UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

PHISHING:

Analisi del fenomeno, contromisure esistenti e casi di studio più famosi

Caterina Bianchini

0320488

Anno accademico 2022/2023

INDICE

PREMESSA

Il progresso tecnologico avvenuto negli ultimi decenni ha portato grandissimi vantaggi nella nostra vita quotidiana, dandoci la possibilità di comunicare velocemente, acquistare a distanza o fare operazioni finanziarie online. Tuttavia, con questi vantaggi sono emerse anche nuove minacce dalle quali dobbiamo proteggerci. Una delle più dannose tra queste è rappresentata dal phishing, un fenomeno sempre più diffuso e sofisticato, che mette a repentaglio la sicurezza degli utenti e delle organizzazioni che operano nel mondo digitale.

Il presente elaborato si propone di analizzare approfonditamente questo fenomeno, esaminando le sue origini, le tecniche utilizzate dagli aggressori, gli impatti sulle vittime e le contromisure disponibili per contrastarlo efficacemente. Attraverso questa ricerca, si mira a contribuire ad una migliore comprensione del phishing, fornendo un quadro completo delle sue implicazioni e raccomandazioni utili per proteggere le informazioni personali online.

1. INTRODUZIONE AL FENOMENO

1.1 PHISHING: DEFINIZIONE

Il **phishing** è una forma di attacco informatico in cui gli aggressori cercano di ottenere informazioni personali e sensibili come nomi utente, password, numeri di carte di credito o altre informazioni finanziarie, ingannando le persone attraverso la creazione di siti web o messaggi falsi che sembrano provenire da fonti legittime. La parola "phishing" è un gioco di parole che combina la parola "fishing" (pesca) con la lettera "ph" che fa riferimento alla parola "phreaking", una pratica illegale legata alla manipolazione dei sistemi telefonici[1].

I truffatori utilizzano **e-mail**, **messaggi** di testo o **chiamate** telefoniche ingannevoli per indurre le vittime a fornire volontariamente le loro informazioni. Ad esempio, si potrebbe ricevere una e-mail che sembra provenire dalla propria banca, che chiede di fare clic su un link e inserire le tue credenziali per verificare il proprio account. Tuttavia, il link indirizzerà a un sito web falso che raccoglie le informazioni personali. Il phishing può anche coinvolgere altre forme di ingegneria sociale, come la creazione di siti web o pagine di accesso che sembrano identiche a quelle legittime, ma che in realtà raccolgono le credenziali dell'utente.

L'**obiettivo** del phishing è quello di rubare le informazioni personali delle vittime al fine di **commettere frodi**, **rubare identità** o **accedere ad account finanziari**. È importante essere consapevoli di questo tipo di attacco informatico e prestare attenzione alle notifiche sospette o alle richieste di informazioni personali provenienti da fonti non attendibili.

1.2 QUANDO NASCE IL PHISHING?

Il fenomeno del phishing ha avuto inizio negli **anni '90**, anche se le sue radici possono essere rintracciate in precedenza. La pratica del phishing si è evoluta parallelamente alla crescita delle comunicazioni elettroniche, come l'uso diffuso delle e-mail e degli strumenti di messaggistica.
Il termine "phishing" è stato coniato nel **1996** da un hacker e programmatore neozelandese, ma la

[1] "Phishing: cos'è?", https://www.euroconsumatori.org/it/ecommerce_phishing#:~:text=Etimologia%3A%20da%20dove%20proviene%20il,dati%20sensibili%20di%20un%20utente.

pratica stessa era già in corso da diverso tempo[2]. Tuttavia, è stato nel corso degli anni 2000 che il phishing ha raggiunto una maggiore notorietà e si è diffuso su larga scala.

Il **primo tipo di phishing documentato** è stato il "phishing bancario", in cui gli aggressori cercavano di ottenere le credenziali di accesso dei clienti delle banche. Questo è stato reso possibile attraverso l'invio di e-mail false che sembravano provenire da istituti finanziari legittimi e che chiedevano agli utenti di fornire le loro informazioni personali.

Negli anni successivi, il phishing si è evoluto ulteriormente e ha incluso **altre forme di ingegneria sociale**, come il phishing basato su siti web falsi e le truffe che coinvolgono marchi e servizi popolari. Gli aggressori hanno affinato le loro tecniche per rendere le loro comunicazioni e i loro siti web sempre più convincenti, cercando di indurre le persone a rivelare le loro informazioni personali senza sospettare nulla. Da allora, il phishing è diventato uno dei tipi di attacchi informatici più diffusi e continua ad essere un problema significativo per gli utenti di Internet in tutto il mondo.

1.3 TIPOLOGIE DI PHISHING

Il phishing può presentarsi in diverse forme e varianti, di seguito sono riportate le più comuni[3]:

1. **Phishing via e-mail**: questa è la variante più diffusa di phishing. Gli aggressori inviano e-mail che sembrano provenire da organizzazioni legittime come banche, fornitori di servizi online, istituzioni governative o società di e-commerce. Le e-mail contengono spesso richieste di aggiornamento delle informazioni dell'account o avvisi di sicurezza, in maniera tale da indurre le vittime a cliccare su link fraudolenti o a fornire le loro credenziali.

2. **Smishing**: questa forma di phishing avviene tramite messaggi di testo (o SMS) anziché tramite e-mail. Le vittime ricevono messaggi che sembrano provenire da organizzazioni legittime, con richieste di cliccare su link o fornire informazioni personali.

[2] "Breve storia del phishing", https://www.datamanager.it/2023/02/breve-storia-del-phishing/#:~:text=Il%20termine%20phishing%20%C3%A8%20stato,fishing%E2%80%9D%20a%20%E2%80%9Cphishing%E2%80%9D.
[3] "Phishing: come riconoscerlo e gli strumenti per difendersi", https://www.agendadigitale.eu/sicurezza/phishing-come-riconoscerlo-e-gli-strumenti-per-difendersi/

3. **Vishing**: variante del phishing che coinvolge chiamate telefoniche. Gli aggressori fingono di essere rappresentanti di istituti finanziari o società legittime e cercano di ottenere informazioni personali o finanziarie attraverso l'inganno.

4. **Pharming**: consiste nel reindirizzare il traffico web da un sito legittimo a uno falso, per richiedere informazioni o installare malware sul computer dell'utente, al fine di ottenere informazioni personali e finanziarie[4].

5. **Spear Phishing**: attacco mirato e personalizzato. Gli aggressori raccolgono informazioni dettagliate sulle loro vittime, come nome, ruolo lavorativo o relazioni personali, per creare e-mail o messaggi convincenti. Questo rende l'attacco molto più efficace, poiché le vittime sono più propense a cadere in inganno[5].

6. **Whaling**: il whaling (letteralmente "cacciare la balena", nell'accezione di grande pesce da far abboccare) è una forma avanzata di phishing rivolto a individui di alto profilo come dirigenti aziendali, politici o celebrità. Gli aggressori cercano di ottenere informazioni sensibili attraverso comunicazioni personalizzate[6].

1.4 FREQUENZE DEGLI ATTACCHI DI PHISHING: DATI UFFICIALI

È difficile fornire una **stima precisa** della frequenza degli attacchi di phishing poiché molti di essi non vengono segnalati o rilevati; in ogni caso, i dati ufficiali indicano che stanno aumentando vertiginosamente nel tempo. Basti pensare che, cercando tramite la parola chiave "phishing" nell'archivio dell'**Arbitro Bancario Finanziario** (ABF), si possono consultare documenti relativi a più di 7.000 decisioni[7].

[4] "BBVA: Cos'è il pharming e come puoi evitarlo", https://www.bbva.it/blog/cybersicurezza/consigli-sulla-sicurezza-/pharming-cose-e-come-evitarlo.html#:~:text=Il%20pharming%20%C3%A8%20un%20tipo,ottenere%20informazioni%20personali%20e%20finanziarie.

[5] "Cos'è il Cyber Spear Phishing e come proteggersi?", https://focus.namirial.it/spear-phishing/#:~:text=Lo%20Spear%20Phishing%20%C3%A8%20una,scaricare%20ransomware%20o%20altri%20malware.

[6] "Whaling", https://it.wikipedia.org/wiki/Whaling

[7] Arbitro Bancario Finanziario, Risoluzione Giudiziale Controversie, https://www.arbitrobancariofinanziario.it/decisioni/ricerca/ricerca.html?numero=&anno=&oggetto=&ft_tutte=phishing&ft_almeno=&ft_expr=&ft_senza=

SlashNext è un'azienda specializzata nella sicurezza informatica che si concentra sulla protezione contro le minacce di phishing e di social engineering. L'azienda utilizza tecnologie avanzate di intelligenza artificiale e machine learning per rilevare e mitigare gli attacchi di phishing in tempo reale. Secondo il rapporto "**2021 Phishing Trends and Intelligence Report**" di SlashNext, questi attacchi sono aumentati del **500%** nel 2020 rispetto all'anno precedente[8]. L'aumento significativo è stato attribuito alle opportunità di attacco create dalla pandemia di **COVID-19**, con aggressori che sfruttavano argomenti correlati come test, vaccini, cure mediche e aiuti finanziari per ingannare gli utenti.

Il rapporto annuale "**Data Breach Investigations Report**" di Verizon è una delle pubblicazioni più autorevoli nel campo delle violazioni dei dati e delle minacce informatiche. Il rapporto analizza una vasta gamma di fattori correlati alle violazioni dei dati, compresi i metodi di attacco utilizzati e le tendenze delle varie minacce. Il rapporto del 2021 ha rilevato che il phishing è stato la causa principale di fuga di dati, costituendo **il 36% della totalità degli attacchi registrati nel 2020**[9]. Ancora una volta, viene sottolineato come la pandemia di COVID-19 abbia creato uno stato favorevole per questo fenomeno: gli hacker hanno sfruttato la confusione, la paura e l'aumento delle attività sul web. Le persone sono state esposte in maniera maggiore ad e-mail spam, falsi siti web di informazioni sulla pandemia e promozioni di vaccini.

APWG (Anti-Phishing Working Group) è un'organizzazione internazionale che si occupa di monitorare e combattere il phishing. Il loro rapporto "**Phishing Activity Trends Report**" offre solitamente un'analisi dettagliata dei trend e dei modelli degli attacchi di phishing rilevati in un determinato periodo. Secondo il rapporto "Phishing Activity Trends Report" pubblicato da APWG nel 2021, è stato osservato un aumento significativo dei tentativi durante l'anno precedente. Nel primo trimestre del 2021, il numero di domini correlati a questo fenomeno rilevati è aumentato del 47,6% rispetto al trimestre precedente[10].

Inoltre, il rapporto "**Internet Security Threat Report**" di Symantec (azienda leader nel settore della sicurezza informatica) per il 2021 ha rilevato che il phishing rappresentava il 75% di tutti gli

[8] "The state of phishing 2021", https://slashnext.com/the-state-of-phishing-2021/
[9] "Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report", https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
[10] "PHISHING ACTIVITY TRENDS REPORT", https://apwg.org/trendsreports/

attacchi di malware osservati. Ciò indica che è ancora uno dei metodi più diffusi e efficaci utilizzati dagli aggressori per ottenere informazioni personali e finanziarie.

1.5 SETTORI BERSAGLIO

Il phishing può mirare a un'**ampia gamma di settori** e **tipi di utenti**, ma ci sono alcuni settori che sono spesso bersaglio privilegiato dei suoi attacchi. Alcuni dei settori più comuni che vengono presi di mira sono:

1. **Settore finanziario**: uno dei bersagli più comuni. Gli aggressori cercano di ottenere informazioni finanziarie sensibili, come numeri di conto bancario, password di accesso ai servizi online o informazioni sulla carta di credito, con l'obiettivo di commettere frodi finanziarie.

2. **E-commerce**: in questo caso si mira agli utenti che fanno acquisti sul web per ottenere informazioni di pagamento o credenziali di accesso ai loro account di compere online. Ciò consente agli hacker di effettuare transazioni illecite o rubare le informazioni personali dei clienti.

3. **Social media**: i social media sono diventati un terreno fertile per gli attacchi di phishing. Creando falsi account o utilizzando tecniche di ingegneria sociale, si convincono gli utenti a condividere le loro credenziali di accesso ai social media. Ciò consente di accedervi, diffondere messaggi malevoli o rubare informazioni personali.

4. **Servizi di posta elettronica e cloud**: gli aggressori mirano spesso agli utenti di servizi di posta elettronica e cloud, come Gmail, Outlook, Dropbox o Google Drive. Attraverso messaggi di phishing, si cerca di ottenere accesso alle credenziali di accesso o alle informazioni personali degli utenti.

5. **Settore governativo**: anche questo settore è preso spesso di mira dagli attacchi di phishing. Gli aggressori cercano di ottenere informazioni sensibili sugli utenti o di compromettere i sistemi governativi per fini malevoli.

6. **Settore delle risorse umane**: gli aggressori possono mirare ai dipendenti o ai responsabili delle risorse umane di un'organizzazione al fine di ottenere informazioni sul personale, dati sensibili o effettuare frodi relative a pagamenti o benefici.

È importante sottolineare che il phishing **può colpire in qualsiasi settore** e che le tattiche degli aggressori possono cambiare nel tempo. Pertanto, è molto importante adottare misure di sicurezza per proteggere sé stessi e le proprie informazioni online, indipendentemente dal settore in cui si opera.

2. PHISHING E GDPR

2.1 BREVE INTRODUZIONE AL GDPR

Il **General Data Protection Regulation** (GDPR) è una legislazione sulla protezione dei dati che è entrata in vigore nell'Unione Europea il 25 maggio 2018. Il GDPR è progettato per armonizzare e rafforzare le norme sulla protezione dei dati personali all'interno dell'UE, fornendo ai cittadini dell'UE maggiori diritti e controllo sulla loro privacy e alle organizzazioni linee guida chiare per la gestione dei dati personali[11].

Il GDPR si applica a tutte le **organizzazioni che gestiscono e trattano dati personali di cittadini dell'UE**, indipendentemente da dove siano situate le organizzazioni stesse. Ciò significa che le aziende al di fuori dell'UE che raccolgono o trattano dati personali di cittadini dell'UE sono tenute a conformarsi al GDPR. Inoltre, esso si basa su una serie di **principi fondamentali** per il trattamento dei dati personali. Tra questi vi sono: liceità, trasparenza, l'accuratezza, limitazione della conservazione, l'integrità e la riservatezza, responsabilità del titolare del trattamento, ecc... Per questi motivi, il GDPR richiede che il trattamento dei dati personali sia basato su una base giuridica. Queste basi possono includere, ad esempio, il consenso esplicito dell'individuo, l'esecuzione di un contratto o l'adempimento di un obbligo legale.

Il GDPR conferisce ai cittadini dell'UE una serie di **diritti in merito ai dati personali**. Questi diritti includono il diritto di accesso, il diritto di rettifica, il diritto alla cancellazione (o "diritto all'oblio"), il diritto alla portabilità dei dati, e il diritto di revocare il consenso.

[11] "Cos'è il GDPR", https://www.cookiebot.com/it/gdpr/

Le organizzazioni sono tenute a **notificare le violazioni dei dati personali** all'autorità di controllo competente entro 72 ore dalla scoperta della violazione, a meno che la violazione non sia improbabile che rappresenti un rischio per i diritti e le libertà degli individui interessati. Inoltre, se viene gestita una grande quantità di dati personali, è obbligatorio nominare un **Responsabile della protezione dei dati**. L'RPD è responsabile della supervisione della conformità del trattamento dei dati e dell'interazione con le autorità di controllo[12].

2.2 COME IL PHISHING VIOLA IL GDPR

Il phishing rappresenta una violazione del GDPR se comporta la **raccolta o l'elaborazione illecita** di dati personali senza il consenso dell'individuo. Dato che gli attacchi di questo tipo spesso mirano a ottenere informazioni personali come nomi, indirizzi, numeri di carta di credito o altre informazioni sensibili, **violano i principi fondamentali** del GDPR (liceità, trasparenza, limitazione della finalità e la sicurezza dei dati personali). Il phishing viola poi direttamente diversi articoli del GDPR, anche a seconda delle circostanze specifiche dell'attacco e del tipo di dati personali che vengono sottratti. Di seguito sono riportati alcuni esempi di violazione degli articoli più conosciuti:

- **Articolo 5**: "I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato"[13]. Il phishing potrebbe violare i principi di liceità, trasparenza e limitazione della finalità del trattamento dei dati personali. Ad esempio, se un hacker acquisisce informazioni personali tramite un attacco di phishing (quindi senza il consenso dell'individuo interessato), viola il principio di liceità.

- **Articolo 6**: "Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità"[14]. Il phishing viola l'articolo 6, poichè l'aggressore non ha una giustificazione giuridica valida per il trattamento dei dati personali

[12] "Il Responsabile della protezione dei dati (RPD)", https://www.studioessepi.it/magazine/privacy/responsabile-della-protezione-dei-dati-rpd
[13] "Articolo 5. Principi applicabili al trattamento di dati personali", https://gdpr-text.com/it/read/article-5/
[14] "Articolo 6. Liceità del trattamento", https://gdpr-text.com/it/read/article-6/

ottenuti attraverso il suo attacco.

- **Articolo 7**: "La richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro."[15]. Il consenso ottenuto tramite un attacco di phishing ingannevole viola le imposizioni dell'articolo 7, che richiedono che il consenso sia libero, specifico, informato e inequivocabile.

- **Articolo 32**, o "articolo sulla sicurezza del trattamento": le organizzazioni sono tenute ad adottare tecniche e misure organizzative adeguate a proteggere i dati personali, e un attacco di phishing può essere considerato una violazione dell'articolo 32 se l'organizzazione non ha implementato adeguate misure di sicurezza per prevenire o mitigare l'attacco.

- **Articolo 33**: "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo"[16]. Se un attacco di phishing portasse alla violazione dei dati personali, l'organizzazione potrebbe essere tenuta a notificare l'autorità di controllo competente e gli individui interessati in conformità con l'articolo 33, a meno che la violazione non sia improbabile che rappresenti un rischio per i diritti e le libertà degli individui interessati.

Il GDPR prevede **multe amministrative** significative per le violazioni dei dati personali, che possono arrivare fino al **4% del fatturato** annuo globale di un'organizzazione o 20 milioni di euro, a seconda di quale cifra sia maggiore[17].

[15] "Articolo 7. Condizioni per il consenso", https://gdpr-text.com/it/read/article-7/
[16] "Articolo 33. Notifica di una violazione dei dati personali all'autorità di controllo", https://gdpr-text.com/it/read/article-33/
[17] "Le sanzioni in materia di protezione dei dati personali", https://protezionedatipersonali.it/sanzioni-protezione-dati-personali

3. CONTROMISURE ESISTENTI

3.1 FILTRI ANTISPAM

I **filtri antispam** sono strumenti di sicurezza progettati per identificare e bloccare e-mail indesiderate o dannose, inclusi i tentativi di phishing. In che modo costituiscono una contromisura di questo fenomeno?

Innanzitutto, i filtri antispam utilizzano algoritmi e regole predefinite per **analizzare il contenuto** delle e-mail in arrivo. Gli algoritmi cercano elementi comuni associati al phishing, come link sospetti, allegati pericolosi o testi ingannevoli. I filtri antispam esaminano anche gli **indirizzi e-mail dei mittenti** per individuare eventuali segni di sospetto o falsificazione. Ad esempio, se un mittente afferma di essere un'organizzazione legittima, ma l'indirizzo e-mail non corrisponde al dominio ufficiale della stessa, il sistema considera il messaggio come sospetto e agisce di conseguenza. Alcuni di questi sistemi possono utilizzare "**black list**" e "**white list**" per prendere decisioni sulle e-mail in arrivo. Le liste nere contengono indirizzi IP o domini noti per essere associati a spam o phishing, mentre le liste bianche contengono quelli considerati affidabili. Se un messaggio proviene da un indirizzo nella lista nera, viene bloccato o contrassegnato come spam. Infine, alcuni filtri antispam consentono agli utenti di creare **regole personalizzate** per il filtraggio delle e-mail[18].

È importante notare che i filtri antispam non sono perfetti e potrebbero occasionalmente identificare erroneamente e-mail legittime come spam o non rilevare alcune e-mail di phishing.

3.2 POLITICHE DI AUTENTICAZIONE A DUE FATTORI

La **2FA**, o **autenticazione a due fattori**, è un metodo di sicurezza che richiede due elementi distinti per verificare l'identità di un utente al momento dell'accesso a un account o a un sistema. Questo metodo di autenticazione è utilizzato per aumentare la sicurezza rispetto alla tradizionale autenticazione basata solo su una password[19].

Il **primo fattore** di autenticazione è solitamente qualcosa che l'utente conosce ed è in grado di fornire, come una password, un PIN o una frase segreta. Il **secondo fattore** di autenticazione è un elemento diverso dal primo che l'utente deve fornire per verificare la propria identità. Può essere qualcosa che l'utente possiede, come un telefono cellulare, un codice di sicurezza o una carta di credito, o qualcosa che l'utente è, come un'impronta digitale o una scansione del voltp. Quando un utente tenta di accedere a un account protetto da questo metodo, viene richiesto di fornire entrambi i

[18] "Filtri antispam: cosa sono e come proteggono i tuoi dati?", https://www.pianetaitalia.com/blog/filtri-antispam-cosa-sono-e-perche-dovresti-attivarli-proprio-adesso#:~:text=E%20la%20funzione%20principale%20di,due%20categorie%3A%20sane%20e%20malate.
[19] "Autenticazione a due fattori: cos'è e a cosa serve", https://www.pandasecurity.com/it/mediacenter/tecnologia/autenticazione-a-due-fattori/

fattori. Ad esempio, dopo aver inserito correttamente la password, viene di inserire un codice di verifica generato inviato per SMS sul proprio cellulare.

L'obiettivo principale della 2FA è creare un ulteriore campo di sicurezza. Anche se un utente dovesse cadere vittima di phishing e la sua password venisse compromessa, l'aggressore avrebbe bisogno del secondo fattore di autenticazione per ottenere l'accesso. Questo rende molto più difficile accedere ai dati sensibili o prendere il controllo dell'account dell'utente.

3.3 FORMAZIONE DEGLI UTENTI E ALTRE CONTROMISURE INDIVIDUALI

Esistono tantissime contromisure che possono essere adottate individualmente per proteggersi dal phishing in maniera autonoma. In primis, è importantissimo **educarsi** e comprendere le tecniche utilizzate dagli aggressori. Ad esempio, conoscere i segni di avvertimento tipici del phishing, come errori di ortografia e grammatica, URL sospetti o richieste di informazioni sensibili, può aiutare a identificare questi tentativi. Inoltre, **mantenersi informati** sulle nuove tecniche di phishing e condividere queste informazioni con colleghi, amici e familiari può contribuire a proteggere molte persone.

Prima di fornire qualsiasi informazione personale o finanziaria online, è importante **verificare l'identità del mittente**. Se si riceve un'e-mail che sembra provenire da una determinata organizzazione, è consigliabile contattare direttamente l'organizzazione stessa utilizzando informazioni di contatto autentiche per verificare se la richiesta è legittima. Può aiutare anche **evitare di fare click su link sospetti** o non richiesti. È meglio digitare l'indirizzo direttamente nella barra degli indirizzi del browser o passare il mouse sopra i link per verificare l'URL prima di fare click.

Ultimo ma non per importanza, è consigliabile assicurarsi che il **sistema operativo**, il browser e gli altri software siano sempre aggiornati con le ultime misure di sicurezza. Questo riduce le vulnerabilità che gli aggressori potrebbero sfruttare per scopi di phishing. Installare un sistema di protezione **antivirus** può aiutare in tal senso[20].

[20] "Commissariato di Polizia Postale: Phishing, consigli" https://www.commissariatodips.it/approfondimenti/phishing/consigli/index.html

4. CASI DI STUDIO

4.1 CASO PAYPAL (2003)

PayPal è un servizio di pagamento online che consente agli utenti di inviare e ricevere denaro in modo sicuro tramite Internet. Ad oggi, 250 milioni di persone usano PayPal per fare acquisti su milioni di siti web nel mondo, in oltre 200 mercati e 25 valute diverse[21]. Nel **2003** fu preso di mira da un attacco di phishing di notevole rilievo. Gli aggressori inviarono milioni di e-mail fraudolente a utenti PayPal, cercando di ingannarli per ottenere le loro informazioni e dati finanziari sensibili. Si stima che oltre **7 milioni di utenti** furono vittima di furto d'identità tra Giugno 2002 e Giugno 2003[22].

Le e-mail inviate sembravano provenire da PayPal e presentavano un aspetto molto simile alle comunicazioni ufficiali dell'azienda. Queste spingevano gli utenti a visitare un **sito web contraffatto** che sembrava identico a quello di PayPal, ma in realtà era controllato dagli aggressori. Qui agli utenti veniva richiesto di inserire le proprie credenziali di accesso, come nome utente e password, così come altre informazioni personali e finanziarie, tra cui numeri di carta di credito e dettagli bancari. Gli aggressori utilizzavano queste informazioni per rubare denaro dagli account PayPal degli utenti o commettere frodi finanziarie.

L'attacco di phishing a PayPal nel 2003 è stato un **evento significativo** perché ha contribuito a portare l'attenzione sul problema del phishing e ha reso le persone più consapevoli dei rischi associati alle e-mail fraudolente. Ha dimostrato che anche i servizi online di fiducia e con una vasta base di utenti possono essere soggetti a questo tipo di attacco. Successivamente a questo caso, PayPal e altre organizzazioni hanno adottato **misure più rigorose** per combattere il phishing. Ciò include l'implementazione di avvisi di sicurezza, l'educazione degli utenti sulla rilevanza del phishing e l'uso di strumenti di rilevamento e prevenzione più avanzati per identificare e bloccare gli attacchi di phishing in modo più efficace.

4.2 CASO RSA SECURITY (2011)

RSA Security è una società che offre soluzioni di sicurezza informatica. e sue tecnologie vengono utilizzate per proteggere dati sensibili, autenticare utenti e garantire la privacy delle comunicazioni digitali[23]. Per quanto assurdo possa sembrare, proprio quest'azienda fu protagonista di uno degli attacchi cibernetici più complessi mai studiati.

L'Attacco di phishing a RSA Security del **2011** è noto anche come "**Operazione Aurora**". L'attacco è stato condotto da un gruppo di hacker avanzati presumibilmente legati al governo cinese. Hacoinvolto varie fasi e tecniche sofisticate per compromettere la sicurezza di RSA Security e

[21] "Che cos'è PayPal?", https://www.paypal.com/it/webapps/mpp/paypal-popup.
[22] "PayPal Fraud: Phishy Business", https://www.csoonline.com/article/2116726/paypal-fraud--phishy-business.html
[23] "About us", https://www.rsa.com/company/

ottenere ccesso a informazioni sensibili[24]. L'attacco è stato avviato inviando **e-mail di phishing mirate agli impiegati** di RSA Security. Queste e-mail sembravano provenire da colleghi di lavoro affidabili e contenevano allegati dannosi o link dannosi. Una volta che un dipendente di RSA Security ha aperto l'allegato o fatto clic sul link, il malware si è insinuato nei sistemi interni dell'azienda. Il malware utilizzato nell'Operazione Aurora era noto come "**Hydraq**" e permetteva agli aggressori di eseguire una serie di azioni dannose, inclusa la raccolta di informazioni sensibili e l'esfiltrazione di dati.

L'obiettivo finale dell'Operazione Aurora era quello di compromettere il sistema di **autenticazione a due fattori** di RSA Security, noto come SecurID. I criminali informatici avevano come scopo il furto delle chiavi utilizzate per generare le password del sistema. L'attacco ha avuto successo e ha compromesso la sicurezza di RSA Security. Sebbene RSA abbia subito perdite significative, il vero impatto di questa operazione è emerso in seguito: le informazioni ottenute dall'attacco sono state utilizzate per compromettere altre aziende e organizzazioni in tutto il mondo, come governi e aziende.

L'Operazione Aurora ha sollevato preoccupazioni sulla sicurezza informatica a livello mondiale e ha messo in evidenza il fenomeno degli **attacchi sponsorizzati dallo Stato**.

4.3 CASO COMITATO NAZIONALE DEMOCRATICO USA (2016)

Il **Comitato Nazionale Democratico americano** ("Democratic National Committee", o DNC) è l'organizzazione ufficiale del Partito Democratico degli Stati Uniti. Il suo ruolo principale è quello di sostenere il Partito Democratico nella promozione dei suoi valori, nella definizione delle politiche, nell'organizzazione delle elezioni e nella raccolta di fondi per le campagne politiche[25].

Nel 2016, il DNC ha subito un attacco di phishing che ha attirato l'attenzione internazionale, in quanto attribuito a un gruppo di hacker russi noto come **Fancy Bear[26]** o APT28, con possibili legami con l'intelligence russa[27]. L'obiettivo principale dell'attacco era compromettere raccogliere informazioni sensibili e influenzare le elezioni presidenziali statunitensi del 2016.

L'attacco è iniziato con l'invio di **e-mail di phishing** indirizzate a membri chiave del DNC. Le e-mail sembravano legittime e spingevano a fare clic su link dannosi, fornendo le proprie credenziali di accesso. Attraverso questa tecnica, gli hacker sono riusciti a ottenere l'accesso non autorizzato ai sistemi del DNC. Successivamente, hanno eseguito operazioni di spionaggio e raccolta di informazioni come e-mail, documenti interni e comunicazioni riservate. Questi ultimi sono stati poi pubblicati su siti come "WikiLeaks" e altri. Le informazioni divulgate hanno avuto un impatto significativo sulle **elezioni presidenziali statunitensi del 2016**.

[24] "RSA: Anatomy of an attack", http://blogs.rsa.com/rivner/anatomy-of-an-attack/
[25] "Democratic National Committee", https://www.britannica.com/topic/Democratic-National-Committee
[26] "Fancy Bear", https://it.wikipedia.org/wiki/Fancy_Bear
[27] "The Guardian: DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach", https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2

Tra le informazioni rilasciate c'erano e-mail interne del DNC che rivelavano conversazioni delicate e strategie politiche. Ciò ha sollevato molte controversie e ha alimentato il dibattito pubblico durante la campagna elettorale. Questo attacco, inoltre, ha evidenziato il potenziale del phishing come strumento di **minaccia per gli organismi governativi**.

5. CONCLUSIONI

Nel corso di questo elaborato, è stato esaminato approfonditamente il fenomeno del phishing e le sue **implicazioni** per gli utenti e le organizzazioni. L'analisi di alcuni casi realmente avvenuti, inoltre, ha permesso di evidenziare la complessità e la costante evoluzione di questa minaccia a livello informatico. Gli aggressori online, infatti, cercano costantemente di ingannare gli utenti fingendo di essere organizzazioni affidabili e usando tecnologie sempre più sofisticate.

Le **conseguenze** di questo fenomeno possono essere devastanti per gli utenti coinvolti: possono subire danni finanziari, furto d'identità o perdita di dati sensibili. D'altro canto, le organizzazioni possono subire danni reputazionali, perdite finanziarie importanti e violazioni della privacy dei loro clienti. In ogni caso, nel corso di questa breve ricerca sono state individuate molteplici **contromisure** efficaci per mitigare il rischio di incappare nel phishing. Le politiche di autenticazione a due fattori, l'implementazione di filtri antispam, l'educazione degli utenti e la sensibilizzazione sono tutti strumenti importanti per contrastarlo. Ognuna di queste contromisure, ovviamente, non è perfetta e ha i suoi punti deboli, prestandosi a diverse migliorie che potrebbero essere implementate in futuro.

Infine, appare evidente come la lotta contro il phishing richieda un **approccio multilivello**, in cui le organizzazioni, gli individui del web e gli enti collaborano per sviluppare delle misure di sicurezza che ne siano all'altezza.

6. SITOGRAFIA

1. **“Phishing: cos’è?”,** https://www.euroconsumatori.org/it/ecommerce_phishing#:~:text=Etimologia%3A%20da%20dove%20proviene%20il,dati%20sensibili%20di%20un%20utente.

2. **“Breve storia del phishing”,** https://www.datamanager.it/2023/02/breve-storia-del-phishing/#:~:text=Il%20termine%20phishing%20%C3%A8%20stato,fishing%E2%80%9D%20a%20%E2%80%9Cphishing%E2%80%9D.

3. **“Phishing: come riconoscerlo e gli strumenti per difendersi”,** https://www.agendadigitale.eu/sicurezza/phishing-come-riconoscerlo-e-gli-strumenti-per-difendersi/

4. **“BBVA: Cos’è il pharming e come puoi evitarlo”,** https://www.bbva.it/blog/cybersicurezza/consigli-sulla-sicurezza-/pharming-cose-e-come-evitarlo.html#:~:text=Il%20pharming%20%C3%A8%20un%20tipo,ottenere%20informazioni%20personali%20e%20finanziarie.

5. **“Cos’è il Cyber Spear Phishing e come proteggersi?”,** https://focus.namirial.it/spear-phishing/#:~:text=Lo%20Spear%20Phishing%20%C3%A8%20una,scaricare%20ransomware%20o%20altri%20malware.

6. **“Whaling”,** https://it.wikipedia.org/wiki/Whaling

7. **Arbitro Bancario Finanziario, Risoluzione Giudiziale Controversie,** https://www.arbitrobancariofinanziario.it/decisioni/ricerca/ricerca.html?numero=&anno=&oggetto=&ft_tutte=phishing&ft_almeno=&ft_expr=&ft_senza=

8. **“The state of phishing 2021”,** https://slashnext.com/the-state-of-phishing-2021/

9. **“Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report”,** https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report

10. **“PHISHING ACTIVITY TRENDS REPORT”,** https://apwg.org/trendsreports/

11. **“Symantec Internet Security Threat Report”,** https://docs.broadcom.com/doc/istr-03-jan-en

12. **“Cos’è il GDPR”,** https://www.cookiebot.com/it/gdpr/

13. **"Il Responsabile della protezione dei dati (RPD)",** https://www.studioessepi.it/magazine/privacy/responsabile-della-protezione-dei-dati-rpd

14. **"Articolo 5. Principi applicabili al trattamento di dati personali",** https://gdpr-text.com/it/read/article-5/

15. **"Articolo 6. Liceità del trattamento",** https://gdpr-text.com/it/read/article-6/

16. **"Articolo 7. Condizioni per il consenso",** https://gdpr-text.com/it/read/article-7/

17. **"Articolo 33. Notifica di una violazione dei dati personali all'autorità di controllo",** https://gdpr-text.com/it/read/article-33/

18. **"Le sanzioni in materia di protezione dei dati personali",** https://protezionedatipersonali.it/sanzioni-protezione-dati-personali

19. **"Filtri antispam: cosa sono e come proteggono i tuoi dati?",** https://www.pianetaitalia.com/blog/filtri-antispam-cosa-sono-e-perche-dovresti-attivarli-proprio-adesso#:~:text=E%20la%20funzione%20principale%20di,due%20categorie%3A%20sane%20e%20malate.

20. **"Autenticazione a due fattori: cos'è e a cosa serve",** https://www.pandasecurity.com/it/mediacenter/tecnologia/autenticazione-a-due-fattori/

21. **"Commissariato di Polizia Postale: Phishing, consigli"** https://www.commissariatodips.it/approfondimenti/phishing/consigli/index.html

22. **"Che cos'è PayPal?",** https://www.paypal.com/it/webapps/mpp/paypal-popup.

23. **"PayPal Fraud: Phishy Business",** https://www.csoonline.com/article/2116726/paypal-fraud--phishy-business.html

24. **"About us",** https://www.rsa.com/about-us

25. **"RSA: Anatomy of an attack",** http://blogs.rsa.com/rivner/anatomy-of-an-attack/

26. **"Democratic National Committee",** https://www.britannica.com/topic/Democratic-National-Committee

27. **"Fancy Bear",** https://it.wikipedia.org/wiki/Fancy_Bear

28. **"The Guardian: DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach",** https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2