IL PHISHING

FACCIAMO CHIAREZZA

Prima di soffermarci a capire cos'è una mail di Phishing e come funziona, è fondamentale trasmettere a chi è meno pratico di queste tematiche il motivo per il quale dovrebbe essere interessato a capire cos'è il Phishing e perché potrebbe essere preso di mira da un attacco informatico di questo tipo.
Tecniche di attacco informatico come il Phishing crescono significativamente ogni anno, a dimostrazione del fatto che **le persone sono il veicolo maggiormente sfruttato per arrivare a dati ed informazioni aziendali**,
Lo confermano i dati:

- Il 75% degli incidenti di sicurezza è imputabile al fattore umano.
- Il 90% degli attacchi informatici inizia proprio con una mail di Phishing.

Sono dati che dimostrano come **chi attacca abbia ben capito quanto sia più facile e proficuo sfruttare le vulnerabilità umane piuttosto di quelle tecnologiche, con la conseguenza che la migliore difesa per questa tipologia di minaccia è la presa di consapevolezza e la formazione degli utenti che quotidianamente utilizzano PC e strumenti aziendali.**

IMQ Intuity
Security Awareness

CHE COS'È IL PHISHING?

Il phishing è un tentativo di frode realizzato mediante **l'invio di messaggi di posta dal contenuto apparentemente legittimo**. Queste mail hanno l'obiettivo di catturare l'attenzione della potenziale vittima, portarla a cliccare su link presenti al suo interno o aprire eventuali allegati.

Il Phishing consente ai malintenzionati di acquisire informazioni sensibili, come ad esempio credenziali di accesso a sistemi di posta aziendali, ad applicazioni e conti correnti o dettagli su carte di credito.

Nel caso la mail fraudolenta contenesse un allegato apparentemente lecito, questo potrebbe avere al suo interno un ransomware, in grado di infettare i dispositivi e rendere inaccessibili i dati aziendali, chiedendo successivamente un riscatto per ripristinarli.

LE TECNICHE UTILIZZATE

SPEAR PHISHING

A differenza del Mass Phishing, il più comune dei phishing, caratterizzato dall'invio di e-mail malevole in maniera massiva senza una regola precisa per la scelta del target, lo **Spear Phishing è invece un tipo di attacco di phishing mirato** che ha molta più probabilità di successo. Il contenuto di questa e-mail, infatti, viene **attentamente adattato in base al profilo aziendale dell'azienda target dell'attacco informatico**.

Questa tipologia di Phishing è molto pericolosa, perché pianificata in modo accurato, presupponendo in fase di preparazione d'attacco, un'attività di OSINT (Open Source INTelligence) focalizzata a raccogliere informazioni sull'azienda e sul suo personale, utili a personalizzare il contenuto delle mail di Phishing con l'obiettivo di renderla il più possibile credibile.

WHALING

Una forma ancor più specifica dello Spear Phishing è quella del Whaling, detta "**caccia alla balena**". Campagne di Phishing di questo tipo prendono di mira figure strategiche per l'azienda (es. CFO) o di alto profilo (es. CEO) e potrebbero avere per l'azienda seri impatti sul business o sulla propria reputazione.

GLI ARGOMENTI PIÙ SFRUTTATI

I contenuti utilizzati per adescare le vittime sono realizzati per mirare alle **"vulnerabilità umane"** quali ad esempio:

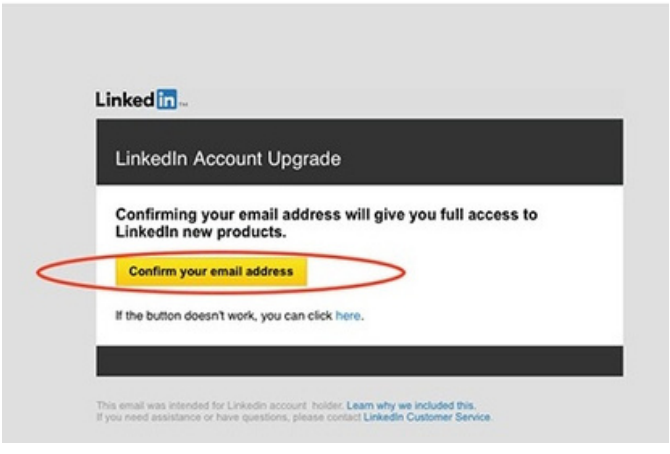
- **Curiosità**: fake-news su celebrità o su fatti davvero insoliti.
- **Paura**: PC compromesso.
- **Emozione**: petizioni a fin di bene.
- **Situazioni:** offerte di Natale o di altre festività.
- **Fretta**: pagamenti o account in scadenza.
- **Ricompensa**: vincite facili.

COVID-19

Da una ricerca di KnowBe4, le campagne di Phishing a tema coronavirus e avvisi di Social Media sono stati gli argomenti maggiormente sfruttati nel primo semestre del 2020.
In particolare, rispetto al **tema di Covid-19** non sorprende notare che il 56% delle mail di Phishing abbia sfruttato proprio una situazione di emergenza globale e di smart working diffuso per rendere credibili, ad esempio, avvisi di riaperture commerciali, inviti a meeting su piattaforme di teleconferenza, aggiornamenti di contagio o approfondimenti sanitari.

LINKEDIN

In cima alla lista dei contenuti Social maggiormente sfruttati per le campagne di Phishing (42%), ritroviamo ancora le mail di **avviso di LinkedIn**, come ad esempio la richiesta di aggiornamento della password, le notifiche di tag o di nuovi messaggi. Le campagne che sfruttano la comunicazione di LinkedIn sono piuttosto pericolose, in quanto spesso le credenziali utilizzate dagli utenti per l'accesso a questa rete professionale sono le stesse utilizzate anche per accedere ad account di posta aziendali.



COME RICONOSCERE UNA MAIL DI PHISHING

I CONSIGLI DI IMQ INTUITY

È possibile attuare alcuni accorgimenti per riuscire a riconoscere una mail di Phishing senza dover essere un esperto in materia.
Innanzitutto, il miglior aiuto che possiamo avere è quello che viene dal nostro **buon senso**: è importante controllare il nome e l'indirizzo e-mail del mittente e porsi alcune domande del tipo:

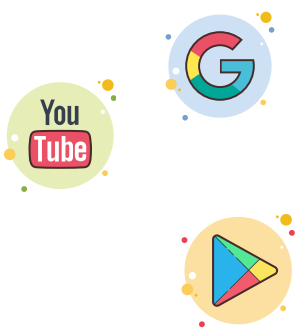
- Si tratta di una persona appartenente all'azienda?
- È correlata al mio lavoro?
- Il dominio dell'indirizzo e-mail con il quale scrive è pertinente al contenuto del messaggio?

Se nella mail ci viene chiesto di fare qualcosa come, ad esempio, inserire e/o modificare delle credenziali, aprire un allegato, visitare un sito web, etc., prima di farlo e di procedere con la richiesta o cliccare su qualche link o documento allegato, chiediamoci "Perché lo dovrei fare? Ha senso quello che mi chiede?".

L'indirizzo e-mail del mittente è un altro elemento utile per poter valutare la mail come autentica o pericolosa. In particolar modo, verificare con attenzione il dominio permette di capire chi è la vera azienda o ente che ci sta contattando.

La lettura dell'indirizzo e-mail del mittente non è un'azione da prendere alla leggera, in quanto gli attaccanti, per ingannare gli utenti più frettolosi e poco attenti, utilizzano una tipologia di truffa informatica chiamata **Typosquatting.** Consiste nella registrazione di domini con nomi molto simili agli originali. Di seguito alcuni tra gli esempi più famosi:

- Yotube.com
- Yutube.com
- Facebok.com
- Goggle.com



LINK

Un'altra raccomandazione è di non fidarsi mai totalmente dei **link** presenti in e-mail dal mittente o dal contenuto sospetti. Una buona abitudine, per effettuare un controllo veloce sull'autenticità o meno di un link, è quello di posizionarci sopra con il cursore del mouse, senza cliccare, ed osservare il pop-up che appare.

L'indirizzo web che compare al suo interno è l'indirizzo web verso il quale il link realmente punta.

Dall'immagine appare chiaro che il link non sta puntando al sito di PayPal, bensì verso qualche altra pagina. In questo caso non clicchiamoci e non fidiamoci della mail che contiene questo link.

ALLEGATI

Un'attenzione scrupolosa va inoltre riservata agli **allegati** che riceviamo via mail. Prima di scaricare e aprire un documento è bene seguire tutte le verifiche appena descritte, chiedendoci in primis perché abbiamo ricevuto tale documento e se lo aspettavamo. Anche di fronte ad un apparente ed innocuo volantino pubblicitario facciamo attenzione e poniamoci alcune semplici domande:

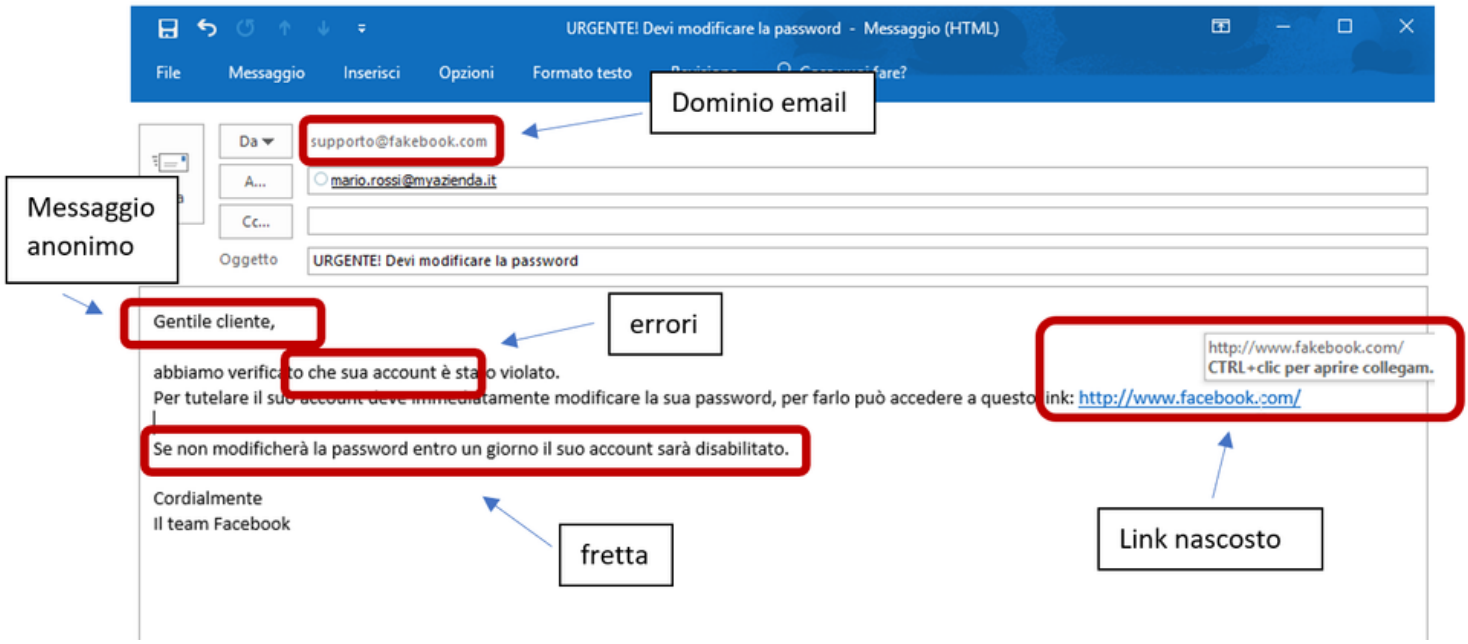
- Il testo della mail è scritto in italiano corretto o presenta errori?
- L'azienda o l'esercizio commerciale che mi manda questo documento esiste davvero?
- Il dominio dell'indirizzo mail corrisponde a quello reale? Questo lo possiamo verificare cercando nel sito, alla sezione contatti, o chiamando direttamente l'azienda per constatare che quanto ricevuto faccia parte davvero di una comunicazione/documento ufficiale.

CHECKLIST

Riassumiamo le attenzioni da prestare nei confronti di e-mail sospette, di cui non conosciamo il mittente, che non attendavamo o che ci chiedono di far qualcosa, come inserire credenziali, effettuare pagamenti, modificare estremi bancari come nuovo IBAN o altre azioni di carattere finanziario/strategico.

- ✓ Controllo dell'**indirizzo e-mail del mittente**, con particolare attenzione al dominio.
- ✓ Controllo del **corpo della mail**: si stratta di un messaggio anonimo? Presenta diversi errori? È scritto con un italiano corretto?
- ✓ Controllo dei **link**: rimandano a siti che non sono plausibili con la mail ricevuta o presentano un URL simile all'originale?
- ✓ Attenzione alla **ragione ed obiettivo della e-mail**: ci viene chiesto di far qualcosa? Perché c'è stata inviata?

Nell'immagine sotto, una di mail di Phishing ricevuta da un'indirizzo mail con dominio "@fakebook": tipico esempio di Typosquatting (vedi sopra).
Nella mail viene richiesto di modificare, al link inserito nel testo, le credenziali di accesso a Facebook, in quanto la mail avvisa che il proprio account potrebbe essere stato violato.
Seguendo gli accorgimenti descritti sopra, si evince come questa mail non sia altro che un tentativo di frode, con l'obiettivo di ottenere delle credenziali personali di accesso, in questo specifico caso, a Facebook.



IMQ intuity
SOCIETÀ DEL GRUPPO IMQ

IMQ Intuity propone un approccio diverso alla Cybersecurity modificando lo status quo che vede nella soluzione tecnologica l'unico modo di affrontare il problema, quest'ultimo invece sempre più legato all'uomo ed al contesto sociale in cui esso opera.

La sicurezza informatica deve essere approcciata da un punto di vista Culturale, mettendo al centro le persone nel processo di sicurezza aziendale: **People-Centric Security**

www.intuity.it

IMQ INTUITY S.r.l.
Soggetta ad attività di direzione e coordinamento di IMQ Group S.r.l.

Sede operativa
via A. Ceron, 2 35129 Padova
049 817 0850 | info@intuity.it

Sede legale
via Quintiliano, 45 20138 Milano
admin@pec.intuity.it