti di fondi, richiedere procedure di verifica aggiuntive o contatti telefonici diretti con le parti coinvolte [52].
- **Whaling:**
  - **Controllo degli accessi:** Limitare l'accesso a informazioni sensibili solo a coloro che ne hanno bisogno, riducendo così le possibilità di accesso non autorizzato.
  - **Filtro avanzato delle email:** Implementare filtri di email avanzati che rilevano e segnalano messaggi sospetti che potrebbero provenire da fonti di alto livello.
  - **Verifica delle richieste:** Prima di rispondere a richieste di azioni o informazioni da parte di figure di alto livello, verificare sempre la loro autenticità attraverso canali ufficiali [19].

- **Pharming:**
  - **Monitoraggio DNS:** Monitorare regolarmente l'infrastruttura DNS per individuare modifiche o attività anomale.
  - **Utilizzo di DNSSEC:** Implementare il Domain Name System Security Extensions (DNSSEC) per garantire l'autenticità e l'integrità dei record DNS.
  - **Aggiornamenti regolari:** Mantenere aggiornati sia il sistema operativo che le applicazioni, riducendo le vulnerabilità sfruttabili dagli attacchi di pharming [37].
- **Vishing:**
  - **Verifica dell'identità:** Quando si ricevono chiamate telefoniche sospette, chiedere sempre al chiamante di fornire ulteriori informazioni per verificare la loro identità.
  - **Non condividere informazioni:** Evitare di condividere informazioni personali o sensibili su richiesta telefonica, a meno che non si sia sicuri dell'autenticità della chiamata.
  - **Chiamare direttamente:** In caso di dubbi su una chiamata, cercare il numero di telefono ufficiale dell'organizzazione e chiamare direttamente per confermare la richiesta[49].
- **Smishing:**
  - **Verifica dei messaggi:** Prima di rispondere a messaggi di testo sospetti, verificare la fonte attraverso canali ufficiali o cercare informazioni sul mittente.
  - **Non cliccare su link:** Evitare di cliccare su link nei messaggi di testo, soprattutto se sembrano sospetti. Invece, visitare manualmente il sito web dall'applicazione ufficiale [11].

6. Tool Di Phishing

Questo capitolo si concentra sullo studio dei tool di phishing, strumenti che vengono utilizzati sia per fini malevoli che per scopi di penetration testing e sensibilizzazione sulla sicurezza informatica. Alcuni di questi strumenti rappresentano un aspetto cruciale nella lotta contro il phishing, poiché permettono agli esperti di testare le vulnerabilità e di addestrare gli utenti a riconoscere gli attacchi. Il capitolo inizia con la Sezione 6.1 in cui viene data una panoramica generale dei principali tool di phishing, fornendo una descrizione di ciascuno di loro e analizzandone alcune funzionalità. Questa analisi è poi riassunta nella Tabella 6.1 in cui sono evidenziate le caratteristiche comuni e le differenze tra questi strumenti. Successivamente, nelle Sottosezioni 6.1.1, 6.1.2, 6.1.3 e 6.1.4 viene approfondita l'analisi di quattro tool di phishing particolarmente rilevanti: Gophish, Pyphisher, PhishInsight e Zphisher. Ognuno di questi strumenti offre un approccio unico al phishing, e ne sono indagate dettagliatamente le funzionalità. Attraverso questa disamina, l'obiettivo è quello di gettare luce sui metodi e gli strumenti utilizzati sia dagli aggressori informatici che dagli esperti di sicurezza per comprendere meglio il fenomeno del phishing e le sfide connesse alla sua identificazione e mitigazione.

6.1 Elenco dei principali tool di Phishing

In questa sezione i protagonisti sono i tool per fare campagne di phishing. Questi tool sono spesso utilizzati per scopi etici, come la formazione e la consapevolezza sulla sicurezza informatica, ma possono anche essere abusati da malintenzionati per condurre attacchi reali. Alcuni esempi di tool per campagne di phishing sono[3]:

- **Gophish:** È un framework open source che consente di eseguire campagne di phishing simulato. Fornisce una varietà di template di phishing e consente di monitorare le risposte degli utenti per valutare la loro consapevolezza sulla sicurezza.
- **SET (Social Engineering Toolkit):** Questo tool è incluso in Kali Linux, una distribuzione Linux di sicurezza informatica. SET offre diverse opzioni di attacco, inclusi attacchi di phishing e vishing, e può generare URL malevoli e pagine web per ingannare le vittime.
- **Cofense PhishMe:** È una piattaforma di simulazione di phishing progettata per educare gli utenti sulle minacce e migliorare la loro capacità di riconoscere gli attacchi. Offre una vasta gamma di template e scenari di phishing.
- **BeEF (Browser Exploitation Framework):** Anche se inizialmente progettato per dimostrare le vulnerabilità dei browser, BeEF può essere utilizzato per eseguire attacchi di phishing mirato. Può sfruttare vulnerabilità nei browser per ingannare gli utenti.

- **Cobalt Strike:** Questo è un tool più avanzato che può essere utilizzato per condurre campagne di phishing e attacchi di ingegneria sociale. Offre funzionalità di comando e controllo, nonché capacità di simulazione di attacco reali.

- **King Phisher:** Un altro tool open source per eseguire campagne di phishing simulato. Consente di creare email di phishing personalizzate e monitorare l'interazione degli utenti con i messaggi.

- **SocialFish:** Questo tool open source è utilizzato per eseguire campagne di phishing su piattaforme di social media. Può generare pagine di accesso false per siti di social media popolari e monitorare le credenziali di accesso.

- **Infosec IQ:** Infosec IQ è una piattaforma di formazione e consapevolezza sulla sicurezza informatica. È progettata per aiutare le organizzazioni a migliorare la sicurezza informatica sensibilizzando i dipendenti e fornendo loro formazione su varie minacce informatiche, tra cui il phishing, le violazioni dei dati, i malware e altro ancora. Infosec IQ consente alle organizzazioni di condurre simulazioni di attacchi di phishing per valutare la capacità dei dipendenti di riconoscere e rispondere alle minacce.

- **69phisher:** Uno strumento di phishing automatizzato adatto ai principianti e con oltre 30 modelli di pagine.

- **PyPhisher:** Un tool di phishing scritto in Python, intuitivo, con 77 template di siti web, permette di ottenere l'ip e le credenziali della vittima e supporta l'autenticazione a due fattori.

- **ZPhisher:** uno strumento open-source progettato per eseguire attacchi di phishing e catturare informazioni sensibili dalle vittime. Questo strumento è spesso utilizzato a scopo educativo o di ricerca per dimostrare le vulnerabilità dei sistemi e per scopi di test della sicurezza.

- **SpeedPhish Framework (SPF)**: è un framework open source scritto in python per semplificare e automatizzare il processo di creazione e distribuzione di campagne di phishing. SPF fornisce agli operatori di sicurezza informatica e agli esperti di penetration testing uno strumento per simulare attacchi di phishing e misurare la consapevolezza della sicurezza all'interno di un'organizzazione.

- **Trend Micro PhishInsight:** un servizio di addestramento e simulazione di phishing offerto da Trend Micro, un'azienda specializzata in sicurezza informatica. Questo strumento è progettato per aiutare le organizzazioni a rafforzare la consapevolezza della sicurezza tra i loro dipendenti, simulando attacchi di phishing realistici al fine di identificare le vulnerabilità e migliorare le pratiche di sicurezza. PhishInsight può essere utilizzato per offrire formazione aggiuntiva ai dipendenti sulla sicurezza informatica, compresi i pericoli legati al phishing e le migliori pratiche per evitare di cadere in tali trappole.

- **Phishing Frenzy**: un'applicazione open-source basata su Ruby on Rails. Ampiamente utilizzata per la creazione e la gestione di campagne di phishing.

- **Usecure - uPhish**: è un componente della suite Usecure progettato per affrontare la crescente minaccia degli attacchi di phishing. Gli utenti possono avviare una simulazione di phishing gratuita come parte di una prova gratuita

di 14 giorni della piattaforma uPhish. Queste simulazioni utilizzano una serie di modelli di phishing personalizzabili per imitare scenari di attacco del mondo reale. uPhish fornisce analisi dettagliate e report sulle prestazioni dei dipendenti durante le simulazioni di phishing. Questi report consentono alle organizzazioni di misurare i progressi dei dipendenti nell'identificazione e nella gestione delle minacce di phishing.

- **Sophos Phish Threat:** è uno strumento finalizzato a migliorare la consapevolezza e la preparazione delle organizzazioni contro gli attacchi di phishing. Gli utenti possono configurare una prova gratuita per accedere alle campagne di phishing simulate. Queste simulazioni consentono di testare la capacità dei dipendenti di riconoscere e gestire gli attacchi di phishing.

- **SafeTitan:** tool progettato per fornire alle persone le conoscenze e le competenze necessarie per proteggersi dalle minacce informatiche. Questa formazione copre vari argomenti, tra cui l'identificazione dei tentativi di phishing, la comprensione delle tecniche di phishing comuni e le migliori pratiche per proteggere le informazioni personali online. Il programma utilizza moduli interattivi e scenari di vita reale per coinvolgere gli studenti e aiutarli a consolidare i concetti chiave.

- **Phished.io:** è una piattaforma completa per la simulazione di attacchi di phishing e smishing progettata per aiutare le organizzazioni a rafforzare le difese informatiche.

- **Phishingbox:** è un marchio specializzato nella fornitura di simulatori di phishing. Un simulatore di phishing è uno strumento che aiuta le organizzazioni a testare e rafforzare le proprie difese contro gli attacchi di phishing. Questo strumento simula diversi tipi di attacchi di phishing, come email, link o allegati, in un ambiente controllato e sicuro. Phishingbox offre una serie di funzionalità e opzioni per soddisfare le esigenze delle diverse organizzazioni. Forniscono interfacce utente user-friendly, modelli personalizzabili e report dettagliati.

È importante notare che l'uso di questi tool deve essere etico e in conformità con le leggi e le normative locali. Utilizzarli per scopi illegali o dannosi è severamente condannato. Inoltre, l'utilizzo di questi tool per scopi di formazione può aiutare a migliorare la consapevolezza degli utenti sulla sicurezza informatica e a prevenire cadute in trappola di attacchi di phishing reali. I tool visti in precedenza hanno caratteristiche simili e differenze tra di loro, il tutto viene sintetizzato nella Tabella 6.1.

Leggendo la Tabella 6.1 è possibile indivuare tante caratteristiche comuni tra questi tool, avendo quasi tutti come obiettivo principale quello di poter effettuare attacchi di phishing, spesso in maniera controllata e nel rispetto della legalità. La scelta sull'usare l'uno o l'altro tool spesso si basa su gusti personali, sulla semplicità di utilizzo di alcuni di questi, su alcune cose particolari che offrono: reportistica, monitoraggio, customizzazione dell'url ecc... Per questo motivo, nelle successive sottosezioni, saranno indagati più nello specifico solo alcuni tool, tra i più famosi tra quelli pensati per il phishing, quali: Gophish, ZPhisher, PhishInsight e PyPhisher.

Nome	**Open Source**	**Funzionalità fornite**	**Funzionalità non fornite**	**Interfaccia Web-Based**	**S.O**
Gophish	Sì	Simulazione di Phishing, Analisi e Monitoraggio, Reportistica.	Sfruttamento di Vulnerabilità, Attacchi Avanzati.	Sì	Linux, Windows, macOS.
Social Engineering Toolkit (SET)	Sì	Ingegneria Sociale, Simulazione di Phishing.	Monitoraggio, Analisi in Tempo Reale.	No	Linux, Windows, macOS.
Cofense PhishMe	No	Simulazione di Phishing, Addestramento degli Utenti, Analisi.	Strumenti di Penetration Testing alternativi.	Sì	Web-Based
BeEF (Browser Exploitation Framework)	Sì	Ingegneria Sociale, Sfruttamento dei Browser, Monitoraggio.	Inizialmente non sviluppato per campagne di phishing.	No	Linux, Windows, macOS.
Cobalt Strike	No	Test di Penetrazione, Simulazione di Phishing, Gestione delle Minacce.	Addestramento Utenti, Analisi in Tempo Reale.	No	Linux, Windows, macOS.
King Phisher	Sì	Simulazione di Phishing, Analisi e Monitoraggio, Reportistica.	Altri strumenti di Ingegneria Sociale.	No	Linux, macOS.
SocialFish	Sì	Phishing su Piattaforme Social, Ingegneria Sociale, Raccolta Informazioni.	Analisi in Tempo Reale, Simulazione di Exploit.	No	Linux
Infosec IQ	No	Simulazione di Phishing, Addestramento degli Utenti, Analisi.	Strumenti di Penetration Testing.	Sì	Web-Based
69phisher	Sì	Simulazione di Phishing, Raccolta di Credenziali, Analisi.	Ingegneria Sociale, Strumenti di Penetration Testing.	No	Linux, Windows.
PyPhisher	Sì	Strumento di Phishing, Raccolta di Credenziali, Personalizzabile, Presenza di pagine OTP fake.	Ulteriori strumenti di Ingegneria Sociale, Dashboard di analisi.	No	Linux
ZPhisher	Sì	Strumento di Phishing Multipiattaforma, Raccolta di Credenziali.	Ulteriori strumenti di Ingegneria Sociale, Dashboard di analisi.	No	Linux, Windows.
SpeedPhish Framework (SPF)	Sì	Simulazione di Phishing, Raccolta di Credenziali, Analisi.	Ulteriori strumenti di Ingegneria Sociale, Monitoraggio.	No	Linux, Windows.
Trend Micro PhishInsight	No	Simulazione di Phishing, Analisi e Monitoraggio, Reportistica.	Poco accessibile agli studenti.	Sì	Web-Based
Phishing Frenzy	Sì	Simulazione di Phishing, Reportistica, Personalizzazione.	Analisi in Tempo Reale, Monitoraggio.	Sì	Linux
Usecure - uPhish	No	Simulazione di Phishing, Addestramento degli Utenti, Analisi.	Penetration Testing.	Sì	Web-Based
Sophos Phish Threat	No	Simulazione di Phishing, Analisi in Tempo Reale, Reportistica.	Monitoraggio.	Sì	Web-Based
SafeTitan	No	Formazione sul Phishing, Moduli Interattivi.	Poco accessibile a studenti, rivolto ad aziende.	Sì	Web-Based
Phished.io	No	Simulazione di Phishing e Smishing, Reportistica, Analisi.	Poco accessibile a studenti, rivolto ad aziende.	Sì	Web-Based
Phishingbox	No	Simulazione di Phishing, Reportistica, Personalizzazione.	Ulteriori strumenti di Ingegneria Sociale.	Sì	Web-Based

Table 6.1: Tabella riassuntiva di alcuni dei principali tool di phishing.

6.1.1 Gophish

Gophish è un framework open source progettato per eseguire campagne di phishing simulato e testare la consapevolezza degli utenti. Questo tool è utilizzato principalmente a scopi etici, come parte dei programmi di formazione sulla sicurezza informatica all'interno delle organizzazioni. L'obiettivo principale di Gophish è educare le persone su come riconoscere e resistere agli attacchi di phishing. Il tool è sviluppato in Go (linguaggio di programmazione open-source sviluppato da google [65]) ed è disponibile per Windows,Mac Os e Linux. Un estratto di codice sorgente di Gophish è visibile in Fig. 6.1. Partendo dalla pagina di installazione è possibile installare Gophish per la piattaforma preferita, in questo caso Windows. L'installazione evidenzia l'intuitività del tool, facilmente accessibile anche ai meno esperti del settore. Nelle Figure 6.2 e 6.3 vengono mostrate le pagine di Login e la Home Page che l'utente visualizza dopo aver inserito le proprie credenziali.

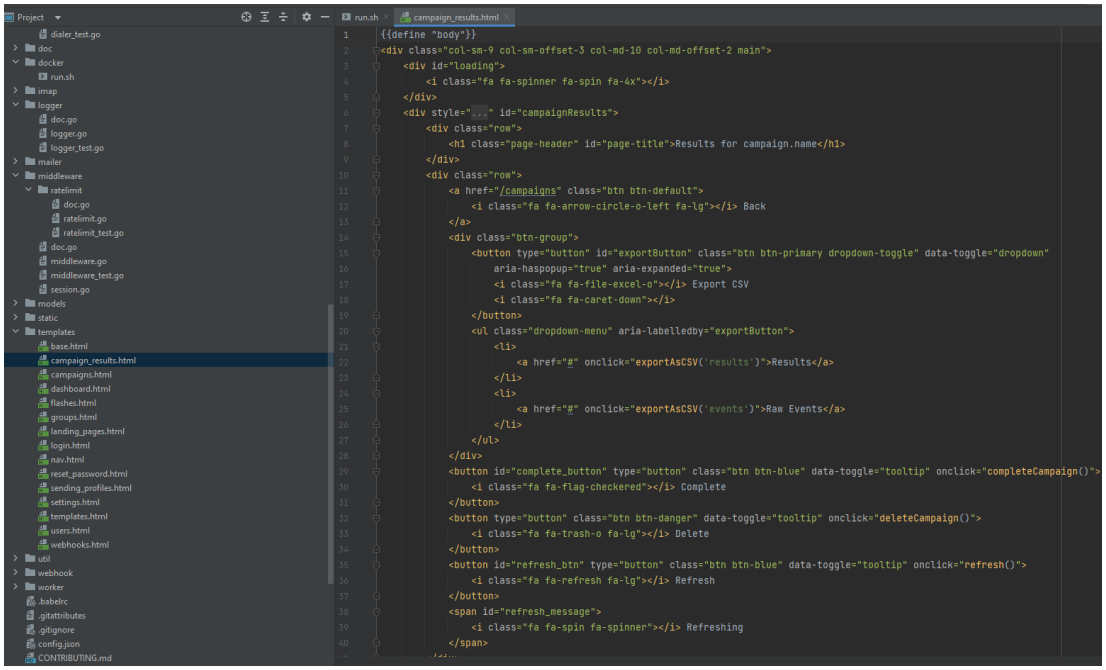


Figure 6.1: Uno screen del codice sorgente di Gophish.

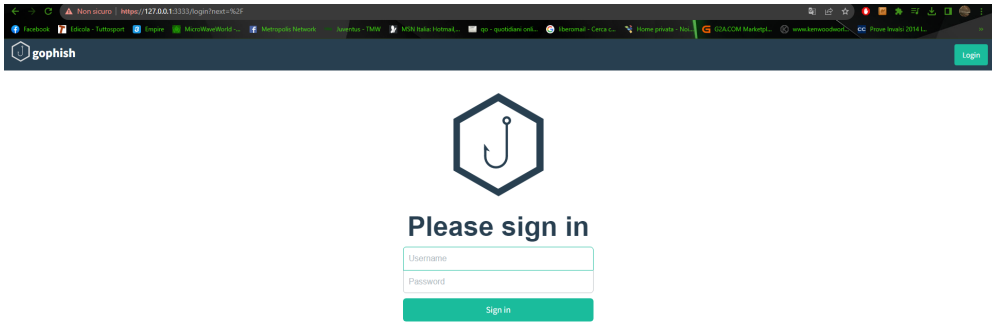


Figure 6.2: Pagina di Login di Gophish

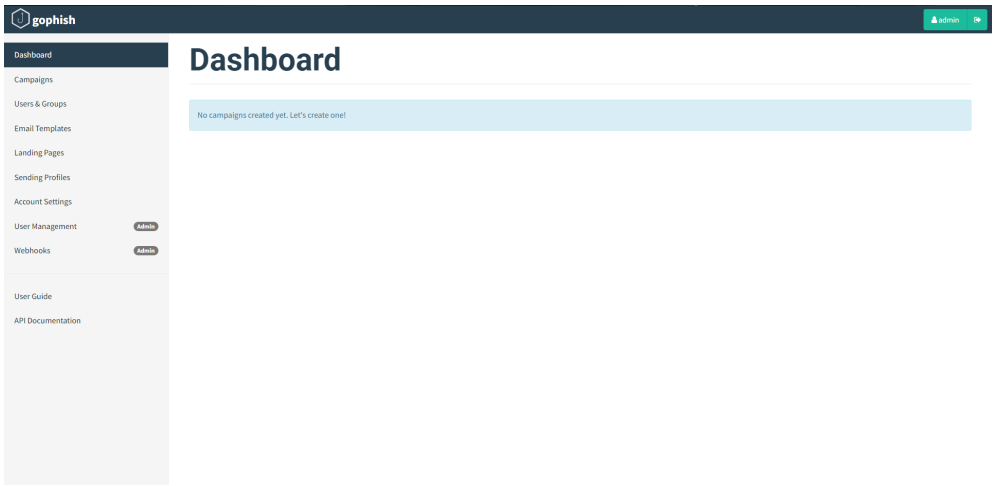


Figure 6.3: Home Page di Gophish

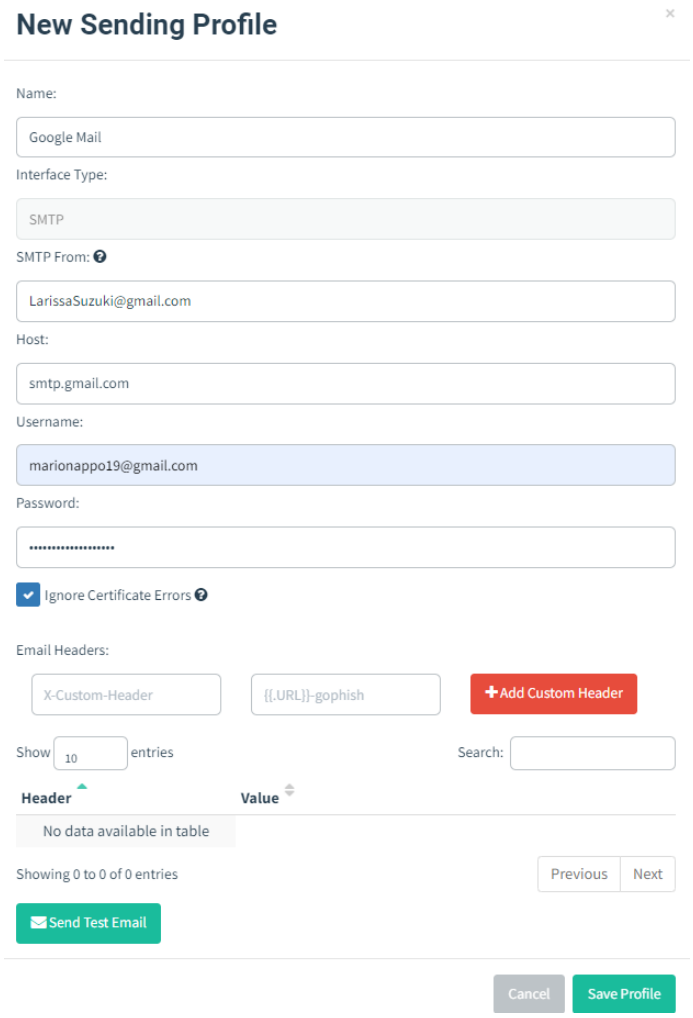


Figure 6.4: Creazione del profilo con cui verranno inviate le email di phishing su Gophish.

Gophish mette a disposizione diverse funzionalità, Di seguito dettagliate.

- **Sending Profiles.** Creare un profilo attraverso il quale inviare le email di phishing. Risulta necessario configurare le impostazioni del server SMTP che verrà utilizzato per inviare le email di phishing, l'indirizzo email che verrà utilizzato come mittente nelle email di phishing, un'email e password personali. In Figura 6.4 sono mostrati i campi da compilare. Infine, è possibile inviare un'email di test per vedere se la configurazione del profilo mittente è andata a buon fine come mostrato in Figura 6.5.

- **Email Templates.** Creare il template di un'email, fondamentale per una buona riuscita dell'attacco di phishing. Occorre inserire l'email del mittente,l'oggetto dell'email e il testo sotto forma di codice HTML. Gophish offre la possibilità di poter importare un'email già esistente clickando su "import email" e di modificarla a nostro piacere. Quando modifichiamo una email o una landing page è fondamentale aggiungere alcune delle variabili presenti in Figura 6.7. Ad esempio nella Figura 6.6, tra le varie cose, è stato aggiunto .FirstName, ciò contrassegna il nome delle vittime a cui è destinata l'email.

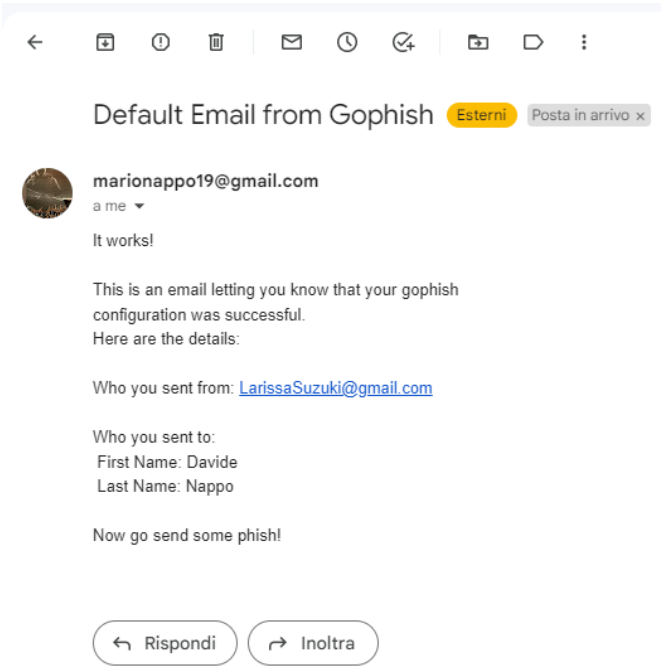


Figure 6.5: Esempio di email di test generata da Gophish

Template Reference

The following variables are available in templates and landing pages:

> Tip: Remember - Templates are *case sensitive*!

Variable	Description
{{.RId}}	The target's unique ID
{{.FirstName}}	The target's first name
{{.LastName}}	The target's last name
{{.Position}}	The target's position
{{.Email}}	The target's email address
{{.From}}	The spoofed sender
{{.TrackingURL}}	The URL to the tracking handler
{{.Tracker}}	An alias for `<img src="{{.TrackingURL}}"/>`
{{.URL}}	The phishing URL
{{.BaseURL}}	The base URL with the path and `rid` parameter stripped. Useful for making links to static files.

Figure 6.7: Template Reference di Gophish

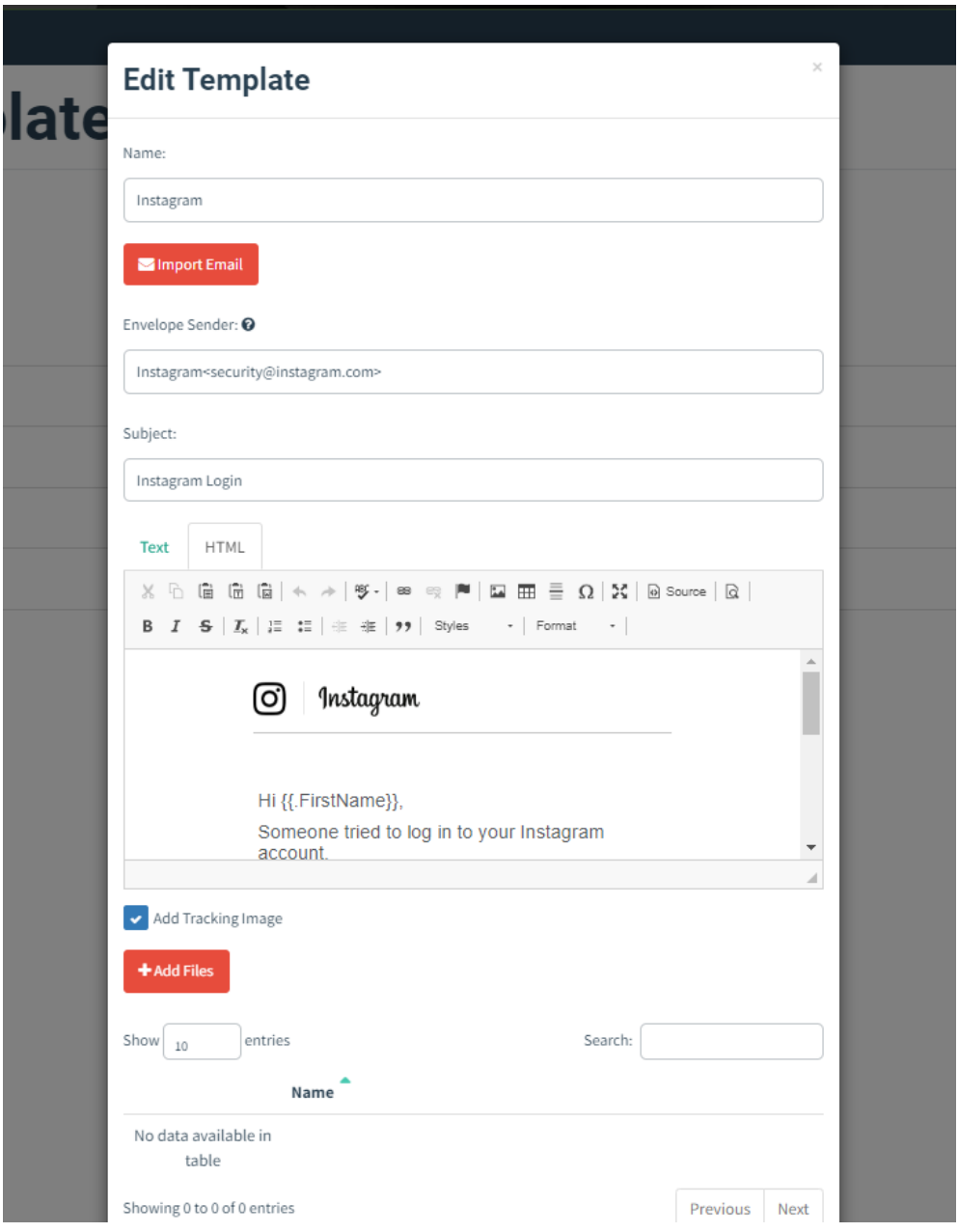


Figure 6.6: Schermata di modifica di un' email su Gophish

- **Landing Pages.** Creare il template della pagina su cui l'utente sarà indirizzato dopo aver cliccato il link malevolo all'interno dell'email. Gophish permette di inserire manualmente il codice HTML della pagina (su internet si trovano tanti codici già pronti all'uso) oppure di clonarlo importando l'url del sito che ci interessa, come mostrato nella Figura 6.8. Se si vogliono catturare i dati inseriti, tra cui le password, occorre spuntare le caselle in questione. Infine, si può inserire l'url del sito dove l'utente verrà reindirizzato dopo aver inserito le credenziali.

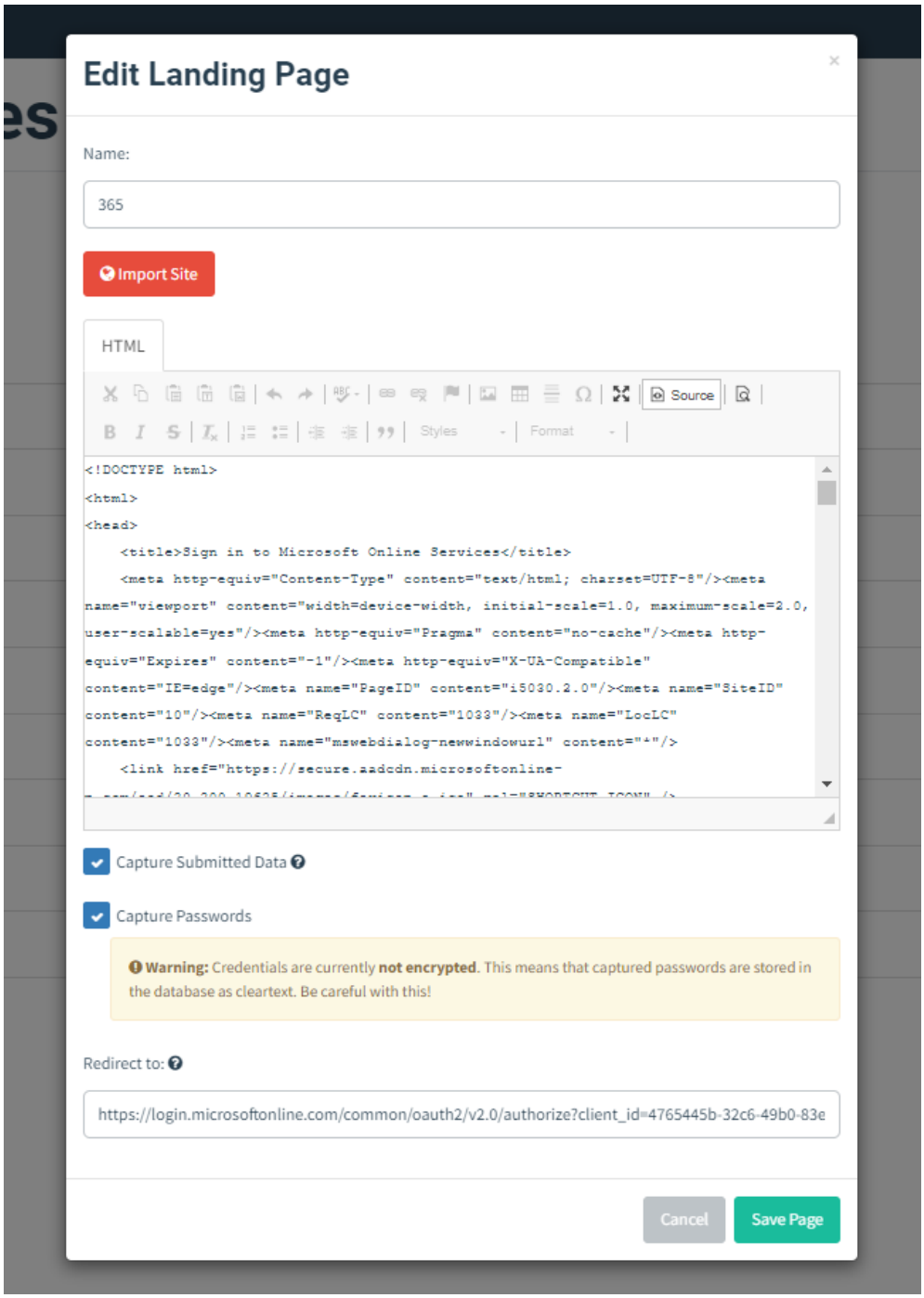


Figure 6.8: Schermata di modifica di una landing page su Gophish

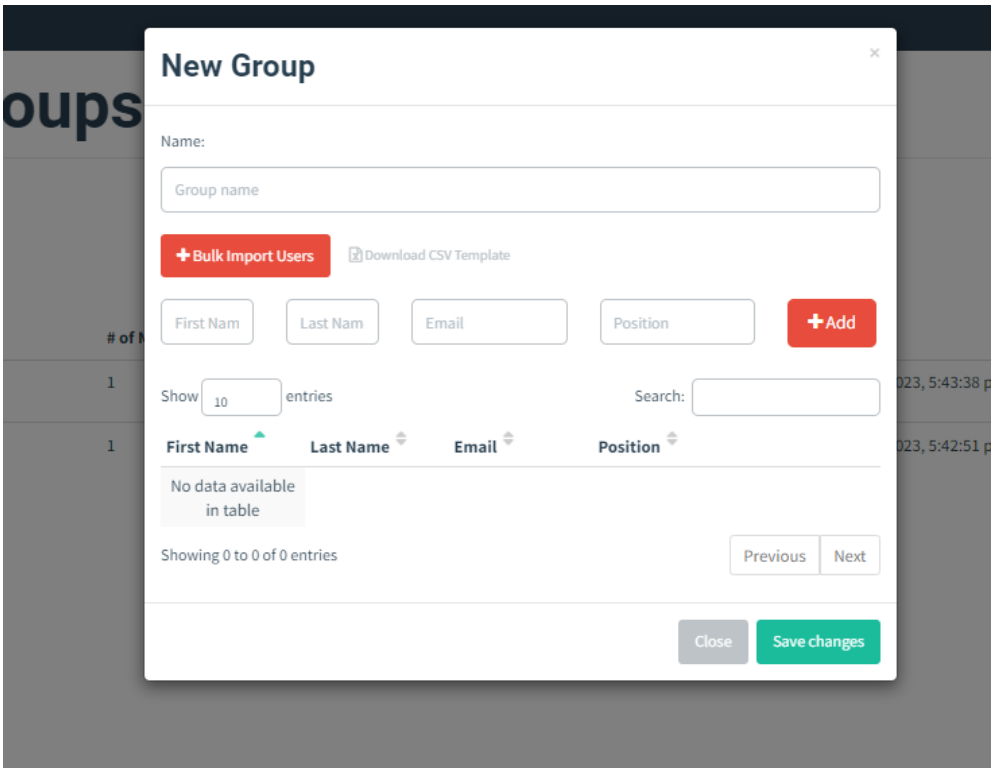


Figure 6.9: Campi da compilare per aggiungere utenti e gruppi su Gophish.

- **Users and Groups.** Inserire nomi,cognomi e email degli utenti che riceveranno le email. I campi da compilare vengono mostrati nella Figura 6.9.
- **Creating a Campaign.** Lanciare una campagna di phishing dandole un nome, il template dell'email, la landing page, un url valido, la data di lancio, il sending profile e gli utenti a cui verranno inviati le email, come mostrato nell'immagine 6.10.
- **Demo and Reports.** Monitorare l'andamento della campagna di phishing attraverso il numero di email inviate, aperte, di click sui link ed è possibile visualizzare i dati quali username e password inseriti dagli utenti. Uno screenshot della dashboard è fornito nella Figura 6.11

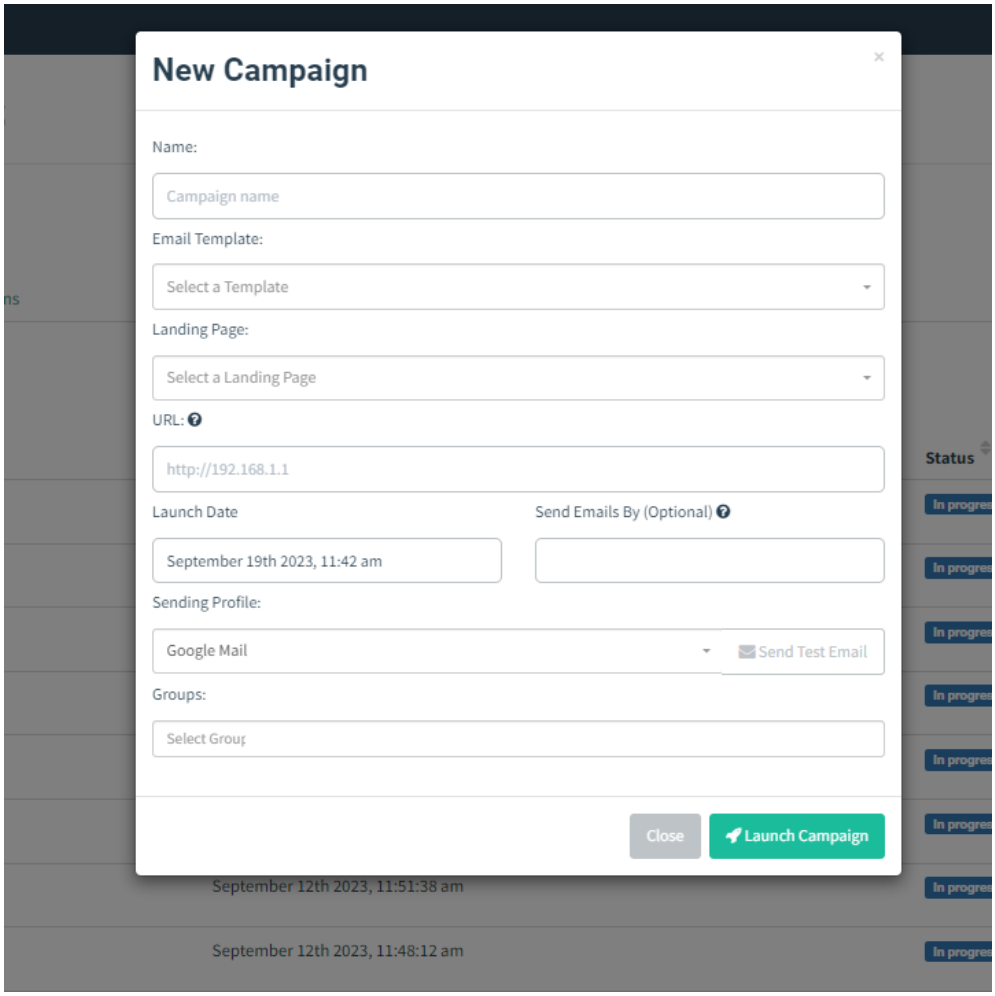


Figure 6.10: Campi da compilare per creare una nuova campagna di Gophish.

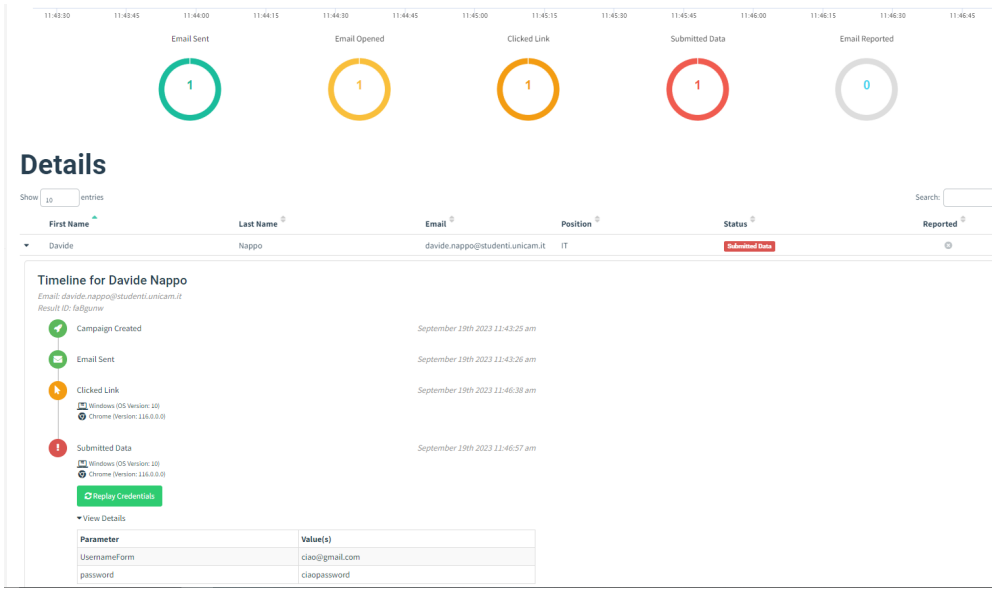


Figure 6.11: Dashboard di Gophish in cui è possibile vedere l'andamento della campagna di phishing ed eventuali dati sulle vittime.

6.1.2 PyPhisher

PyPhisher è uno strumento di phishing open source scritto in Python. Questo strumento è progettato per condurre campagne di phishing, consentendo agli utenti di creare pagine web di phishing per ingannare le vittime e ottenere informazioni sensibili come nomi utente, password e altre credenziali.
PyPhisher presenta queste caratteristiche:

- **Interfaccia da riga di comando:** PyPhisher è basato su un'interfaccia da riga di comando che consente agli utenti di configurare e gestire le loro campagne di phishing.
- **Personalizzazione delle pagine di phishing:** Gli utenti possono personalizzare le pagine di phishing per farle sembrare autentiche e convincenti per le vittime. Tale tool permette anche di poter utilizzare finte pagine in cui viene richiesto il codice OTP.
- **Registrazione delle informazioni delle vittime:** PyPhisher registra le informazioni delle vittime che cadono nell'inganno, consentendo agli utenti di raccogliere dati sul successo della campagna.
- **Dati dettagliati:** Fornisce dati dettagliati sulle vittime, inclusi dati come l'ip, il sistema operativo su cui è stato aperto il link e le credenziali raccolte.
- **Open Source:** PyPhisher è open source, il che significa che il suo codice sorgente è accessibile e può essere personalizzato dagli utenti.

Vediamo nel dettaglio come funziona tale tool:

1. **Installazione:** L'installazione è semplice e può essere fatta seguendo le indicazioni scritte sulla pagina github dell'autore[1]. Il tool in questo caso è stato scaricato su una macchina virtuale con Kali Linux come sistema operativo.
2. **Avvio del tool:** l'avvio avviene spostandosi nella cartella dove è stato scaricato il tool, in questo caso il comando da digitare è "cd PyPhisher"e successivamente "python3 pyphisher.py" per avviare il tool. Nella finestra di avvio viene presentata la lista dei siti fake disponibili all'uso come testimoniato dall'immagine 6.12.
3. **Esecuzione:** Nella Figura 6.13 viene mostrato il tool in esecuzione. Viene selezionata l'opzione 05 facente riferimento alla pagina Instagram tradizionale. Viene domandato se si vuole utilizzare anche una pagina OTP in cui viene richiesto il codice temporaneo, una protezione in più che solitamente viene inviata all'utente per verificare se sia effettivamente lui ad accedere. In questo caso viene risposto di sì e viene inserito il link di reindirizzamento alla vera pagina di Instagram dove la vittima verrà portata dopo aver inserito le credenziali e il codice OTP.

Successivamente il tool inizializza un server PHP sul localhost:8080 e i tunnelers utilizzando Cloudflared. I tunellers consentono di rendere visibile su rete internet globale ciò che è in esecuzione sul localhost della nostra macchina e sono approfonditi nella

[1] https://github.com/KasRoudra/PyPhisher

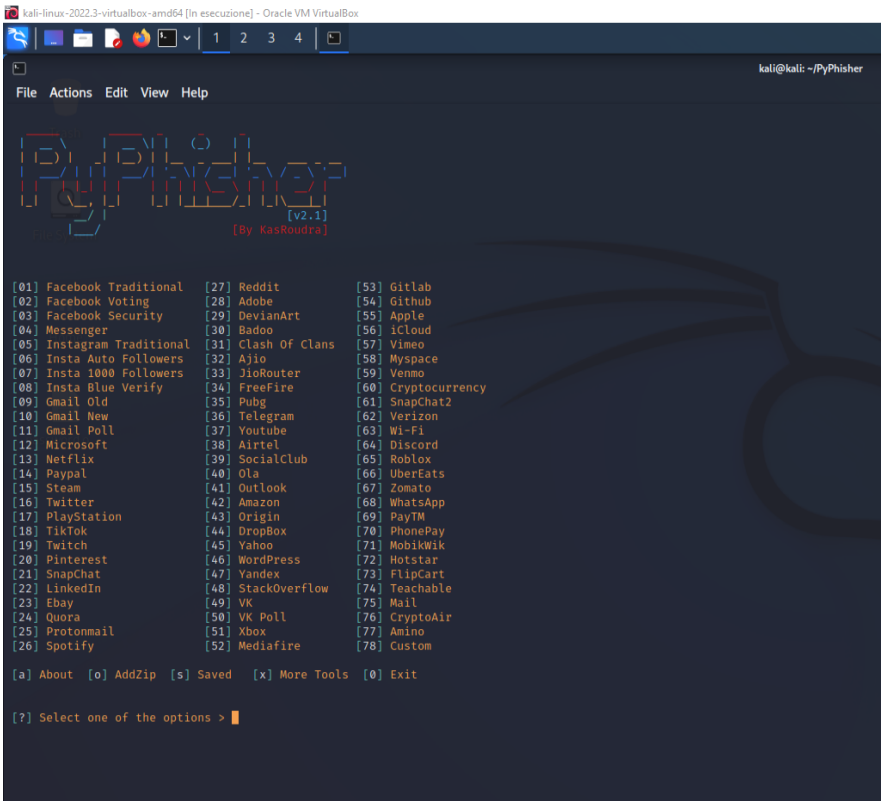


Figure 6.12: Schermata di avvio di PyPhisher

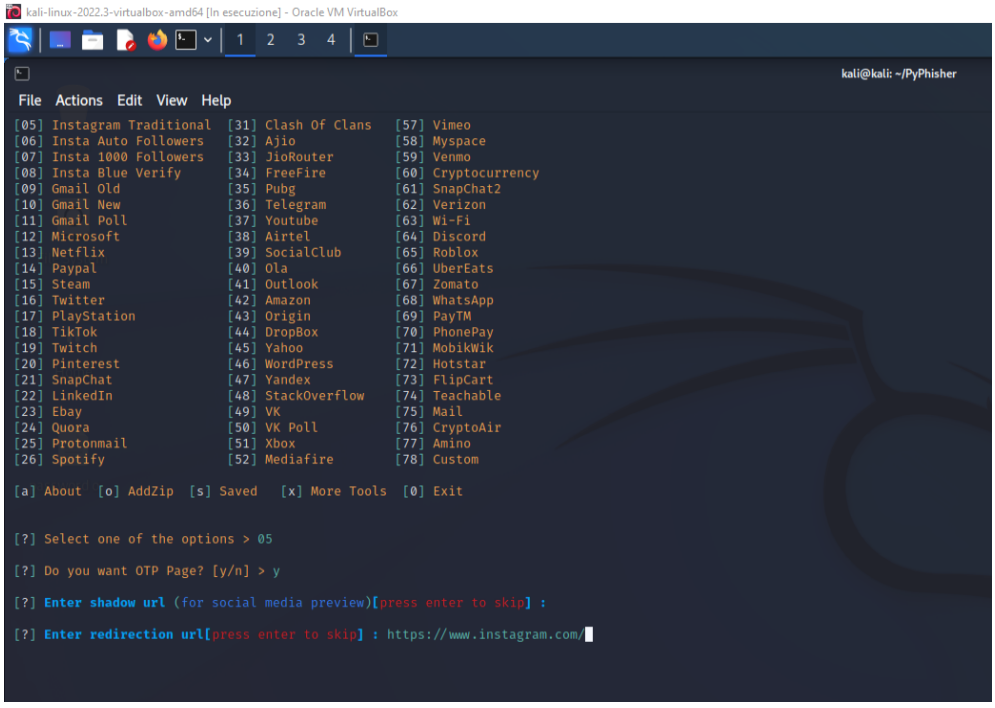


Figure 6.13: Schermata di esecuzione del tool.

Sezione 6.2 di questa tesi. In questo caso viene anche provato a customizzare l'url, e, alla fine verrà fornito il link alla pagina di phishing come è possibile vedere in 6.14.

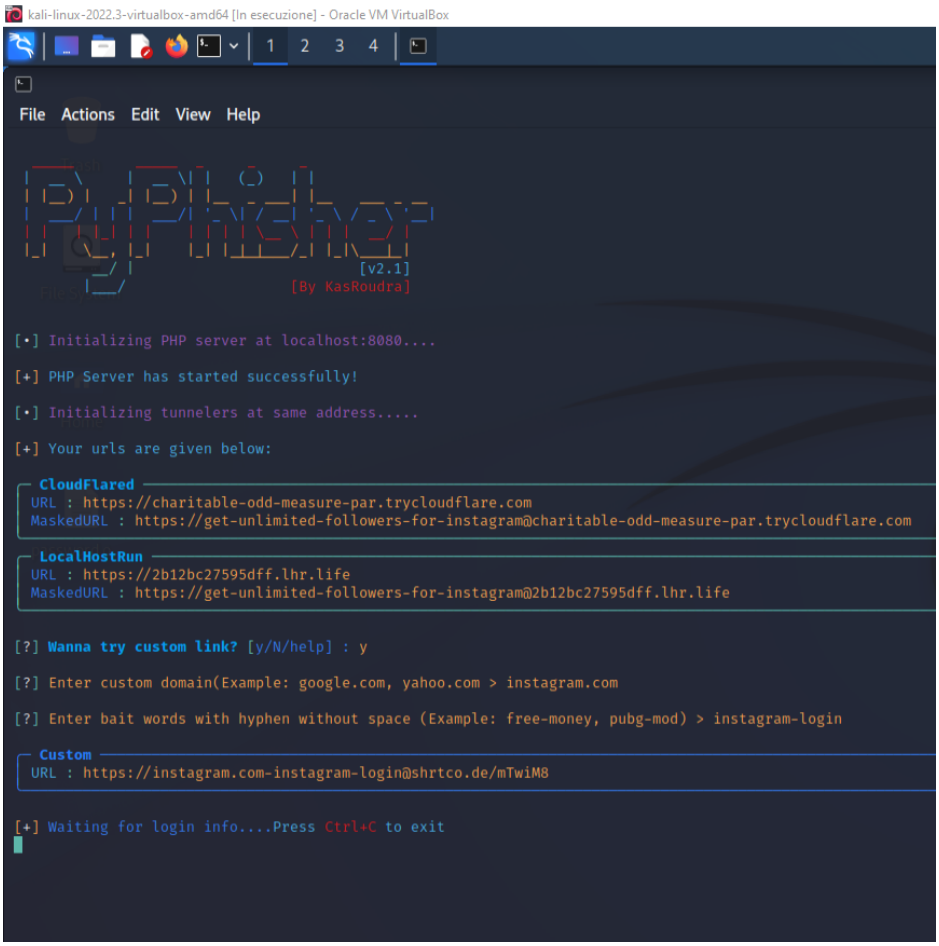


Figure 6.14: Schermata di esecuzione del tool. In questa immagine è possibile vedere la creazione del link della pagina di phishing

Clickando sul link la vittima arriva nella pagina di phishing, quasi identica a quella originale. Uno screen della pagina è visibile in Figura 6.15. Dopo aver inserito le credenziali viene dirottata sulla pagina in cui viene richiesto il codice OTP e dopo averlo inserito arriva alla vera pagina di Instagram. I dati della vittima, tra cui indirizzo Ip, sistema operativo usato e le credenziali, compreso codice temporaneo per l'autenticazione a 2 fattori, vengono visualizzate e salvate in un file di testo. Attraverso le successive immagini 6.16, 6.17, 6.18 e 6.19 è possibile vedere tutto quello descritto nelle righe precedenti.

Da questa breve descrizione di PyPhisher si evince come esso sia un tool dalle molteplici funzionalità, pericoloso ed estremamente facile da usare. L'utente può non cadere nella trappola del malitenzionato osservando attentamente l'url del sito di phishing, diverso da quello della pagina originale di Instagram. Prestare attenzione è una forma di difesa utilissima. Inoltre, è importante notare che l'uso di PyPhisher o di qualsiasi altro strumento di phishing per scopi illegali o fraudolenti è illegale e può comportare conseguenze legali gravi. Questi strumenti dovrebbero essere utilizzati solo a fini di test di sicurezza legittimi o per dimostrare vulnerabilità nei sistemi di sicurezza.

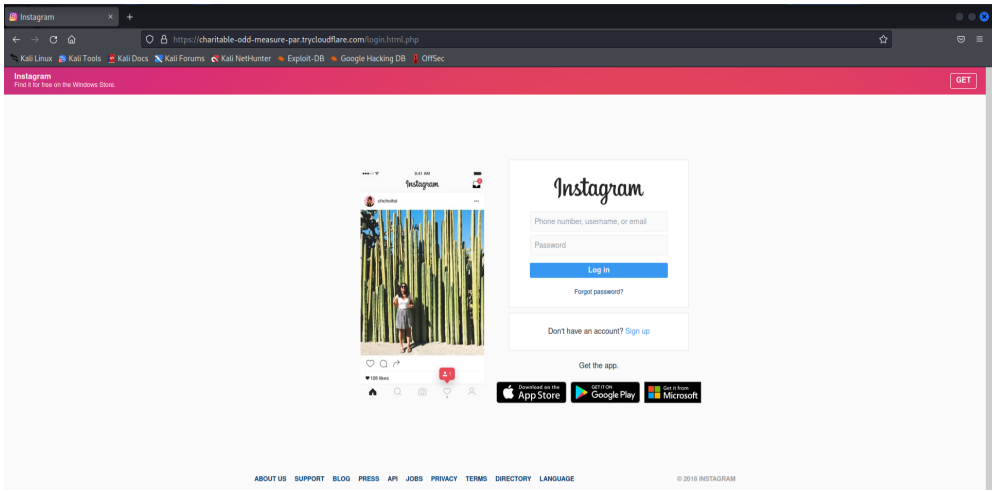


Figure 6.15: Pagina di phishing con template basato sulla login page di Instagram.

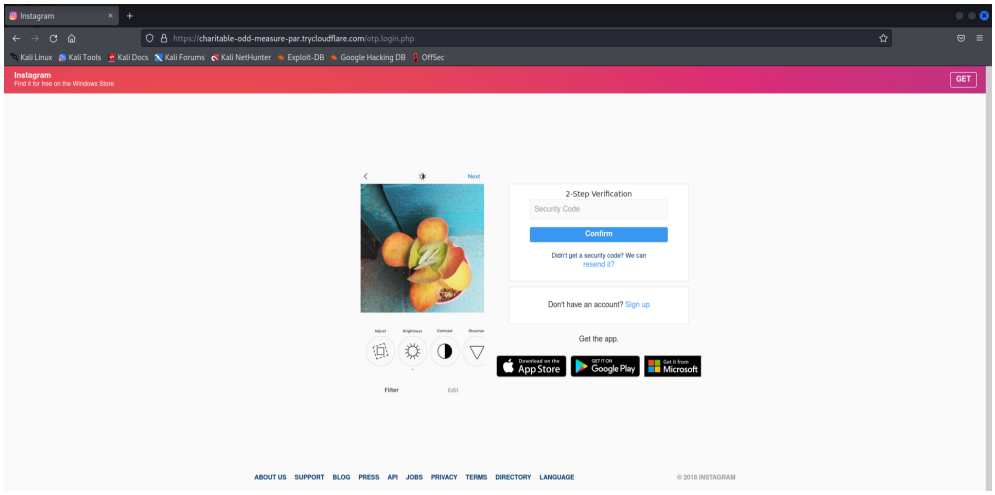


Figure 6.16: Pagina di phishing con template basato sulla pagina dell'autenticazione a 2 fattori di Instagram.

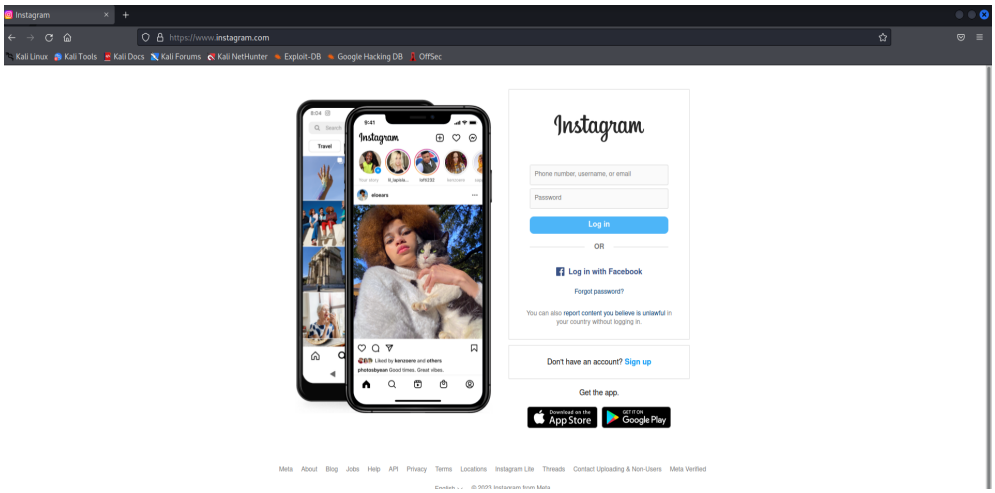


Figure 6.17: Pagina reale di Instagram su cui viene reindirizzata la vittima.

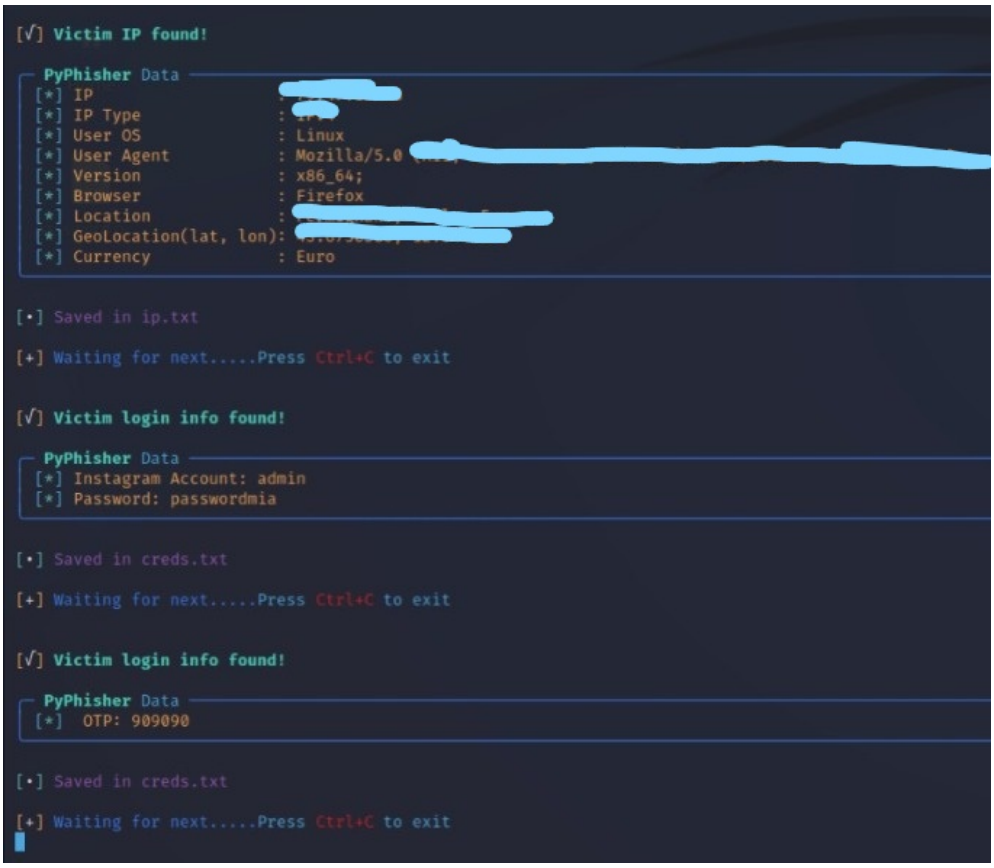


Figure 6.18: Credenziali catturate. Nella foto vengono censurati alcuni dati della vittima.

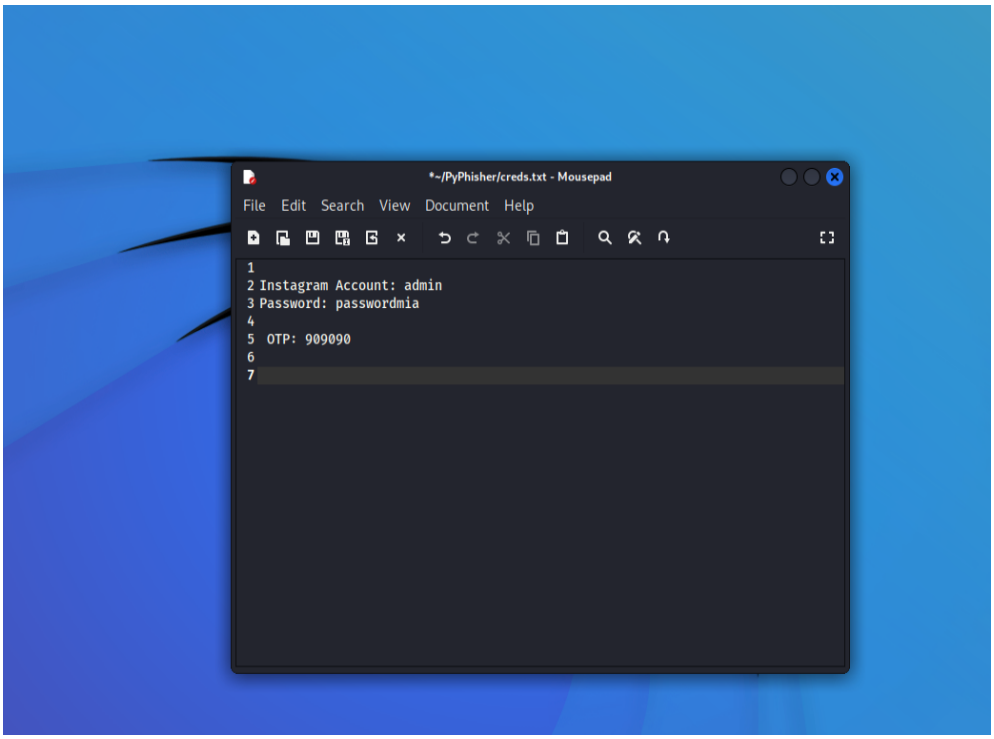


Figure 6.19: File di testo su cui vengono salvate le credenziali e il codice OTP.

6.1.3 PhishInsight

PhishInsight è un'applicazione e servizio di addestramento e simulazione di phishing sviluppato da Trend Micro, un'importante azienda di sicurezza informatica. PhishInsight è progettato per aiutare le organizzazioni a migliorare la consapevolezza sulla sicurezza informatica dei propri dipendenti attraverso l'addestramento, le simulazioni di phishing e la generazione di report dettagliati. La scelta di approfondire tale tool è dovuta alla presenza al suo interno di una sezione che permette di addestrare i dipendenti sul phishing dando enfasi alla formazione del personale, cosa fondamentale per la lotta a questo tipo di attacco informatico. Di seguito verrà spiegato come creare una campagna di phishing utilizzando tale tool attraverso vari passi.

- **Creazione dell'email di phishing.** Phish Insight permette di selezionare tra una moltitudine di email templates già presenti nella piattaforma. E' possibile scegliere i template in base alla lingua con cui questi sono scritti (ad esempio italiano o inglese), la loro difficoltà nell'essere riconosciuti, l'argomento e ciò che è contenuto (ad esempio link o documenti allegati). Partendo dalla base dei template è possibile modificare le email in maniera simile a quanto accadeva per GoPhish,analizzato nella Sottosezione 6.1.1. La modifica dell'email coinvolge diversi aspetti tra cui: nome del template, nome e indirizzo email del mittente, landing page collegata al link, contenuto, oggetto ecc.. Tali modifiche possono essere salvate in modo da creare un template da utilizzare per campagne successive. Tutto ciò viene rappresentato nelle Figure 6.20, 6.21, 6.22, 6.23.

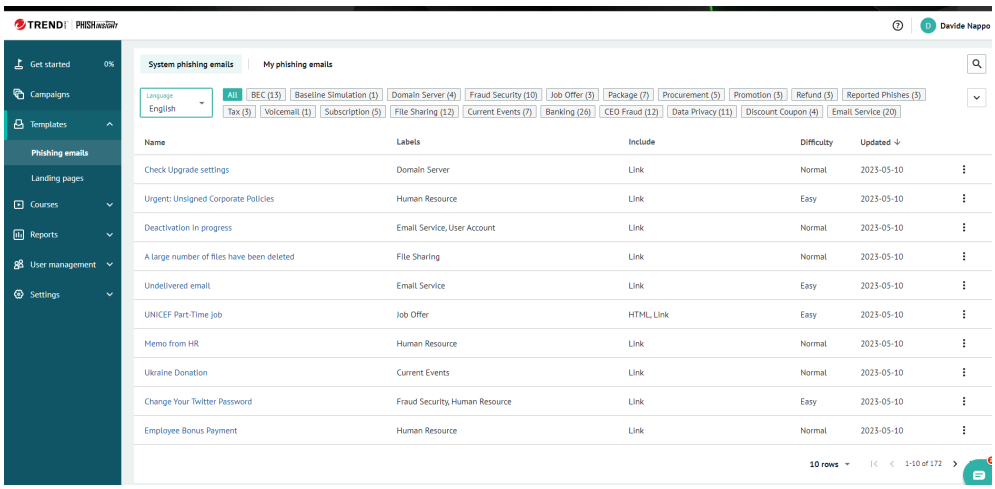


Figure 6.20: Lista degli email template presenti su PhishInsight con testo in inglese.

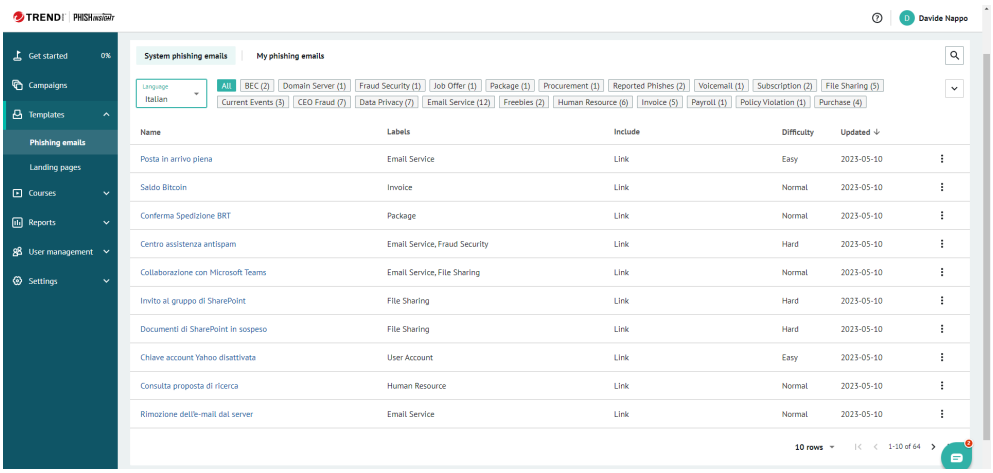


Figure 6.21: Lista degli email template presenti su PhishInsight con testo in italiano.

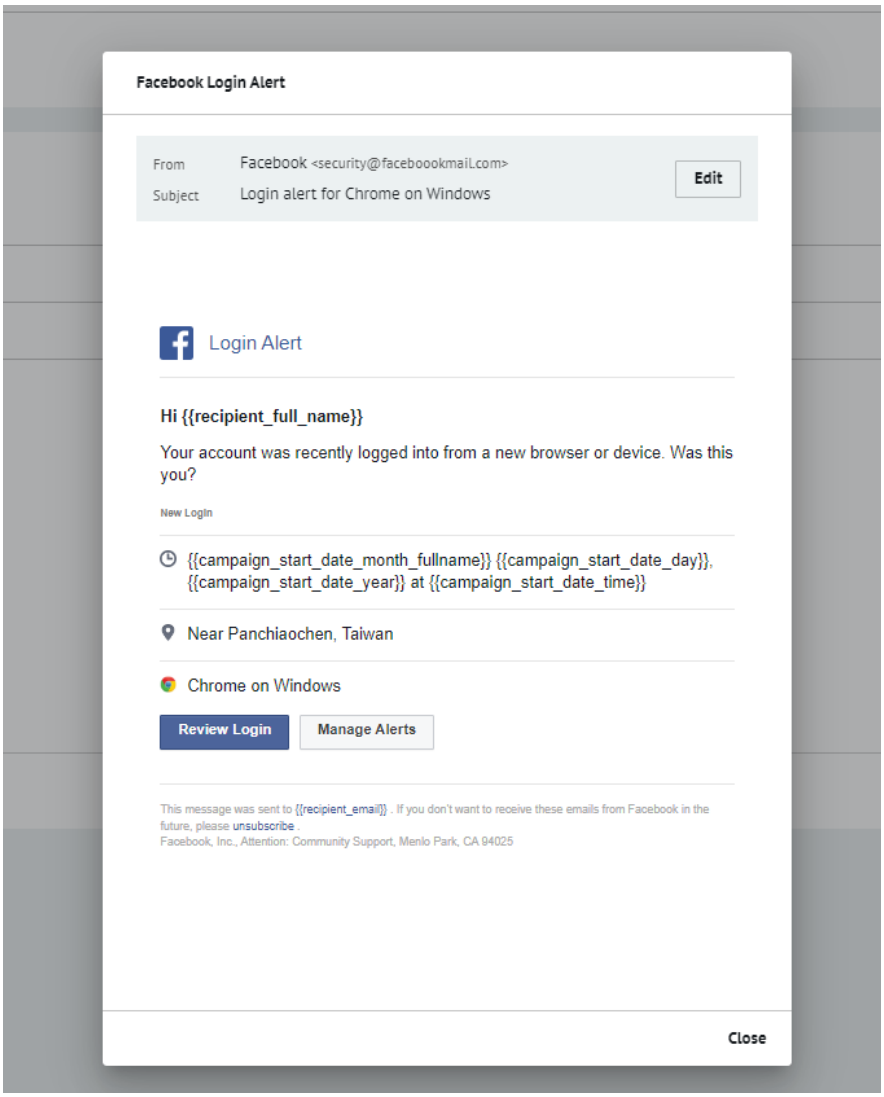


Figure 6.22: Email template di tentato accesso all'account Facebook.

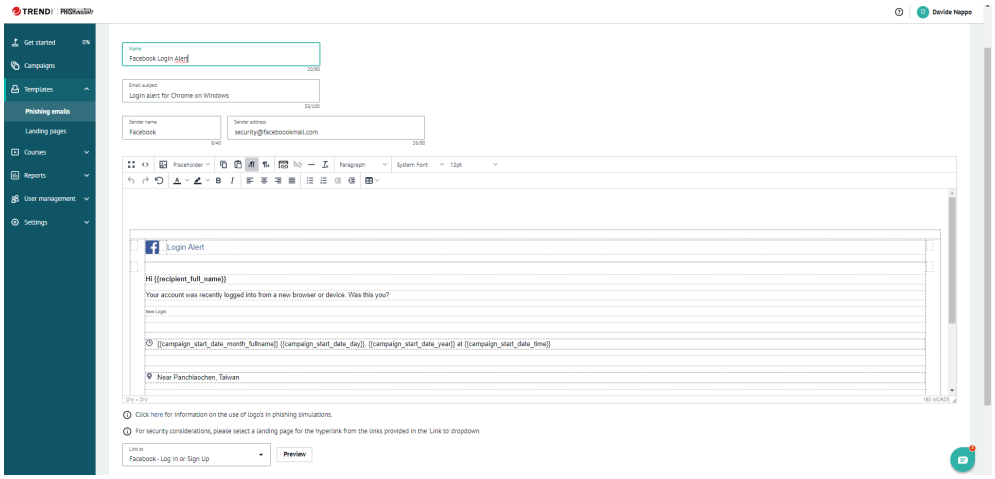


Figure 6.23: Schermata di modifica di un template email su PhishInsight.

- **Creazione della landing page.** La landing page è la pagina in cui la vittima viene reindirizzata dopo aver clickato il link presente nell'email di phishing. Come nel caso dell'email è possibile scegliere tra una moltitudine di template già presenti, modificarli all'occorrenza e salvarli, in maniera identica. Ad esempio nella Figura 6.24 viene mostrato il template di una landing page clone di Facebook.

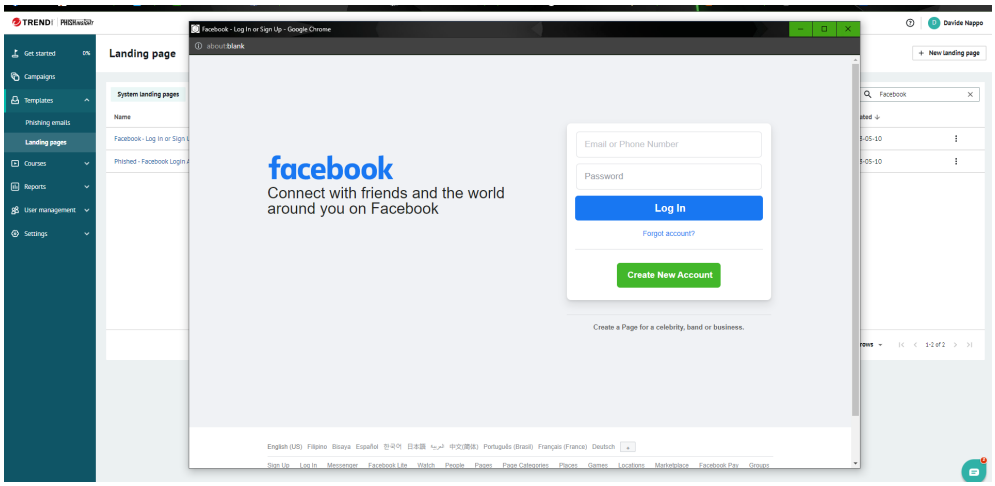


Figure 6.24: Landing page di Facebook.

- **Creazione della lista di vittime.** Clickando su User Management è possibile creare i singoli utenti compilando i dati necessari quali nome, cognome, email ecc.. oppure importarne una lista selezionando "import user list". Successivamente tali utenti possono essere accorpati in un gruppo a cui viene dato un nome e la lista degli utenti che lo compongono. I dati da inserire per creare uno user e un nuovo gruppo sono mostrati nelle Figure 6.25 e 6.26.

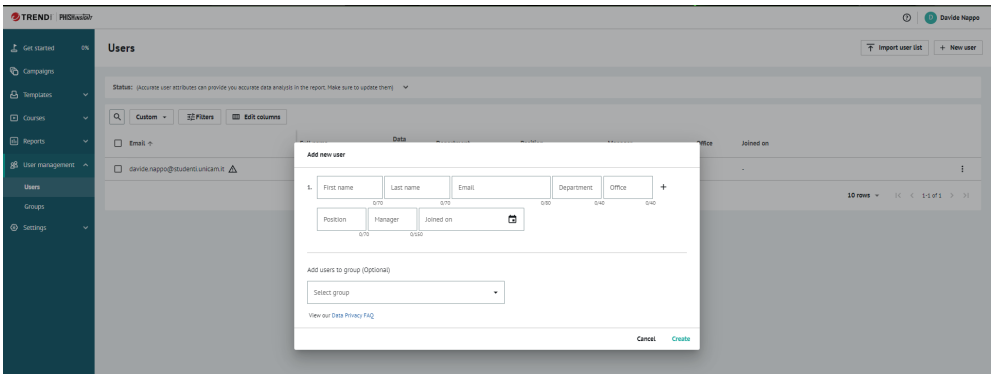


Figure 6.25: Dati da compilare per aggiungere un utente alla user list su PhishInsight.

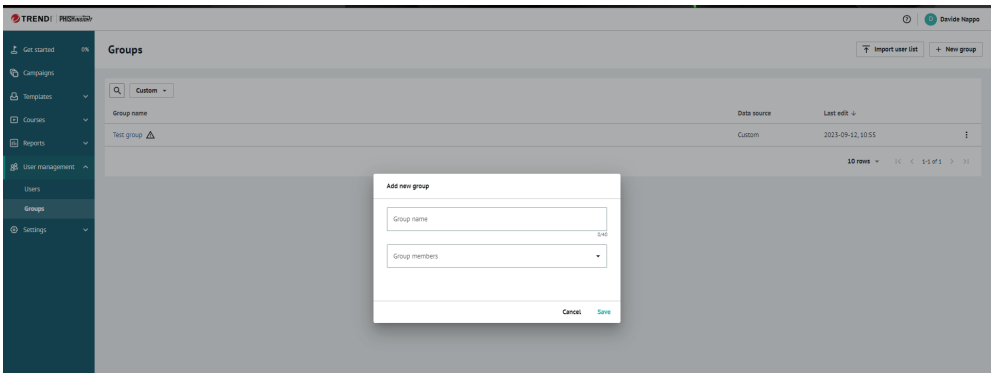


Figure 6.26: Dati da compilare per creare un nuovo gruppo ed aggiungervi uno user su PhishInsight.

- **Creazione campagna.** Per creare una campagna basta posizionarsi su "Campaigns" e clickare su "new campaign". Dopo aver inserito i dati richiesti tra cui nome della campagna, tipo di simulazione, email di phishing da usare, landing page, orario di inizio e fine. Con "create campaign" viene creata ufficialmente la campagna di phishing. La fase successiva consiste nel monitoraggio dei dati. Nelle Figure 6.27, 6.28, 6.29, 6.30 è possibile vedere tutta la procedura che porta all'effettiva creazione e realizzazione della campagna. In Figura 6.31 è mostrato il messaggio che l'utente riceve dopo essere caduto vittima della simulazione di phishing.

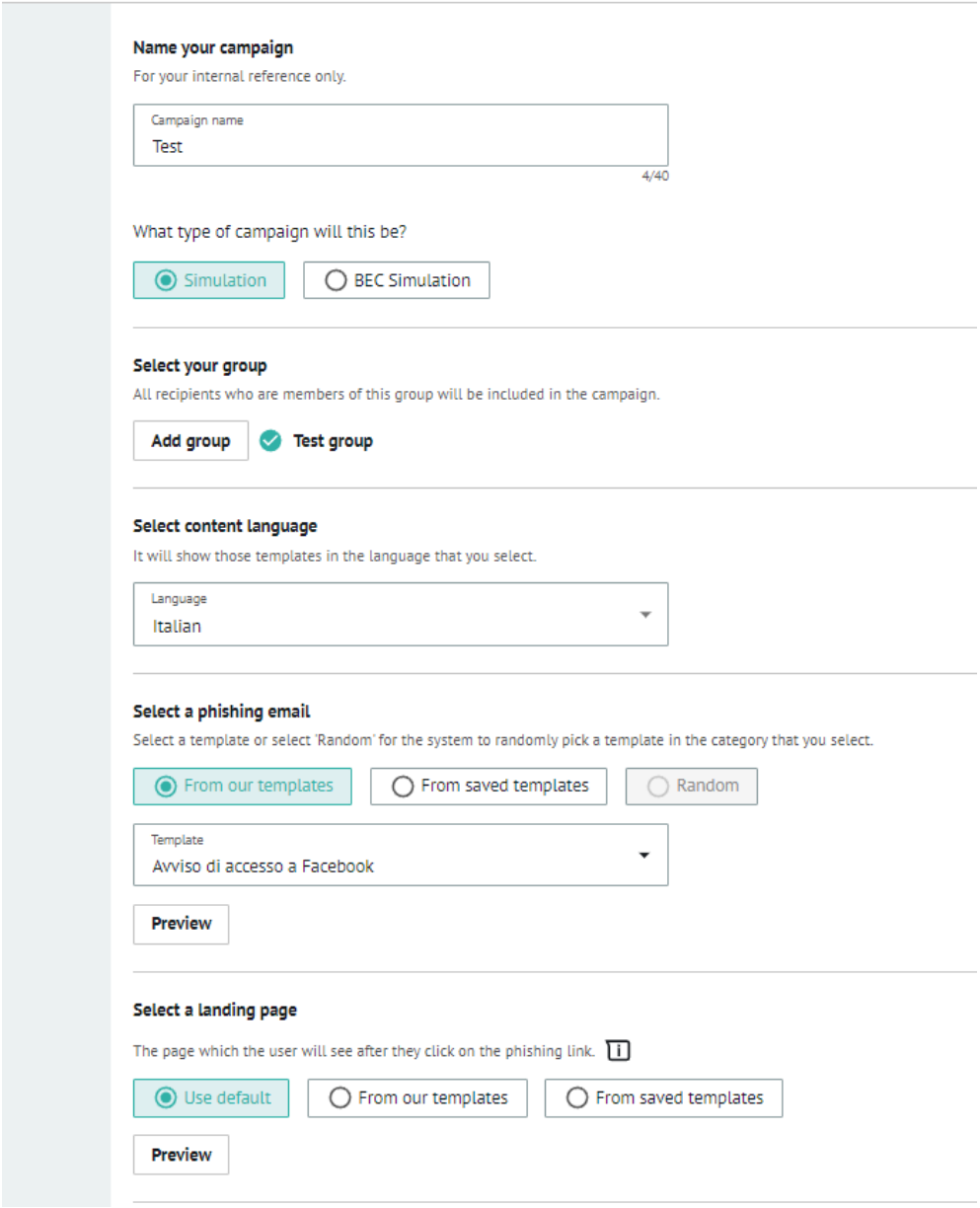


Figure 6.27: Prima parte dei dati da inserire per avviare una campagna con PishInsight.

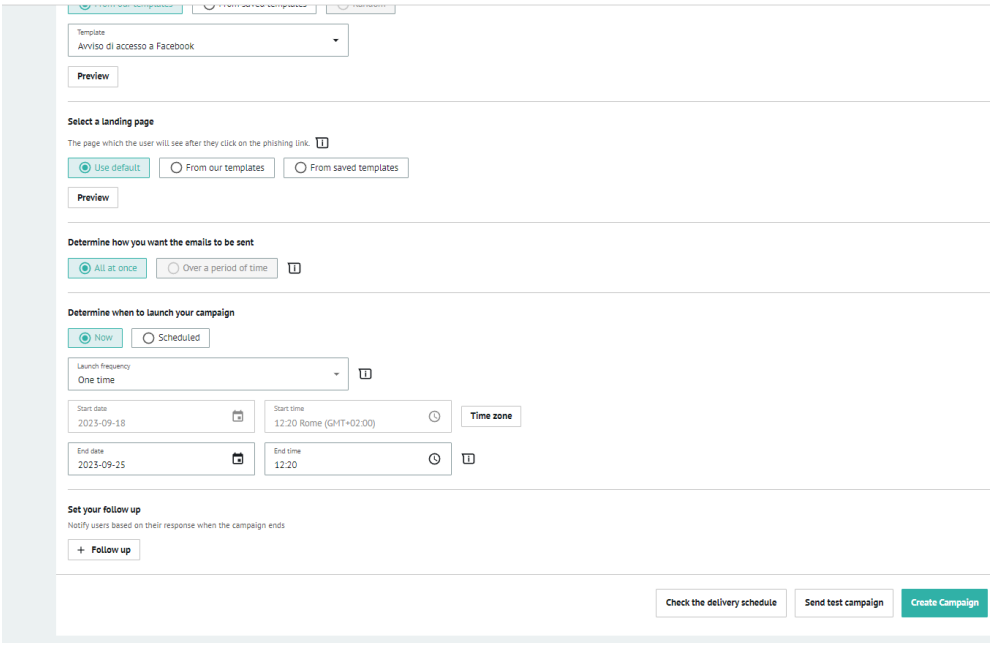


Figure 6.28: Seconda parte dei dati da inserire per avviare una campagna con PishInsight.

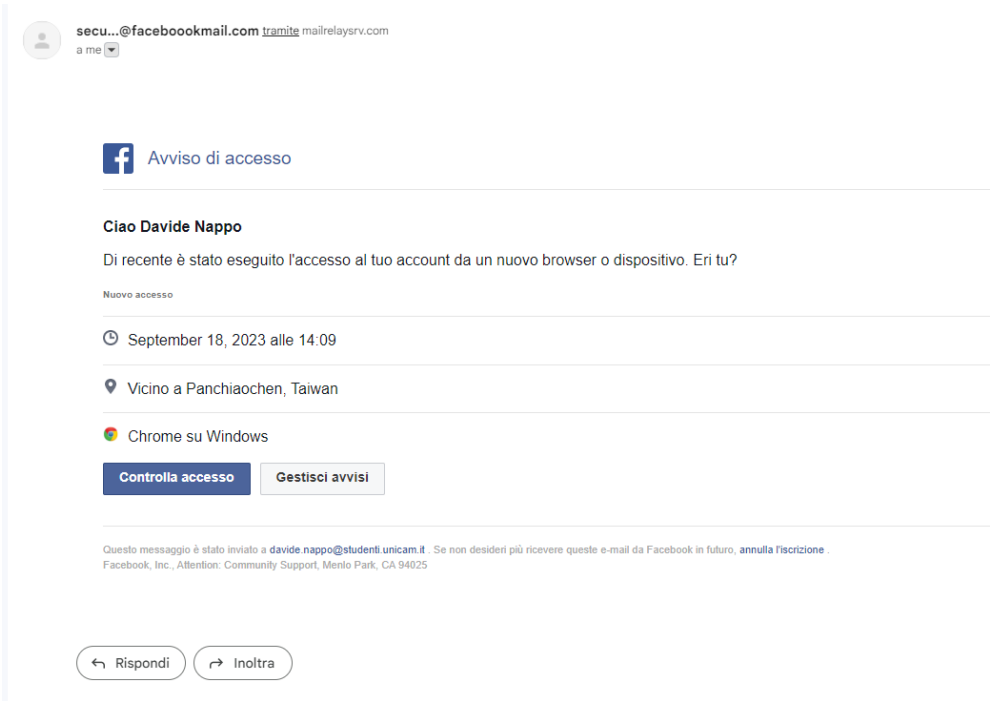


Figure 6.29: Email di pishing della campagna avviata, presente come template in PishInsight.

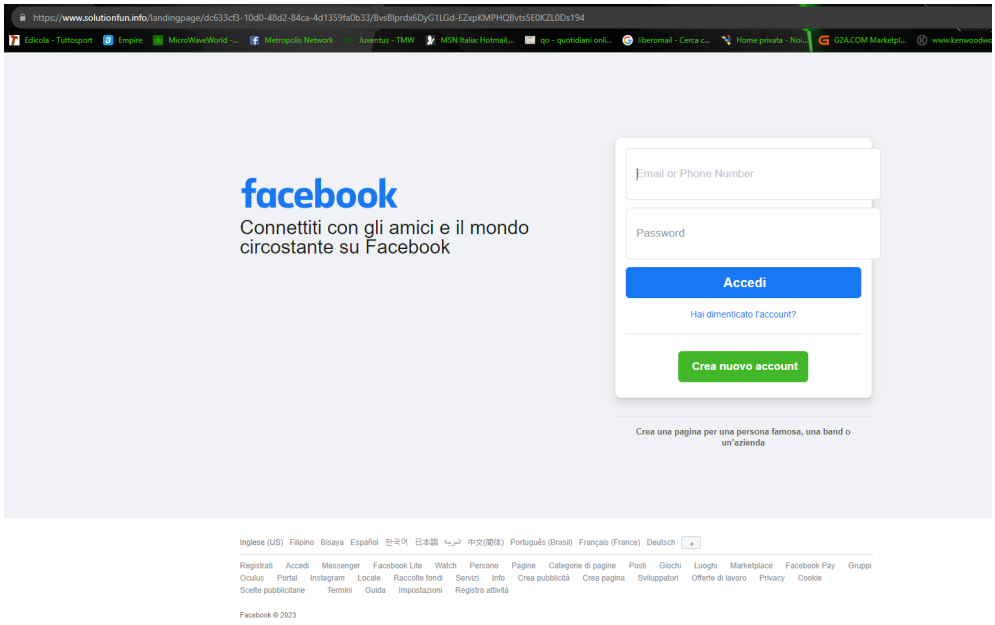


Figure 6.30: Landing page di Facebook della campagna avviata, presente come template in PishInsight. La vittima arriva qui dopo aver clickato il link presente nell'email.

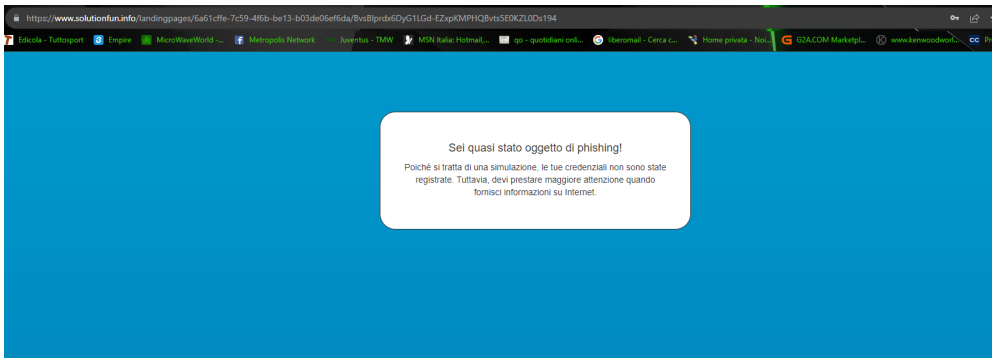


Figure 6.31: Messaggio a cui l'utente viene reindirizzato dopo essere caduto vittima della simulazione di phishing.

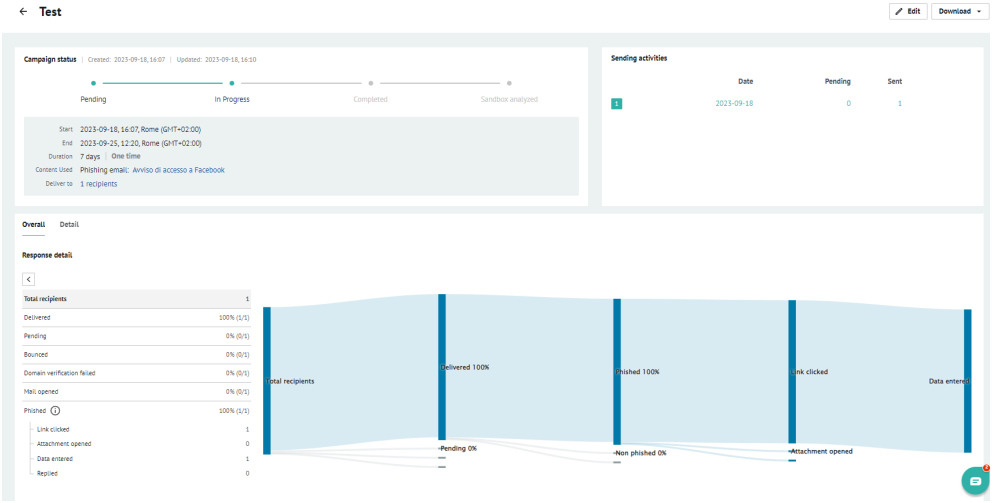


Figure 6.32: Dashboard di PhishInsight che mostra i dati sulla campagna di phishing avviata.

- **Monitoraggio.** Facendo click sulla campagna avviata PhishInsight permette di tenere traccia del numero di utenti che hanno ricevuto l'email, quanti sono cascati nella trappola, quanti hanno visitato il link presente nell'email e inserito i dati. Un esempio della dashboard di monitoraggio è visibile in Figura 6.32.

Una peculiarità di PhishInsight è il suo focus sulla formazione dato da alcuni elementi:

- **Corsi di Formazione:** PhishInsight offre una serie di corsi di formazione sulla sicurezza informatica. Questi corsi coprono una vasta gamma di argomenti, tra cui i concetti di base della sicurezza informatica, le tattiche utilizzate dai truffatori online e le migliori pratiche per riconoscere le minacce.

- **Moduli Interattivi:** I corsi di formazione sono presentati attraverso moduli interattivi che coinvolgono gli utenti. Questi moduli possono includere video, quiz, esercitazioni pratiche e scenari di attacco simulati. Questo approccio coinvolgente rende il training più efficace ed è progettato per mantenere l'attenzione degli utenti.

- **Adattamento ai Livelli di Competenza:** PhishInsight consente di adattare il training ai diversi livelli di competenza degli utenti. Ciò significa che sia i principianti che gli utenti esperti possono trarre beneficio dai corsi. Gli utenti possono essere indirizzati verso contenuti appropriati in base alle loro esigenze.

- **Monitoraggio della Progressione:** L'azienda può monitorare la progressione degli utenti attraverso i corsi di formazione. Questo consente di identificare chi sta progredendo bene e chi potrebbe avere bisogno di ulteriore formazione.

- **Report e Analisi:** PhishInsight fornisce report dettagliati sull'andamento del training e sulle prestazioni degli utenti. Questi report possono aiutare l'azienda a identificare i dipendenti che potrebbero richiedere ulteriore formazione o supporto.

- **Simulazioni di Phishing:** Oltre ai corsi di formazione, PhishInsight offre la possibilità di effettuare simulazioni di phishing. Queste simulazioni consentono

agli utenti di mettere in pratica ciò che hanno imparato nei corsi. Gli utenti riceveranno messaggi di phishing simulati e verranno monitorati per valutare la loro risposta.

- **Valutazione della Consapevolezza:** Il training di PhishInsight non si limita a fornire informazioni; è progettato per valutare e migliorare la consapevolezza sulla sicurezza informatica degli utenti. Il training mira a rendere gli utenti più vigili e a prepararli per riconoscere e gestire situazioni reali di phishing.

Nelle Figure 6.33, 6.34, 6.35 vengono mostrati esempi della componente di formazione offerta da Trend Micro PhishInsight.

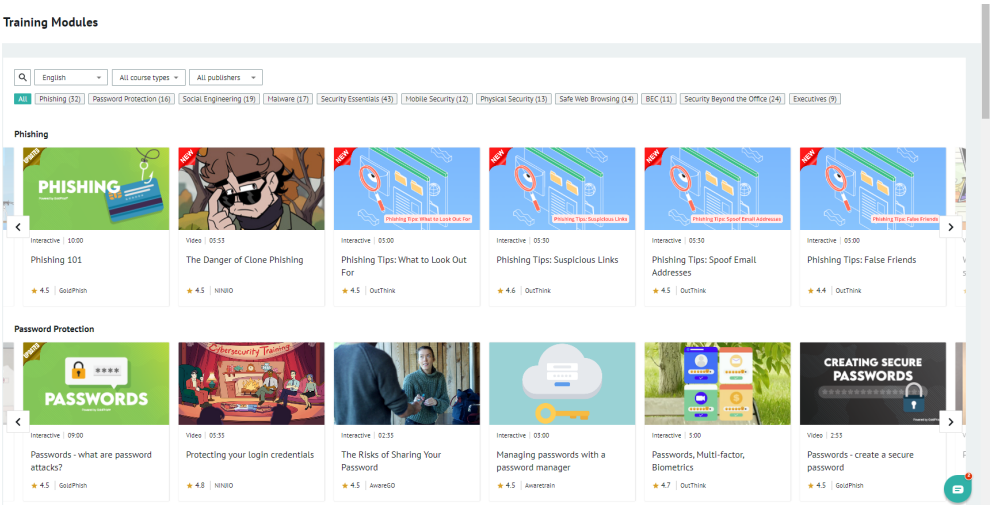


Figure 6.33: Alcuni dei moduli di allenamento presenti su PhishInsight.

In particolare nella Figura 6.36 è presente una lista di moduli in italiano utili per la formazione degli utenti contro il phishing.

In generale, il training di PhishInsight è una componente chiave per migliorare la consapevolezza sulla sicurezza informatica degli utenti aziendali. Offre un approccio completo alla formazione, alla valutazione e al miglioramento della sicurezza informatica all'interno di un'organizzazione.

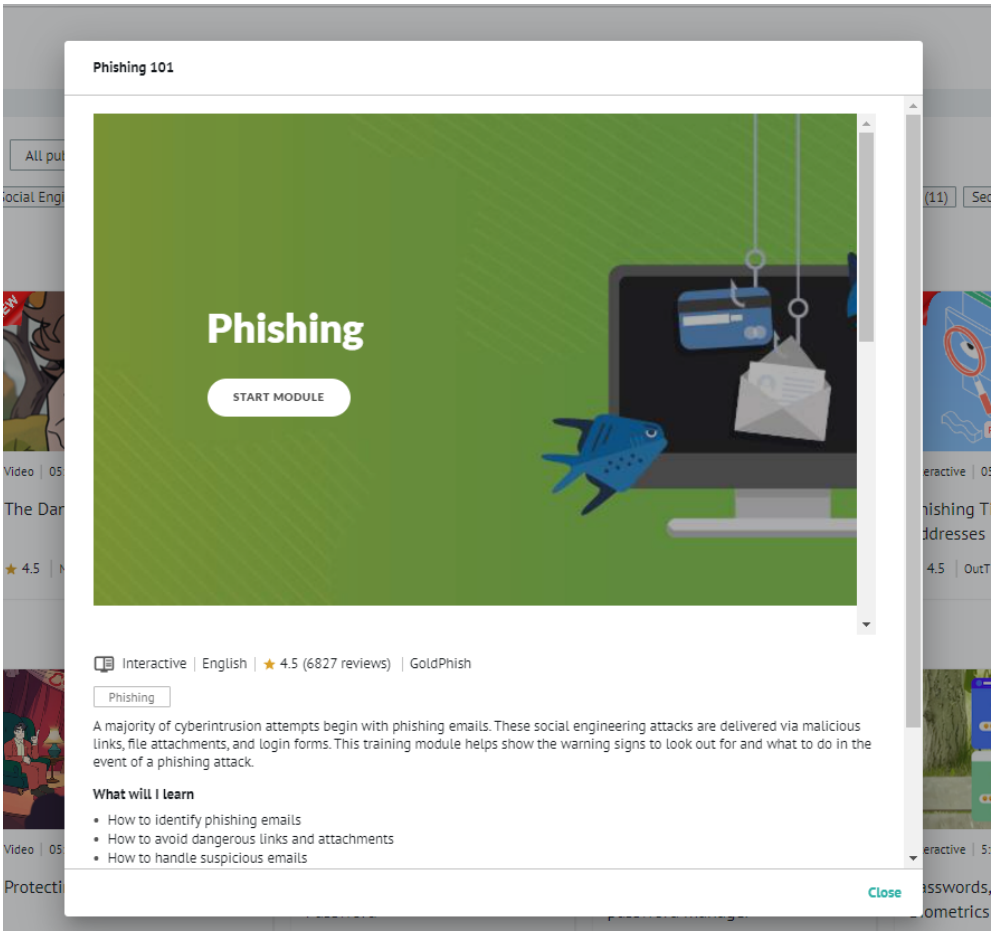


Figure 6.34: Esempio di modulo di allenamento sul phishing presente su PhishInsight.

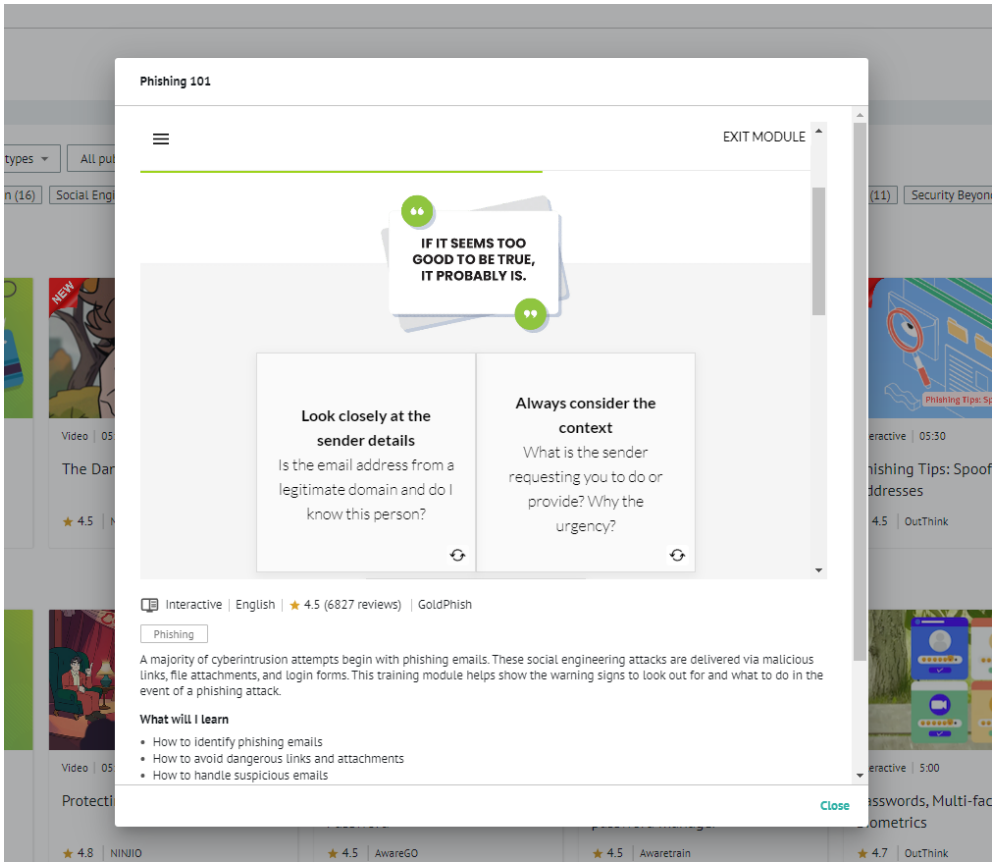


Figure 6.35: Esempio di modulo di allenamento sul phishing presente su PhishInsight. Attraverso la gamification è possibile spronare i dipendenti all'apprendimento.

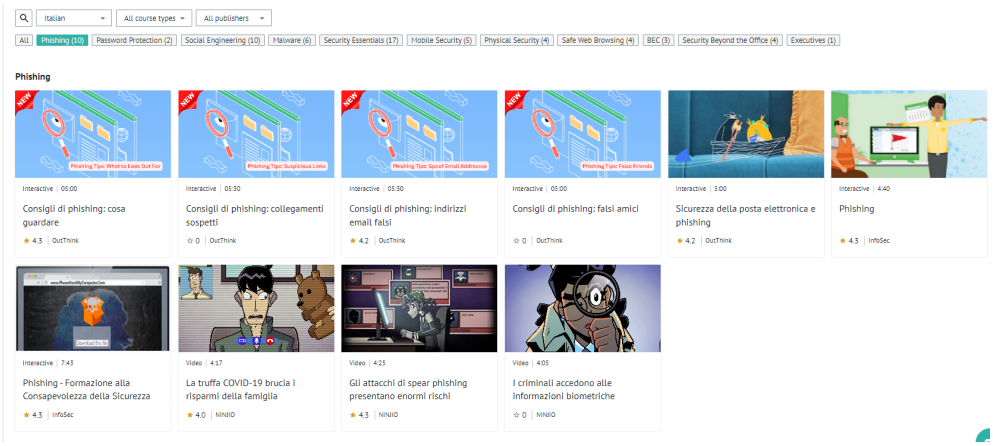


Figure 6.36: Moduli di allenamento di PhishInsight in italiano sul phishing.

6.1.4 Zphisher

Zphisher è un tool presente su ambienti Linux, open source e progettato per il phishing. Consente agli utenti di creare facilmente pagine web contraffatte di siti web popolari al fine di raccogliere informazioni sensibili, come nomi utente e password, da vittime ignare. Si tratta di uno strumento creato per scopi educativi e di consapevolezza, ma può essere abusato da individui malevoli per scopi dannosi. Data la sua semplicità di utilizzo, molto spesso viene preferito rispetto a SET(Social Engineering Toolkit).
Alcune delle caratteristiche di Zphisher includono:

- **Template di molteplici siti web:** Zphisher supporta un'ampia gamma di siti web popolari, consentendo agli utenti di creare facilmente pagine fake per eseguire attacchi di phishing.
- **Facilità d'uso:** Lo strumento è progettato per essere user-friendly, il che significa che anche utenti con conoscenze tecniche limitate possono utilizzarlo per creare pagine di phishing.
- **Personalizzazione delle pagine di phishing:** Gli utenti possono personalizzare le pagine di phishing in base alle loro esigenze, rendendole più convincenti per le vittime.
- **Supporto per tunneling:** Zphisher offre funzionalità di tunneling per rendere più difficile il rilevamento delle pagine di phishing da parte delle soluzioni di sicurezza.
- **Monitoraggio delle vittime:** Gli utenti possono monitorare le vittime che interagiscono con le pagine di phishing, consentendo loro di raccogliere le informazioni raccolte.

Nelle seguenti righe viene spiegato dettagliatamente come funziona Zphisher:

- **Installazione:** L'installazione è molto intuitiva e può essere effettuata seguendo le istruzioni presenti sul github del progetto [2]. Nella Figura 6.37 viene mostrata l'installazione effettuata clonando il repository github.
- **Avvio del tool:** Per avviare il tool è sufficiente posizionarsi nella cartella dove è stato installato, digitando, in questo caso, "cd zphisher" e, successivamente, con il comando "bash zphisher.sh" viene eseguito Zphisher. Nella finestra di avvio, di cui è fornito uno screen nella Figura 6.38 , viene elencata la lista dei siti fake disponibili all'uso.

[2] https://github.com/htr-tech/zphisher

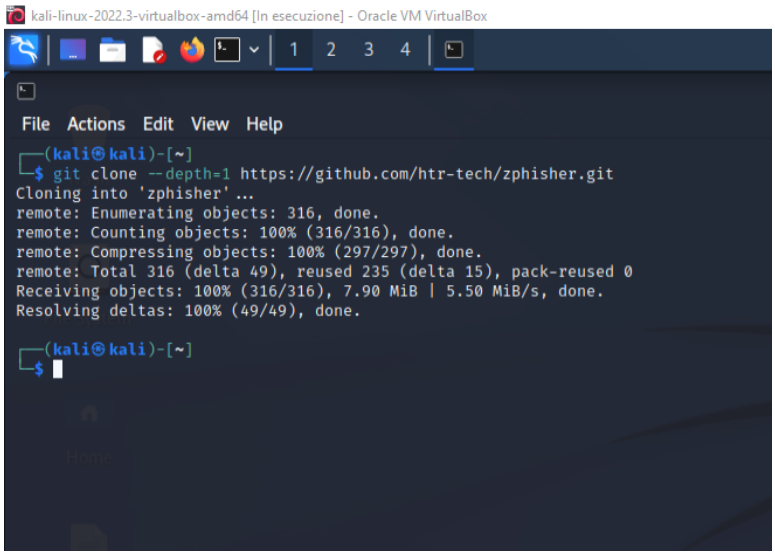


Figure 6.37: Installazione di Zphisher su una macchina virtuale con sistema operativo Kali Linux.

Figure 6.38: Schermata di avvio di Zphisher.

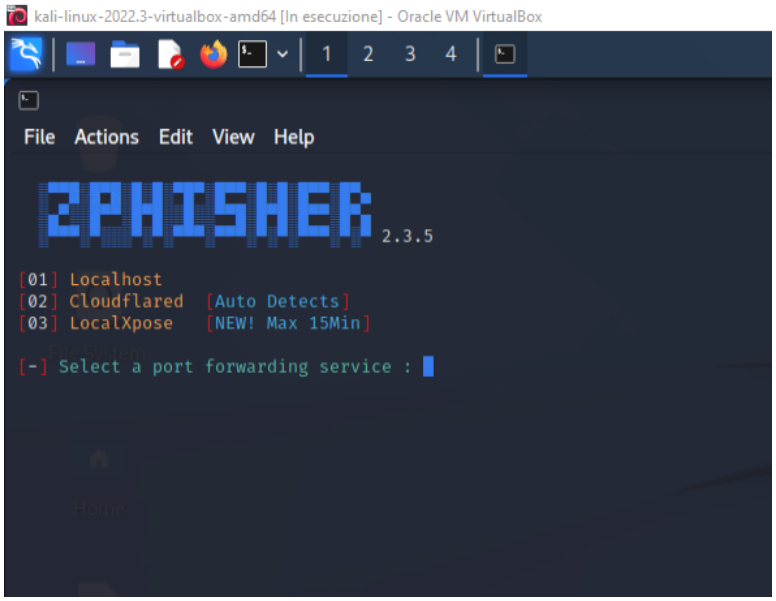


Figure 6.39: Zphisher in esecuzione. In questa Figura viene chiesto all'utente come esso desideri far apparire la pagina fake scelta in precedenza, in locale o su rete internet globale.

- **Esecuzione:** Nella Figura 6.38 è mostrato il tool in azione. In questo esempio viene selezionata l'opzione 06 facente riferimento a una pagina Paypal fake. Successivamente, come è possibile vedere nella Figura 6.39 il tool pone l'utente di fronte alla scelta su come rendere disponibile la pagina fake. La prima scelta consiste nel renderla disponibile all'interno della rete locale. Le altre due opzioni invece, Cloudflared e LocalXpose, permettono di rendere visibile su rete internet globale ciò che è in esecuzione sul localhost, sfruttando il concetto di "tunneling", in maniera analoga a quanto avviene con Pyphisher, tool descritto nella Sottosezione 6.1.2. Tale concetto viene approfondito nella Sezione 6.2 In questo caso viene selezionato Cloudflared, preferito a LocalXpose in quanto quest ultimo ha un limite di 15 minuti entro il quale è possibile visualizzare la pagina web. Successivamente il tool inizializza un server PHP sul localhost:8080 e lo rende visibile su rete internet globale utlizzando il servizio di tunneling offerto da Cloudflared, come in Figura 6.40, per poi fornire il link alla pagina di phishing. Prima di fornire l'url, come mostrato in Figura 6.41, il tool chiede all'utente se vuole modificarlo in modo da renderlo più "appetibile" a una potenziale vittima, decisione presa anche in questo caso. Dopo aver clickato sul link l'utente può accedere alla pagina fake di Paypal, dove, la vittima ignara, inserirà i dati, i quali verranno salvati in un file di testo. Nella Figura viene fornito uno screen della landing page.

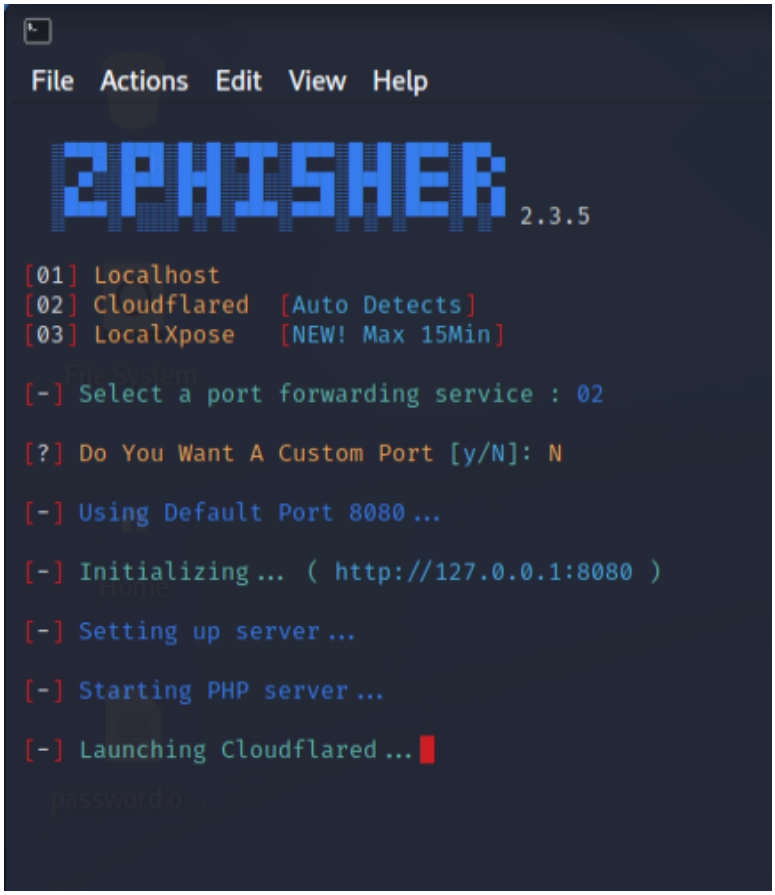


Figure 6.40: Esempio del servizio di tunneling offerto da Zphisher. Il tool inizializza un server PHP sul localhost:8080 e lo rende visibile su rete internet globale.

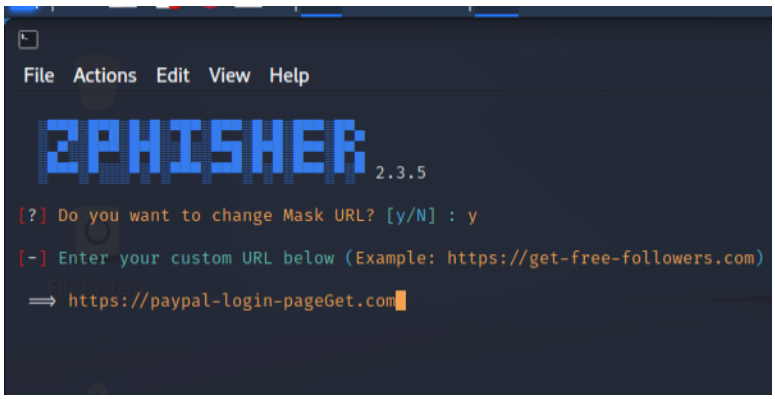


Figure 6.41: Esempio di "customizzazione" dell'url con Zphisher.

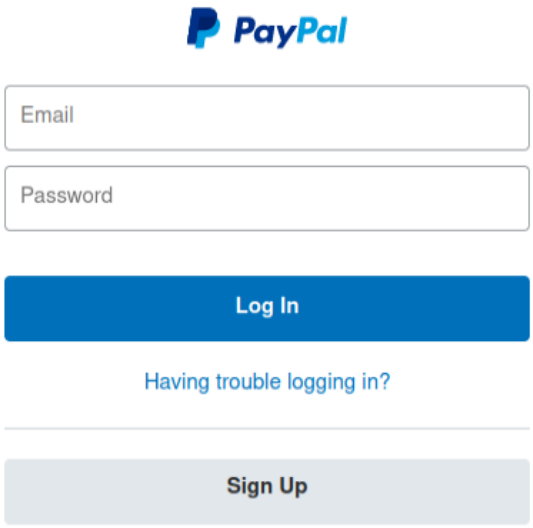


Figure 6.42: Template di una pagina di login fake di Paypal fornita da Zphisher.

6.2 Tunneling

In questa sezione viene approfondito il concetto di "Tunneling". Nell'ambito delle reti di computer, un protocollo di tunneling è un protocollo di comunicazione che permette ad un utente di fornire o accedere ad un servizio non supportato o non fornito direttamente dalla rete[67]. Le informazioni scambiate attraverso la rete Internet o tra due dispositivi digitali richiedono l'impiego di protocolli. Questi protocolli suddividono il messaggio in diverse sezioni, solitamente due: una contenente i dati effettivi da trasmettere e l'altra contenente le direttive relative alle modalità di trasmissione. Affinché si possa stabilire una connessione, entrambe le parti coinvolte devono comprendere e utilizzare lo stesso protocollo di comunicazione. Un protocollo di tunneling aggiunge al suo pacchetto di dati un altro insieme completo di informazioni, facendo uso di un protocollo di comunicazione diverso. In pratica, crea un tunnel tra due punti di una rete, consentendo loro di condividere dati di qualsiasi tipo in modo sicuro [30]. Un esempio di tunnelling è visibile nella Figura 6.43. Nell'esempio in questione è presente un Ethernet connesso a un altro Ethernet attraverso una WAN (Wide Area Network o rete geografica). Il task viene inviato su un pacchetto IP dall'host A di Ethernet-1 all'host B di Ethernet-2 tramite una WAN [17]. I passi che avvengono sono:

- L'host A costruisce un pacchetto che contiene l'indirizzo IP dell'host B.
- Quindi inserisce questo pacchetto IP in un frame Ethernet e questo frame viene indirizzato al router multiprotocollo M1.
- L'host A inserisce quindi questo frame sull' Ethernet.

- Quando M1 riceve questo frame, rimuove il pacchetto IP, lo inserisce nel pacchetto payload(carico utile [64]) del pacchetto del livello di rete WAN e indirizza il pacchetto WAN a M2. Il router multiprotocollo M2 rimuove il pacchetto IP e lo invia all'host B in un frame Ethernet.

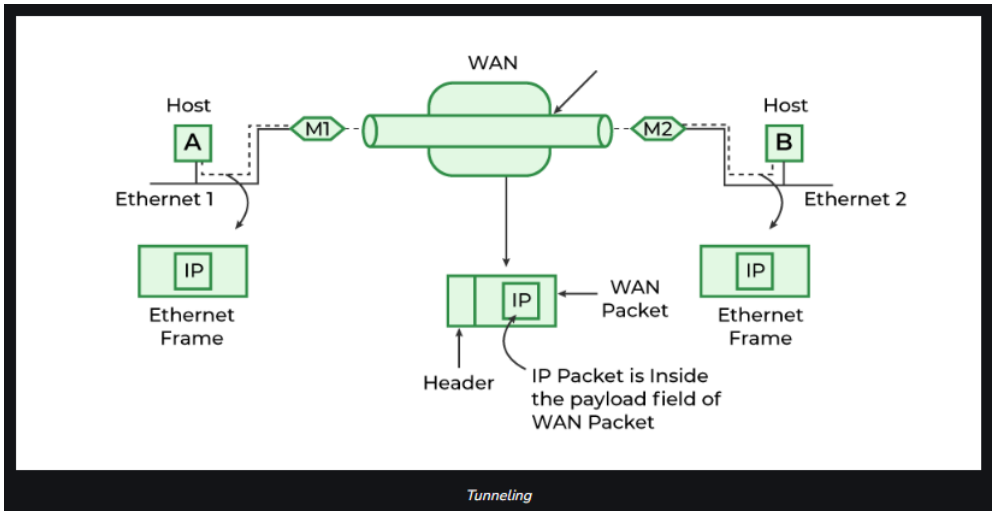


Figure 6.43: Esempio di funzionamento del tunneling [17].

Il "tunneling", dunque, è una tecnica utilizzata nella comunicazione e nella sicurezza informatica che consente di instradare il traffico di rete attraverso una connessione sicura o attraverso un canale diverso da quello originale. Questa tecnica può essere utilizzata per vari scopi, inclusi quelli legati alla sicurezza, all'anonimato e all'accesso a risorse in rete in situazioni particolari.
Alcune caratteristiche del tunneling sono[17]:

- **Utilizzo:** Il tunneling viene utilizzato principalmente per inviare dati attraverso una rete non sicura o non attendibile, in modo sicuro. Può anche essere utilizzato per aggirare restrizioni geografiche o censura online.

- **Tunneling Sicuro:** In molti casi, il tunneling viene utilizzato per creare una connessione sicura tra due punti, consentendo di cifrare i dati in transito. Ad esempio, il protocollo VPN (Virtual Private Network) utilizza il tunneling per creare connessioni sicure su Internet.

- **Protocolli di Tunneling:** Esistono vari protocolli di tunneling utilizzati per scopi diversi. Alcuni dei protocolli di tunneling più noti includono Secure Shell (SSH), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), e Internet Protocol Security (IPsec).

- **Scopo Malevolo:** Poiché i protocolli di tunneling incorporano un intero pacchetto all'interno del loro datagramma, potrebbero essere sfruttati in modo improprio. Spesso, il tunneling viene impiegato per eludere firewall poco sofisticati o configurati in modo non adeguato, incorporando protocolli bloccati all'interno

di protocolli consentiti dal firewall. Inoltre, l'uso dei protocolli di tunneling complica la realizzazione di attività come l'ispezione approfondita dei pacchetti, in cui l'infrastruttura di rete esamina il datagramma alla ricerca di contenuti sospetti, o il filtraggio dei dati in entrata/uscita, che verifica l'integrità degli indirizzi di destinazione dei dati per prevenire potenziali minacce. Vi sono anche casi di malware trasmessi tramite la tecnologia IPv6, che utilizza il tunneling per comunicare con dispositivi non compatibili. I criminali informatici possono utilizzare il tunneling per nascondere la loro posizione o per eludere la rilevazione durante attività illegali, come negli attacchi di phishing [30].

In sintesi, il tunneling è una tecnica importante nell'ambito delle comunicazioni e della sicurezza informatica, poiché consente di instradare il traffico di rete in modo sicuro attraverso canali sicuri o connessioni cifrate. È ampiamente utilizzato in applicazioni come VPN, accesso remoto sicuro e per bypassare restrizioni di rete.

Cloudflare, Ngrok e localXpose, visti all'opera nelle Sottosezioni 6.1.2 e 6.1.4, in tool come Pyphisher e Zphisher, sono tre strumenti che sfruttano questa tecnica. Nelle successive sottosezioni verranno indagati i servizi di tunneling offerti da questi 3 programmi ma in maniera breve, non essendo l'obiettivo principale di questa tesi.

6.2.1 Cloudflare

I Tunnel Cloudflare [3] sono principalmente utilizzati per migliorare la sicurezza e l'efficienza delle comunicazioni su Internet, proteggendo e accelerando il traffico tra i sistemi degli utenti e la rete Cloudflare[42].

Per utilizzare i Tunnel Cloudflare, è necessario installare un client sul server o sul dispositivo che si desidera connettere alla rete Cloudflare. Questo client stabilisce una connessione sicura con i server di Cloudflare attraverso un tunnel crittografato, consentendo l'invio e la ricezione sicura dei dati.

Il traffico viene instradato attraverso i PoP (Point-of-Presence) di Cloudflare in tutto il mondo, posizionati fisicamente vicino ai server degli utenti. Questo permette di massimizzare le prestazioni e ridurre la latenza.

Tuttavia, secondo un rapporto di GuidePoint Security [16], si è osservato un crescente abuso dei tunnel Cloudflare da parte di aggressori informatici. Questi utilizzano i tunnel per ottenere un accesso furtivo e persistente alle reti delle vittime, eludendo la rilevazione da parte delle soluzioni di sicurezza. Una volta ottenuto l'accesso, gli aggressori possono quindi rubare dati personali e informazioni riservate dai dispositivi compromessi. Tutto ciò avviene con l'esecuzione di un singolo comando sul sistema della vittima, che espone solo il token univoco del tunnel Cloudflare stabilito dall'aggressore. Inoltre, l'aggressore ha la possibilità di modificare la configurazione del tunnel in qualsiasi momento, inclusa la sua disabilitazione e riabilitazione, per adattarsi alle proprie necessità.

6.2.2 Ngrok

Ngrok è uno strumento molto utile che consente di creare in modo rapido e sicuro tunnel verso un server o un servizio locale, rendendoli accessibili su Internet. Questo strumento è particolarmente utile durante lo sviluppo di applicazioni web, il testing

[3] https://www.cloudflare.com/it-it/products/tunnel/

di webhook, la condivisione di progetti in fase di sviluppo o l'accesso remoto a risorse locali. Alcune delle caratteristiche principali di Ngrok [4] sono:

- **Tunneling sicuro:** Ngrok utilizza connessioni crittografate per garantire che i dati trasmessi attraverso il tunnel siano protetti da occhi indiscreti. Questo è particolarmente importante quando si desidera rendere accessibili servizi o risorse interni su Internet senza esporli direttamente.
- **Facilità d'uso:** Ngrok è facile da installare e configurare. Una volta installato, è sufficiente eseguire un comando per creare un tunnel verso una porta o un servizio locale.
- **Port forwarding:** consente di esporre i propri servizi locali su Internet in modo sicuro senza la necessità di configurare il port forwarding sul proprio router.
- **Supporto per protocolli diversi:** Ngrok supporta una varietà di protocolli, tra cui HTTP, HTTPS, TCP e UDP, il che lo rende adatto per una vasta gamma di applicazioni.
- **Sottodomini personalizzati:** è possibile personalizzare l'URL del proprio tunnel con un sottodominio di scelta personale, rendendo più facile condividere il proprio servizio con gli altri.
- **Monitoraggio e registrazione:** Ngrok offre funzionalità di monitoraggio e registrazione del traffico attraverso il tunnel, consentendo di tenere traccia dell'utilizzo e degli errori.
- **Versione gratuita e a pagamento:** Ngrok offre una versione gratuita con alcune limitazioni, ma è disponibile anche un piano a pagamento con funzionalità avanzate e supporto.

Nella Figura 6.44 è possibile vedere il processo di funzionamento tipico di ngrok. Il tutto è esplicato nei seguenti passi [41] :

- **Esecuzione dell'applicazione locale:** Inizialmente, l'utente deve avviare l'applicazione sul proprio computer in modo che questa sia accessibile tramite il localhost (ad esempio: http://localhost:8080).
- **Avvio di un tunnel con Ngrok:** Utilizzando l'eseguibile Ngrok, disponibile su diverse piattaforme, viene creato un "tunnel" tra l'applicazione locale e Ngrok. Questo crea un collegamento sicuro tra l'applicazione e Internet.
- **Fornitura di un URL pubblico da parte di Ngrok:** Dopo aver configurato il tunnel, Ngrok fornisce un URL unico e pubblicamente accessibile che punta all'applicazione locale. Questo URL può essere utilizzato dagli utenti finali per accedere all'applicazione da qualsiasi parte del mondo.
- **Condivisione dell'URL pubblico:** Ora è possibile condividere l'URL pubblico con gli utenti finali o con qualsiasi altra persona desiderata. Questo URL verrà utilizzato dagli utenti per accedere all'applicazione.
- **Accesso degli utenti all'URL Web:** Gli utenti finali apriranno un browser web e inseriranno l'URL pubblico nella barra degli indirizzi.

[4] https://ngrok.com/

- **Invio della richiesta al server Ngrok:** Quando un utente fa clic sull'URL, la richiesta viene indirizzata al server di Ngrok. Poiché l'URL è basato su un sottodominio di ngrok.com, la richiesta viene inizialmente inviata a Ngrok.
- **Inoltro della richiesta da parte di Ngrok:** Ngrok identifica l'applicazione di destinazione in base all'URL e inoltra la richiesta verso il tunnel precedentemente creato.
- **Connessione all'applicazione locale:** Infine, la richiesta inoltrata si connette all'applicazione ospitata localmente sul computer dell'utente. In questo modo, gli utenti finali possono interagire con l'applicazione come se fosse online, anche se in realtà è ospitata su un computer locale.

In breve, Ngrok funge da intermediario che consente agli utenti di accedere all'applicazione locale su Internet in modo sicuro e semplice.

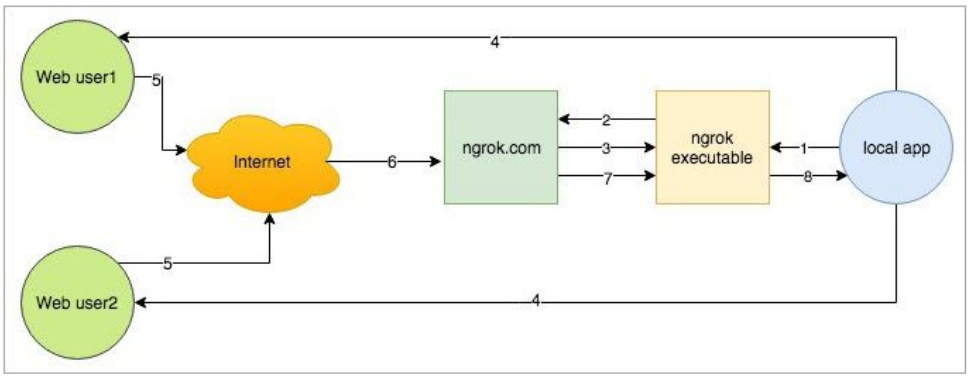


Figure 6.44: Esempio di funzionamento di ngrok [41].

6.2.3 LocalXpose

LocalXpose è un reverse proxy [5] che offre funzionalità simili a Ngrok e Cloudflared, consentendo agli sviluppatori di esporre le loro app o i loro servizi ospitati in locale su Internet in modo sicuro. Un esempio del funzionamento di questo software è disponibile nella Figura 6.45. Alcune delle caratteristiche di LocalXpose [6] sono[36]:

- **Esposizione di servizi locali:** LocalXpose permette agli sviluppatori di esporre servizi o applicazioni ospitati sul proprio computer in locale. Questi servizi potrebbero essere siti web in fase di sviluppo, API o altre applicazioni a cui è necessario accedere da Internet.
- **Sicurezza:** LocalXpose offre una connessione crittografata per proteggere i dati trasmessi tra il servizio locale e Internet. Ciò garantisce che le informazioni siano al sicuro durante la trasmissione.
- **Configurazione semplice:** Gli sviluppatori possono configurare facilmente LocalXpose per esporre i propri servizi locali. È possibile specificare la porta locale su cui il servizio è in ascolto e LocalXpose genererà un URL pubblico unico.

[5] https://www.ionos.it/digitalguide/server/know-how/che-cose-un-reverse-proxy/
[6] https://localxpose.io/blog

- **Tunneling sicuro:** LocalXpose utilizza un tunneling sicuro per instradare il traffico da Internet al servizio locale. Ciò consente agli utenti finali di accedere al servizio come se fosse ospitato su un server remoto.
- **Monitoraggio e registrazione:** LocalXpose offre strumenti per monitorare il traffico e tenere traccia delle richieste in arrivo al servizio locale. Questo può essere utile per scopi di debug e analisi.
- **Versioni gratuite e a pagamento:** LocalXpose offre sia una versione gratuita con funzionalità limitate che piani a pagamento con funzionalità avanzate e maggiore flessibilità.

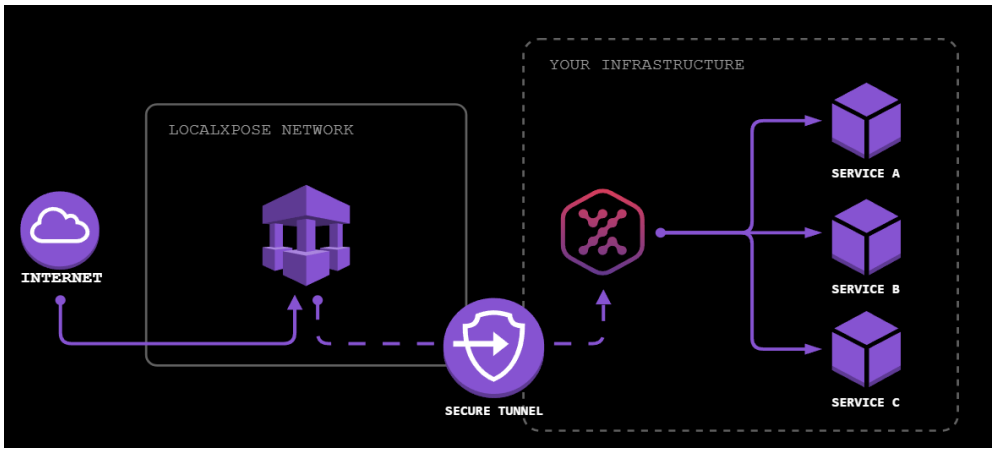


Figure 6.45: Esempio di funzionamento di LocalXpose[36].

In generale, LocalXpose è una soluzione utile per gli sviluppatori che desiderano testare o condividere le loro applicazioni locali con gli altri su Internet in modo rapido e sicuro.

7. Esperimento di Phishing

In questo capitolo il focus sarà sulle simulazioni di phishing, in particolare verranno analizzate le varie fasi che compongono una simulazione di phishing e verranno effettuati degli esperimenti.

7.1 Fasi di un esperimento di Phishing

In questa sezione verranno elencati e spiegati i vari passi che compongono un esperimento di phishing [26], quali :

- **Pianificazione:** Prima di iniziare la campagna, gli esperti di sicurezza collaborano con l'organizzazione per pianificare l'intero processo. Questo include la definizione degli obiettivi, la determinazione del campo di test, la selezione dei bersagli e l'ottenimento delle autorizzazioni necessarie. Tutto ciò può essere fatto anche attraverso la stesura di un questionario in cui vengono poste domande come:
  - Quale livello di informazioni sui dipendenti verrà fornito al team della campagna? Informazioni personali come nome, cognome, banca abituale, ecc.?
  - Quali siti Web o applicazioni comuni utilizzano quotidianamente gli utenti interni?
  - Quali sono i tipi di file più comuni con cui lavorano gli utenti? (PDFS, Word, Excel, ecc.).
  - Si tratta di una campagna di Phishing mirata (es. Spear Phishing) o di una campagna di Phishing generica?
  - I dipendenti sono autorizzati a utilizzare siti di social media come Facebook, Twitter, ecc. utilizzando le loro postazioni di lavoro e le e-mail di lavoro?
  - Con quali organizzazioni collabora l'azienda? (Fornitori, supporto IT, partner commerciali, enti di beneficenza).
  - Qual è il principale prodotto o servizio interno dell'azienda a cui i dipendenti danno maggiore priorità?
  - Esiste un gruppo di dipendenti che cade abitualmente vittima delle e-mail di phishing?
  - Esistono siti Web inseriti nella lista nera come giochi d'azzardo, porno, ecc. che si sospetta che i dipendenti visitino?

  Dopo aver ricevuto le risposte alle domande fornite può essere utile fare un ulteriore incontro in cui queste vengono discusse, così da, eventualmente, far emergere nuove informazioni che potrebbero non essere state incluse nel questionario.

- **Selezione dei Bersagli:** Gli esperti di sicurezza identificano i bersagli all'interno dell'organizzazione che saranno soggetti agli attacchi di phishing simulati. Questi bersagli possono includere dipendenti di diversi livelli gerarchici e reparti.
- **Creazione dei Messaggi di Phishing:** Gli esperti di sicurezza creano messaggi di phishing realistici che possono includere e-mail, messaggi di testo o messaggi su piattaforme di social media. Questi messaggi sono progettati per ingannare i destinatari e spingerli a intraprendere azioni non sicure, come fare clic su un link o fornire informazioni riservate. Ci sono poche opportunità di apprendimento per i dipendenti se la campagna è troppo facile o troppo difficile. L'obiettivo finale non è vedere quante persone si possono ingannare, ma quante si possono aiutare nell' educazione o rafforzamento della loro conoscenza delle minacce di ingegneria sociale.
- **Simulazione di Phishing:** Gli esperti di sicurezza lanciano le simulazioni di phishing contro i bersagli selezionati. Queste simulazioni possono variare in complessità e realismo, a seconda degli obiettivi della campagna.
- **Monitoraggio delle Risposte:** Durante la campagna, vengono monitorate le risposte dei bersagli. Questo include il monitoraggio di chi ha aperto i messaggi di phishing, chi ha cliccato sui link, chi ha fornito informazioni riservate e così via.
- **Formazione:** Dopo ogni simulazione di phishing, gli utenti che hanno interagito con i messaggi di phishing ricevono formazione sulla sicurezza. Questa formazione mira a educare gli utenti su come riconoscere e rispondere agli attacchi di phishing.
- **Rapporti e Analisi:** Alla fine della campagna, gli esperti di sicurezza compilano rapporti dettagliati sull'efficacia delle misure di sicurezza dell'organizzazione contro il phishing. Questi rapporti possono includere statistiche sulle risposte dei bersagli, analisi dei punti deboli e raccomandazioni per il miglioramento della sicurezza.
- **Feedback e Miglioramenti:** L'organizzazione utilizza i risultati e le raccomandazioni della campagna per apportare miglioramenti alle proprie misure di sicurezza, inclusa la formazione degli utenti e la protezione contro il phishing.
- **Ripetizione:** Le campagne di phishing e penetration testing possono essere condotte periodicamente per garantire che le misure di sicurezza siano sempre aggiornate ed efficaci.

È importante sottolineare che una campagna di phishing come penetration testing dovrebbe essere condotta in modo etico e in conformità con tutte le leggi e le regolamentazioni applicabili. L'obiettivo principale è identificare i punti deboli e migliorare la sicurezza dell'organizzazione, non danneggiare l'organizzazione o i suoi dipendenti.

7.2 Esempio di un esperimento di phishing

In questa sezione viene fornito un esempio di campagna di phishing effettuata seguendo alcuni dei passi citati nella Sezione 7.1. Non verranno seguiti tutti i passi in quanto la campagna di questa tesi non viene fatta in un contesto aziendale, bensì informale, con le dovute autorizzazioni e con la criptazione delle password catturate. Il tool scelto, per

la sua accessibilità e immediatezza, è Gophish, già ampiamente trattato nella Sezione 6.1.1 del Capitolo 6. L'esperimento è articolato nei seguenti passi.

Selezione bersagli e pianificazione. I "bersagli" sono un gruppo di 15 persone, prese tra colleghi studenti, familiari e conoscenti, di età differenti. Mentre in un contesto aziendale sarebbe preferibile somministrare un test ai dipendenti in modo da ottenere informazioni specifiche, in tale contesto le informazioni sono state reperite da una conoscenza personale con i "bersagli" che dura da diversi anni.

Scelta dell'email di phishing e della Landing Page. Il passo successivo consiste nella creazione dell'email di phishing e dell'eventuale pagina dove il bersaglio verrà indirizzato dopo aver clickato uno dei link presenti. Uno dei motivi per cui in questo esperimento è stato scelto Gophish è dovuto alla sua immediatezza, in pochi minuti è infatti possibile importare un'email, modificarla e fare lo stesso per le landing pages. In tale campagna è stato deciso di utilizzare un' email template in cui si avverte l'utente di un tentativo di accesso avvenuto al proprio account facebook con la conseguente richiesta di inserire nuovamente le proprie credenziali. L'email in questione è stata ottenuta importando un'email originale che Facebook invia in questi casi. L'email originale è stata poi modificata attraverso l'aggiunta di alcune delle variabili presenti in Figura 6.7. Un esempio dell'email realizzata è fornito nella Figura 7.1. La landing page è stata realizzata importando la login page di Facebook [1]. Nella Figura 7.2 viene mostrata la landing page creata.

Figure 7.1: Esempio di email realizzata per la campagna di phishing.

[1] https://www.facebook.com/

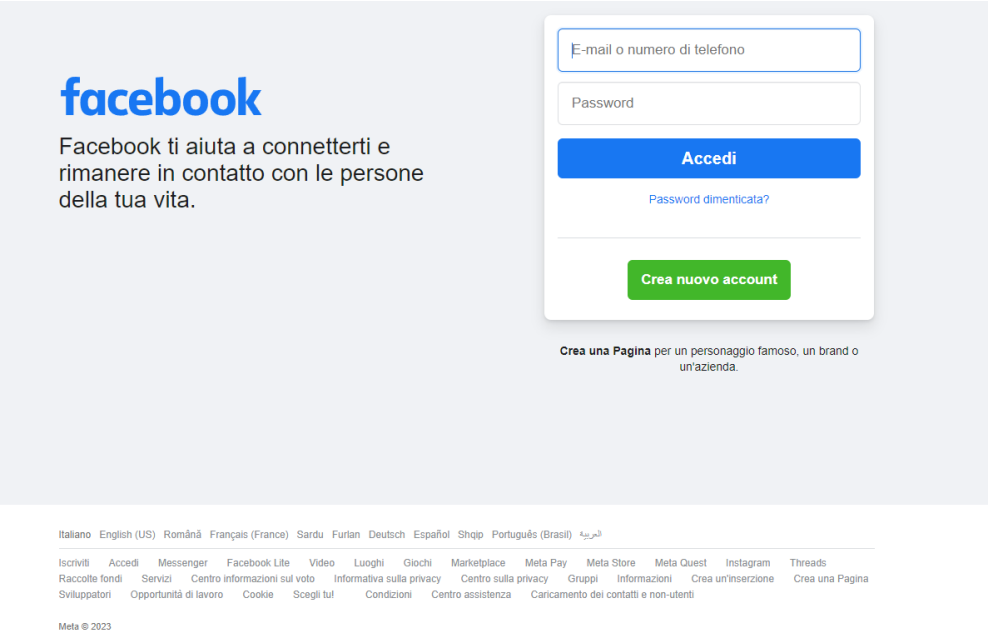


Figure 7.2: Esempio di landing page realizzata per la campagna di phishing.

Lancio e monitoraggio della simulazione. Dopo aver realizzato l'email e la landing page, viene effettivamente lanciata la campagna di phishing. Attraverso la dashboard intuitiva di Gophish diventa facile monitorare il numero di email inviate e aperte, il numero di click effetuati sui link presenti nelle varie email e quanti utenti hanno inserito delle credenziali. La dashboard con i risultati della campagna è mostrata nella Figura 7.3

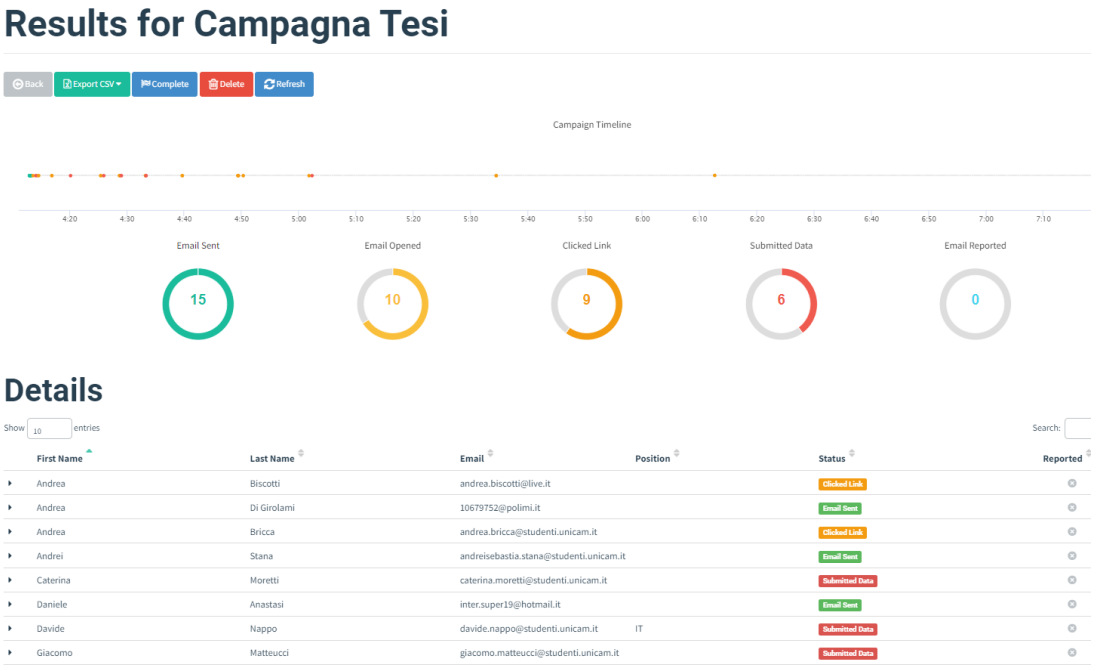


Figure 7.3: Esempio della dashboard intuitiva di Gophish in cui sono contenute le varie informazioni riguardanti la Campagna effettuata.

Conclusioni. Essendo la campagna effettuata in un contesto non lavorativo, e, per ragioni di tempo e complessità, sono state saltate alcune fasi come la realizzazione di rapporti sulle misure di sicurezza o la ripetizione dell'esperimento più volte. L'obiettivo della campagna era quello di utilizzare uno dei tool presentati nel Capitolo 6 in modo etico e con lo scopo di sensibilizzare sull'argomento. Studiando i dati della campagna in questione è stato possibile constatare la preparazione già presente nei bersagli scelti, alcuni dei quali, intuendo che si trattasse di una pagina di phishing, hanno inserito credenziali fittizie. Va però considerato il fatto che queste tipologie di phishing generico puntano sulla quantità, vengono inviate milioni di email, molte delle quali indirizzate a persone molto anziane e poco avvezze all'uso di strumenti tecnologici. Nonostante i risultati positivi, dunque, è importante non sottovalutare l'argomento e notare come anche il semplice clickare sul link presente nelle email, pur non inserendo le credenziali, può essere considerato un rischio, in quanto potenzialmente permette all'attaccante di accedere ad alcune informazioni personali, come l'indirizzo IP, o, nel caso di Gophish, sistema operativo e versione del browser utilizzata dalla vittima.

8. Conclusioni e Sviluppi Futuri

In conclusione, la minaccia del phishing rimane una delle sfide più significative per individui e organizzazioni in tutto il mondo. Nel corso degli anni, gli attacchi di phishing sono diventati più sofisticati e diffusi, mettendo a repentaglio la sicurezza dei dati personali e aziendali. La presente tesi ha esaminato nel dettaglio il fenomeno del phishing, la storia e le origini, le tipologie, le contromisure da attuare e si è posta l' obiettivo di sensibilizzare sull'argomento mettendo in luce la facilità con cui gli aggressori possono perpetrare tali attacchi e le modalità con cui questi avvengono. Questa tipologia di attacco è in continua evoluzione, in particolare negli ultimi anni e nel futuro, l'integrazione dell'intelligenza artificiale e del machine learning [35] negli attacchi di phishing ha rappresentato e rappresenterà una nuova sfida per la sicurezza informatica. Guardando al futuro, la lotta contro gli attacchi di phishing richiederà un impegno continuo nella ricerca e nello sviluppo di nuovi strumenti e tecniche di sicurezza. Alcuni possibili sviluppi futuri potrebbero essere, ad esempio : lo sviluppo di tecniche di difesa avanzate, una formazione e un monitoraggio continuo, lo sviluppo di leggi e normative più severe per i trasgressori e una collaborazione maggiore tra gli addetti al settore. In definitiva, il phishing rimarrà una minaccia persistente, ma, con la giusta combinazione di tecnologie avanzate, formazione e collaborazione, sarà possibile ridurre in modo significativo la sua efficacia e proteggere meglio le nostre informazioni personali e aziendali. La sicurezza informatica è una sfida in continua evoluzione, e la nostra capacità di adattarci a nuove minacce determinerà il nostro successo nella protezione dei nostri dati e sistemi informatici.

Bibliography

[1] *5 Smishing Attack Examples Everyone Should See*. URL: https://www.secureworld.io/industry-news/5-smishing-attack-examples-everyone-should-see.

[2] AntiPhishingWorkingGroup. *Phishing Activity Trends Report*. URL: https://docs.apwg.org/reports/apwg_report_Q1_2010.pdf?_ga=2.183811502.985136970.1691399834-351066385.1688919862&_gl=1*gjuh1k*_ga*MzUxMDY2Mzg1LjE2ODg5MTk4NjI.*_ga_55RF0RHXSR*MTY5MTM5OTgzMy4yLjEuMTY5MTQwMDQyMC4wLjAuMA..

[3] Andrei Antipov. *The best 9 phishing simulators for employee security awareness training (2023)*. URL: https://resources.infosecinstitute.com/topics/phishing/top-9-free-phishing-simulators/.

[4] Anti-Phishing Working Group (APWG). "Phishing Activity Trends Report 1st Quarter 2013". In: (2013).

[5] Andrea Boggio. *Cyberspazio: minacce e fattore umano*. URL: https://www.ictsecuritymagazine.com/articoli/cyberspazio-minacce-e-fattore-umano/.

[6] MARCO DAL BROI. "ChatGPT. La sicurezza informatica aziendale: tra prevenzione e mitigazione dei danni economici". In: ().

[7] Niccolò Caranti. *Cybersecurity: rischi e attori malevoli*. URL: https://www.balcanicaucaso.org/Progetti/ESVEI/Notizie-Esvei/Cybersecurity-rischi-e-attori-malevoli-206837.

[8] Clusit. "Rapporto Clusit 2022 sulla sicurezza ICT in Italia". In: (2022).

[9] *Cos'è un virus del settore di avvio?* Dec. 26, 2022. URL: https://www.kaspersky.it/resource-center/definitions/boot-sector-virus.

[10] Marco Cozzi. "Cyber Risk Protection". In: ().

[11] Dennis Kaburu David Njuguna John Kamau. "A Review of Smishing Attaks Mitigation Strategies". In: ().

[12] Trasporti Attività produttive Finanze e Affari comunitari Servizio Studi Dipartimento Difesa con la collaborazione dei seguenti Dipartimenti: Istituzioni Giustizia. *Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa cyber*. URL: http://documenti.camera.it/leg18/dossier/pdf/DI0162.pdf.

[13] Mandeep Yadav Dr. LatikaKharb. "What is Pharming?" In: *International Journal of Advance Engineering and ResearchDevelopment* (October 2017).

[14] Gabriele Faggioli. *Cyber security, Italia nel mirino: serve un fronte comune per difendersi meglio*. Mar. 14, 2023. URL: https://www.cybersecurity360.it/outlook/cyber-security-italia-nel-mirino-serve-un-fronte-comune-per-difendersi-meglio/.

[15] *Famous Phishing Incidents from History*. URL: https://hempsteadny.gov/635/Famous-Phishing-Incidents-from-History.

[16] Nic Finn. *Tunnel Vision: CloudflareD AbuseD in the WilD*. URL: https://www.guidepointsecurity.com/blog/tunnel-vision-cloudflared-abused-in-the-wild/.

[17] GeeksforGeeks. *Tunneling*. URL: https://www.geeksforgeeks.org/tunneling/.

[18] Assicurazioni Generali. *Come proteggersi dal Cyber Risk*. URL: https://www.generali.it/magazine/business/cyber-risk#:~:text=Cyber%20Risk%3A%20danni%20potenziali,-Scopriamo%20insieme%20alcuni&text=danni%20materiali%20ai%20sistemi%20elettronici,costi%20emergenti%20per%20servizi%20professionali..

[19] Luigi Gobbi. *Attacchi whaling: la "caccia informatica alle balene" che minaccia CEO, CFO e tutti i C-Level*. URL: https://www.cybersecurity360.it/nuove-minacce/attacchi-whaling-la-caccia-informatica-alle-balene-che-minaccia-ceo-cfo-e-tutti-i-c-level/.

[20] IT Governance. *Cos'è la cyber security?* URL: https://www.itgovernance.eu/it-it/what-is-cyber-security-it#:~:text=La%20cyber%20security%20(anche%20detta,il%20rischio%20di%20attacchi%20informatici..

[21] Charles Griffiths. *The Latest 2023 Phishing Statistics (updated August 2023)*. URL: https://aag-it.com/the-latest-phishing-statistics/#:~:text=In%202021%2C%20the%20average%20click,12%25%20delivered%20malware.

[22] Christopher Hadnagy. *Human Hacking: Influenzare e manipolare il comportamento umano con l'ingegneria sociale*. Milano: Apogeo, 2019.

[23] Adam Hayes. *Phishing: What it is And How to Protect Yourself*. URL: https://www.investopedia.com/terms/p/phishing.asp.

[24] IBM. *Cos'è l'ingegneria sociale?* URL: https://www.ibm.com/it-it/topics/social-engineering.

[25] Luke Irwin. *The 5 Biggest Phishing Scams of All Time*. Oct. 20, 2022. URL: https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time.

[26] MBA Jason Firch. *How To Create An Email Phishing Campaign In 8 Steps*. URL: https://purplesec.us/phishing-campaign/.

[27] Lauren Lusty Julian Sexton John Sweetnam Anne Townsend Jennifer Cawthra Michael Ekstrom. *Data Integrity:Identifying and Protecting Assets Against Ransomware and Other Destructive Events*. URL: https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html.

[28] Felix Jerry and Hauck Chris. "System Security: A Hacker's Perspective". In: (1987).

[29] Sgt. Andrew Joyce. *Nova Scotians lose record* 3.6*Mtoscams*. Mar. 1, 2023. URL: https://www.rcmp-grc.gc.ca/en/news/2023/nova-scotians-lose-record-36m-scams.

[30] Kaspersky. *Cos'è un protocollo di tunneling?* URL: https://www.kaspersky.it/resource-center/definitions/tunneling-protocol.

[31] Saadia Zahidi Klaus Schwab. "The Global Risks Report 2021 16th Edition". In: *World Economic Forum Journal* (2021).

[32] Laura Klusaitė. *La storia della cybersecurity*. URL: https://nordvpn.com/it/blog/la-storia-della-cybersecurity/.

[33] Elmer Lastdrager. "Achieving a consensual definition of phishing based on a systematic review of the literature". In: (2014).

[34] Vito Lavecchia. *Caratteristiche e differenza tra Spear Phishing e Whaling in informatica*. URL: https://vitolavecchia.altervista.org/caratteristiche-e-differenza-tra-spear-phishing-e-whaling-in-informatica/.

[35] Anzen Technologies Private Limited. "Forecasting the Future of Phishing - Trends and Tactics for 2022-2023". In: ().

[36] LocalXpose. *Bye Bye Localhost Hello World*. URL: https://localxpose.io/#download.

[37] Salvatore Lombardo. *Pharming: cos'è, come funziona e i consigli per difendersi dalla truffa dei "siti-trappola"*. URL: https://www.cybersecurity360.it/nuove-minacce/pharming-cose-come-funziona-e-i-consigli-per-difendersi-dalla-truffa-dei-siti-trappola/.

[38] Andrey Kostin Maria Vergelis. *2018 Fraud World Cup*. May 28, 2018. URL: https://securelist.com/2018-fraud-world-cup/85878/.

[39] Trend Micro. *Che cos'è lo smishing?* URL: https://www.trendmicro.com/it_it/what-is/phishing/smishing.html.

[40] Presidenza del Consiglio dei Ministri. "Quadro strategico nazionale per la sicurezza dello spazio cibernetico". In: (2013).

[41] myservername.com. *Tutorial Ngrok: una breve introduzione all'installazione e alla configurazione*. URL: https://ita.myservername.com/ngrok-tutorial-brief-introduction-with-installation.

[42] Michele Nasi. *Tunnel Cloudflare usati per sottrarre dati dai sistemi delle vittime: ecco come*. URL: https://www.ilsoftware.it/tunnel-cloudflare-usati-per-sottrarre-dati-dai-sistemi-delle-vittime-ecco-come/.

[43] Università di Pavia. *I VIRUS INFORMATICI*. URL: http://biblioteche.unipv.it/wp-content/uploads/2013/11/Guida-ai-virus-informatici.pdf.

[44] Garante Per La Protezione Dei Dati Personali. *Ransomware*. URL: https://www.garanteprivacy.it/temi/cybersecurity/ransomware#:~:text=Ci%20sono%20due%20tipi%20principali%20di%20ransomware%3A&text=i%20cryptor%20(che%20criptano%20i%20file%20contenuti%20nel%20dispositivo%20rendendoli%20inaccessibili)%3B&text=i%20blocker%20(che%20bloccano%20l'accesso%20al%20dispositivo%20infettato)..

[45] *Phishing History - The Earliest Phishing Scams*. URL: https://www.brighthub.com/internet/security-privacy/articles/82116/?expand_article=1.

[46] Oxford Reference. *phishing*. URL: https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100323446.

[47] Institute of Risk Management. *Cyber Risk*. URL: https://www.theirm.org/what-we-say/thought-leadership/cyber-risk/.

[48] Ivan Robiati. "Decifrare il Phishing: Tecniche di Attacco e Strategie di Difesa". In: ().

[49] Walter Rocchi. *Il vishing e la truffa del "consenso rubato": cos'è e come difendersi dal phishing vocale*. URL: https://www.cybersecurity360.it/nuove-minacce/il-vishing-e-la-truffa-del-consenso-rubato-cose-e-come-difendersi-dal-phishing-vocale/.

[50] Shouhuai Xu1 Rosana Montañez Edward Golob. "Human Cognition Through the Lens of Social Engineering Cyberattacks". In: (Sept. 30, 2020).

[51] Ahona Rudra. *Why is Phishing so effective?* URL: https://powerdmarc.com/why-is-phishing-so-effective/#:~:text=Phishing%20is%20an%20effective%20and,victim%20to%20a%20phishing%20attack..

[52] Panda Security. *Scopriamo cos'è lo spear phishing e come utilizza il social engineering per colpire le vittime*. URL: https://www.pandasecurity.com/it/mediacenter/spear-phishing-come-difendersi/.

[53] Casey C. Rackley Slade E. Griffin. "Vishing". In: ().

[54] *The Dirty Dozen: The 12 Most Costly Phishing Attack Examples*. Apr. 29, 2021. URL: https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/.

[55] *The Worst Phishing Attacks in History*. Jan. 5, 2023. URL: https://www.graphus.ai/blog/worst-phishing-attacks-in-history/.

[56] Caleb Townsend. *What is a Honeypot?* URL: https://www.uscybersecurity.net/honeypot/.

[57] Dizionario Treccani. *phishing*. URL: https://www.treccani.it/enciclopedia/phishing.

[58] Dizionario Treccani. *phishing*. URL: https://www.treccani.it/vocabolario/phishing/.

[59] Abi Tyas Tunggal. *Why is Cybersecurity Important?* URL: https://www.upguard.com/blog/cybersecurity-important.

[60] Ilma Vienažindytė. *I principali tipi di attacchi informatici*. Dec. 26, 2022. URL: https://nordvpn.com/it/blog/tipi-di-attacchi-informatici/.

[61] *What is a whaling phishing attack?* URL: https://www.mimecast.com/content/whaling-phishing-attack/#:~:text=What%20is%20a%20whaling%20phishing,transfer%20to%20a%20fraudulent%20account.

[62] *What is Rock Phish?* URL: https://www.complianceandprivacy.com/News-Verisign-R-Ph-commentary.asp.

[63] *What is spear-phishing? Definition with examples*. URL: https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/.

[64] Wikipedia. *Carico utile (informatica)*. URL: https://it.wikipedia.org/wiki/Carico_utile_(informatica).

[65] Wikipedia. *Go (linguaggio di programmazione)*. URL: https://it.wikipedia.org/wiki/Go_(linguaggio_di_programmazione).

[66] Wikipedia. *Phreaking*. URL: https://it.wikipedia.org/wiki/Phreaking.

[67] Wikipedia. *Protocollo di tunneling*. URL: https://it.wikipedia.org/wiki/Protocollo_di_tunneling.

[68] Wikipedia. *Whaling*. URL: https://it.wikipedia.org/wiki/Whaling.

Ringraziamenti

Ringrazio chiunque mi sia stato vicino in questi anni di università, la mia famiglia e tutti gli amici che hanno rappresentato per me una seconda famiglia, Andrea, Samuel, Irene, Marco, Giacomo, i coinquilini avuti e tanti altri, non basterebbe una pagina per elencarvi tutti. Ringrazio mia sorella Ilaria e i miei genitori Mario e Silvana, che, attraverso i loro sforzi, mi hanno permesso di vivere questa esperienza formativa che custodirò per sempre nel mio cuore. Ringrazio Stefano e tutti i dipendenti dell'ATF, che, con la loro immensa disponibilità e professionalità, mi hanno aperto le porte della loro azienda durante i mesi del tirocinio, formandomi durante questo bellissimo periodo e rendendo possibile la conclusione di questo percorso. Infine un pensiero va ai miei relatori, Fausto Marcantoni e Fabrizio Fornari per il sostegno e la pazienza avuta nei miei confronti. A tutti voi dico grazie e dedico questa piccola grande tappa del mio viaggio.