



Incontro informativo

Benvenuti, dipendenti di Epicodesecurity!
L'argomento di oggi sarà: i rischi di attacchi di ingegneria sociale, in particolare il phishing!
Siete pronti?

Programma di oggi

Cosa è il phishing?

Attenzione: esistono vari tipi di phishing!

Impareremo a riconoscerli.

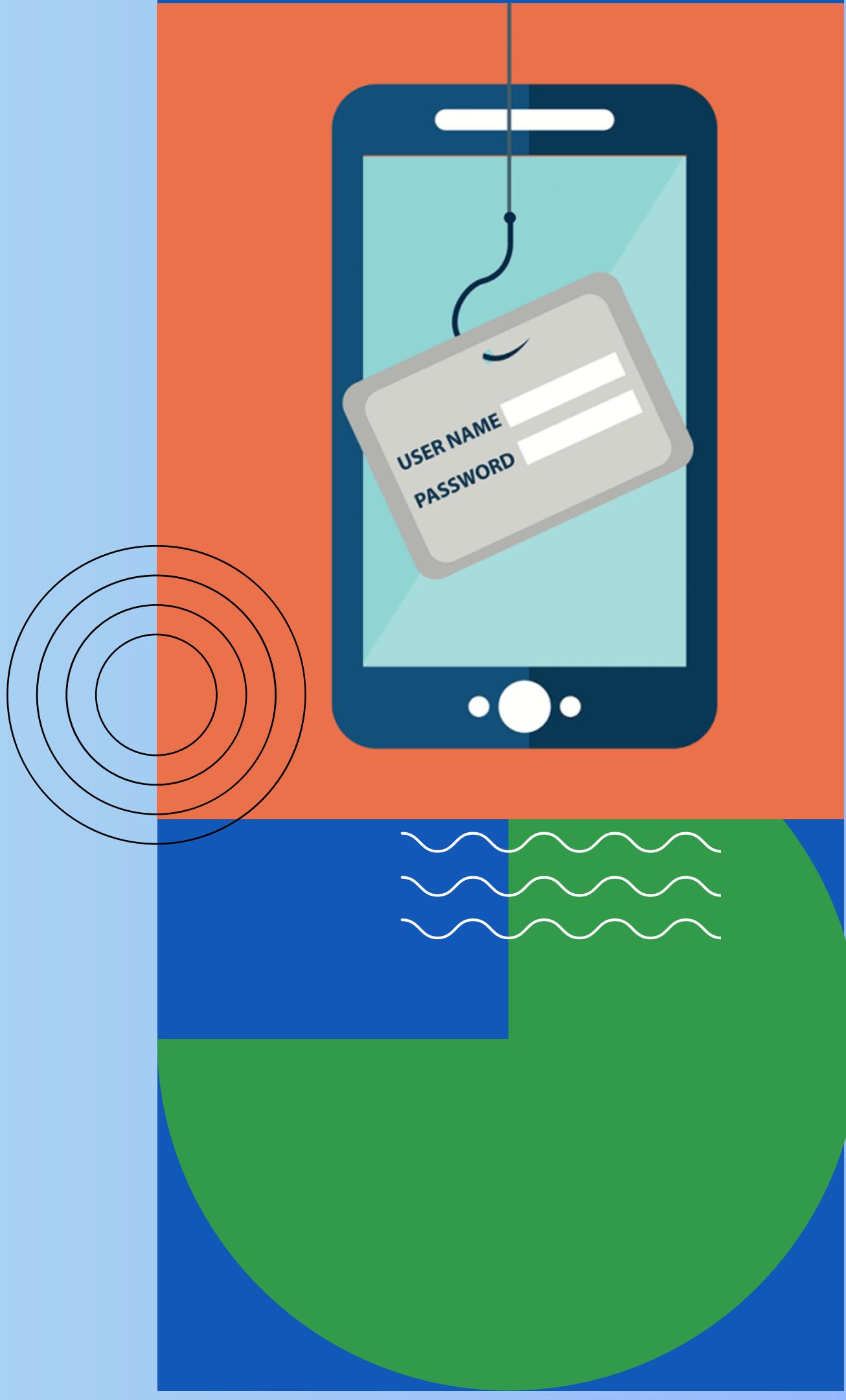
Come evitare di cadere nel phishing?

Seguite la presentazione di oggi
e sarete degli esperti!



Partiamo dalle basi: cosa è il phishing?

Il **phishing** coinvolge l'invio di e-mail o messaggi ingannevoli che cercano di indurre le persone a rivelare **informazioni personali**, come nomi utente, password o dati finanziari. Questo attacco sfrutta la fiducia della vittima, convincendola erroneamente che il messaggio provenga da una **fonte affidabile o legittima**.



Vari tipi di phishing:

Email phishing, spear phishing, whaling, smishing e vishing sono i principali tipi di attacco informatico che potrebbero essere messi a segno dai malintenzionati.

Ora esamineremo in dettaglio i vari tipi!



Email phishing

L'attacco viene messo a segno inviando un'**email**, che a prima vista potrebbe sembrare autentica, in cui ti si chiede di inserire i tuoi **dati sensibili** (credenziali, dati bancari, dati personali) per poter risolvere un problema o gestire un'emergenza. In queste email, si parla sempre a una **persona generica**, spesso dando del tu all'utente.



Spear phishing

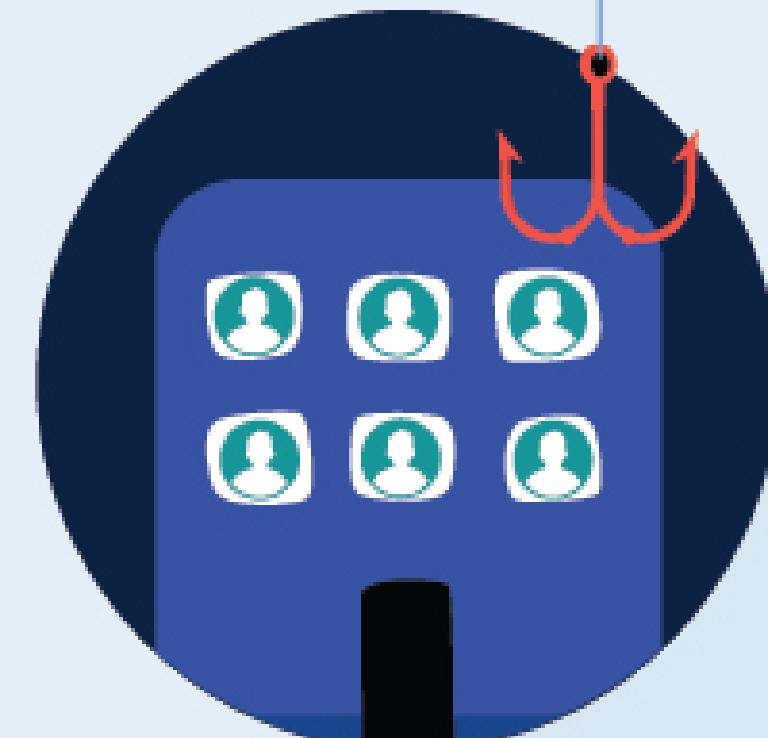
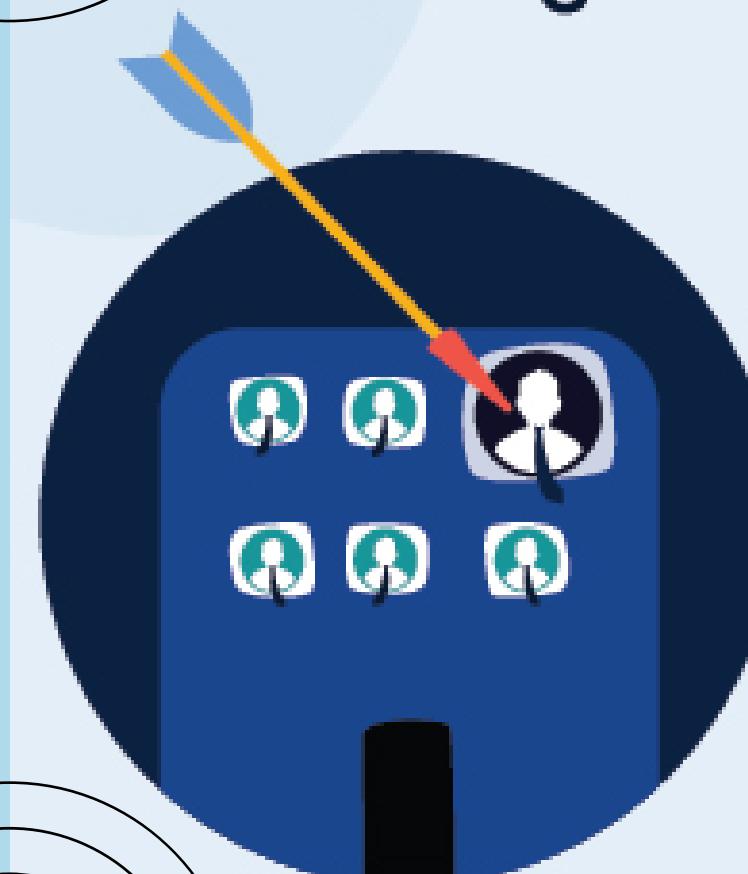
La finta comunicazione in questo caso viene indirizzata a una persona, un'organizzazione o un'azienda **specifica**. L'email quindi si rivolgerà direttamente a **te**, con il tuo nome e cognome, oppure all'organizzazione o all'azienda per cui lavori. Ad esempio: "Egregio Signor Rossi".



**Spear
Phishing**

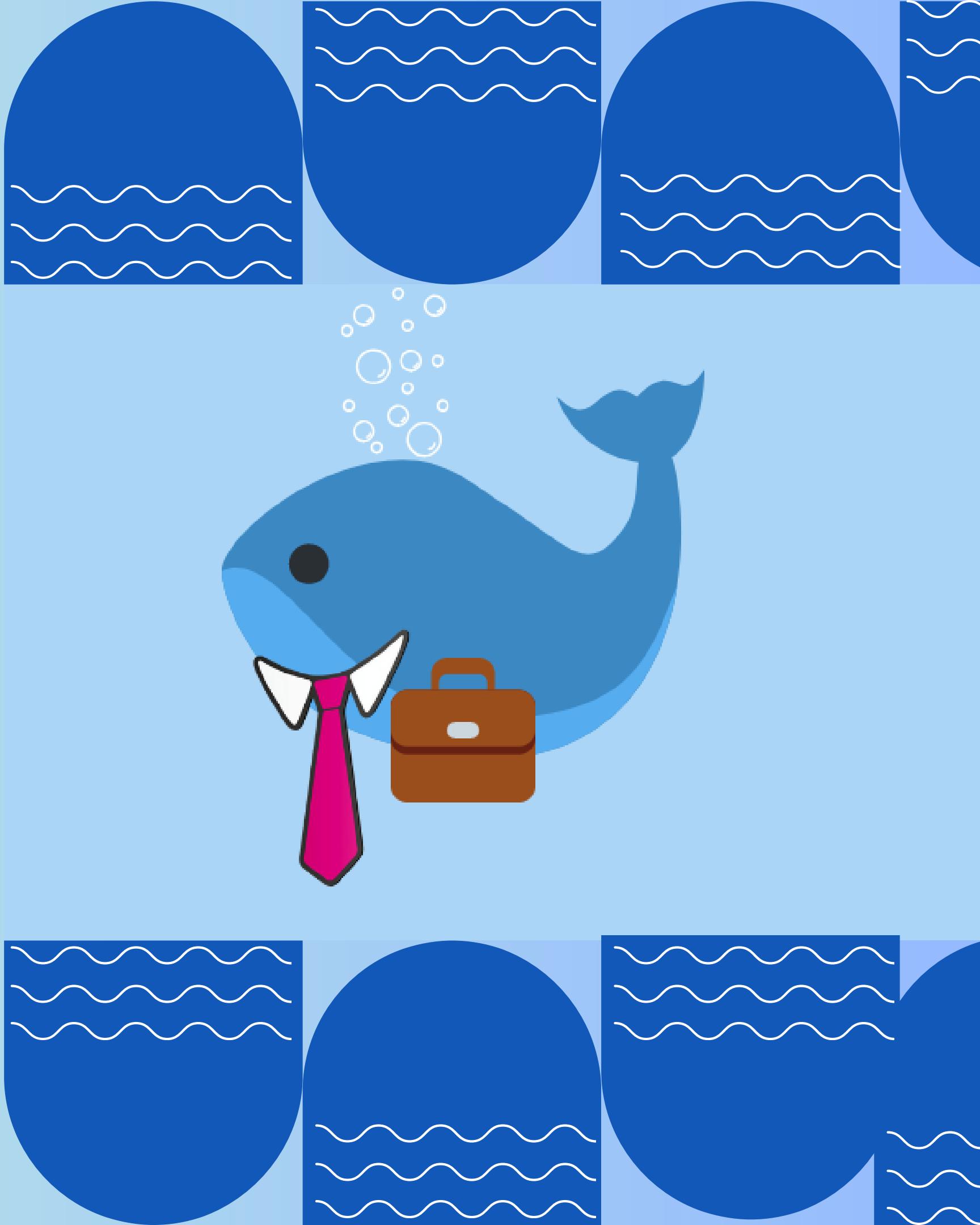
vs

Phishing



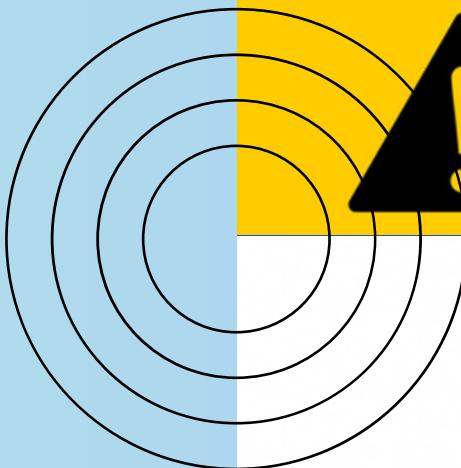
Whaling

Questo tipo di attacco prende di mira **professionisti** che svolgono un ruolo di spicco all'interno di un'azienda o di una associazione. L'esca che viene lanciata dai cybercriminali sarà quindi molto personalizzata, così da trarre in inganno la vittima. Puntando a persone che ricoprono posizioni di spicco, i cybercriminali sperano di recuperare informazioni e **dati sensibili di alto valore**.



Smishing

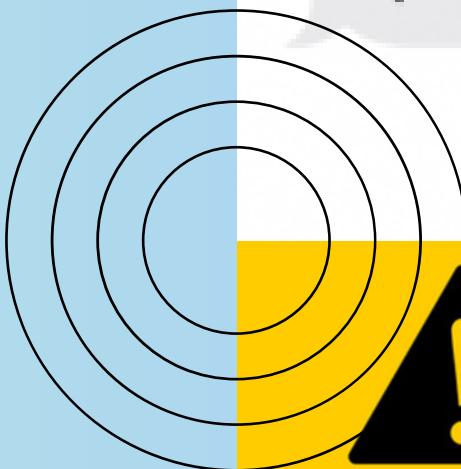
In questo caso la minaccia non arriva dalla tua email, l'attacco informatico è messo a segno attraverso l'invio di **SMS**. Si tratta di una minaccia insidiosa, perché solitamente si tende a **fidarsi** maggiormente di un SMS che di una email, rischiando così di cadere facile preda dei malintenzionati.



ATTENZIONE

SMS
oggi 16:55

Banca N26
ATTENZIONE! il Suo Conto
Verra' Sospeso Per Evitare La
Sospensione Clicca Su'
[https://banca-n26-sicuro-
com.preview-domain.com](https://banca-n26-sicuro-com.preview-domain.com)
(N26)



ATTENZIONE

Vishing

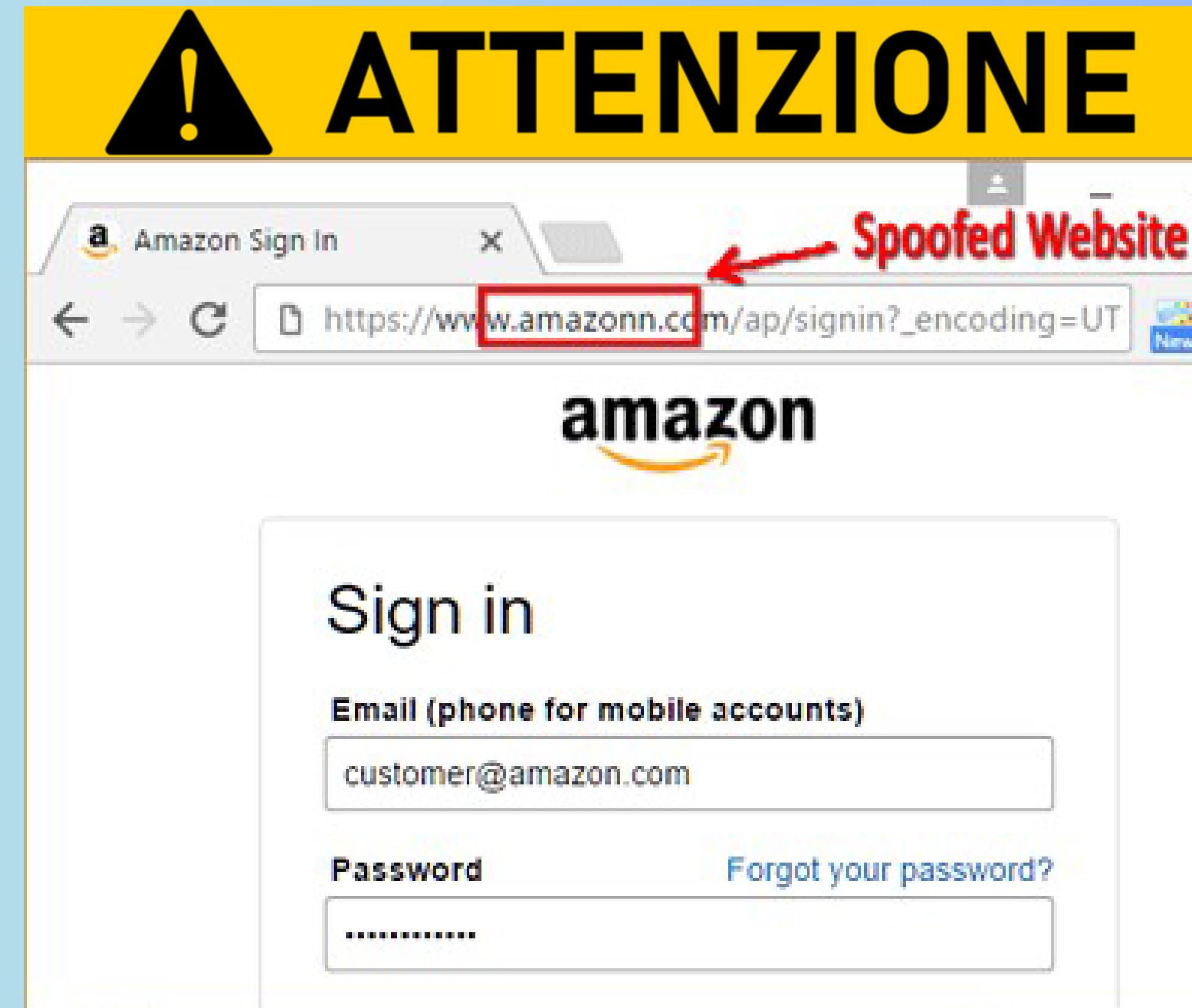
Anche detto “voice phishing”, perché la vittima viene contattata attraverso una **telefonata** oppure un **messaggio vocale**. In questo caso, riceverai una telefonata in cui ti si chiede di intervenire subito perché qualcuno ha cercato di accedere al tuo conto corrente, oppure di aderire a un’offerta speciale, fornendo i tuoi dati.



Come ci si difende dal phishing?

Ecco a cosa bisogna stare attenti:

1. Indirizzo email e logo. Prima di tutto, fai attenzione all'indirizzo email da cui è stata spedita: anche se sono presenti loghi ufficiali, verifica che sia stata spedita da un indirizzo ufficiale. Se noti che l'indirizzo da cui proviene l'email è sconosciuto, oppure sospetto, cestinala subito.



Come ci si difende dal phishing?

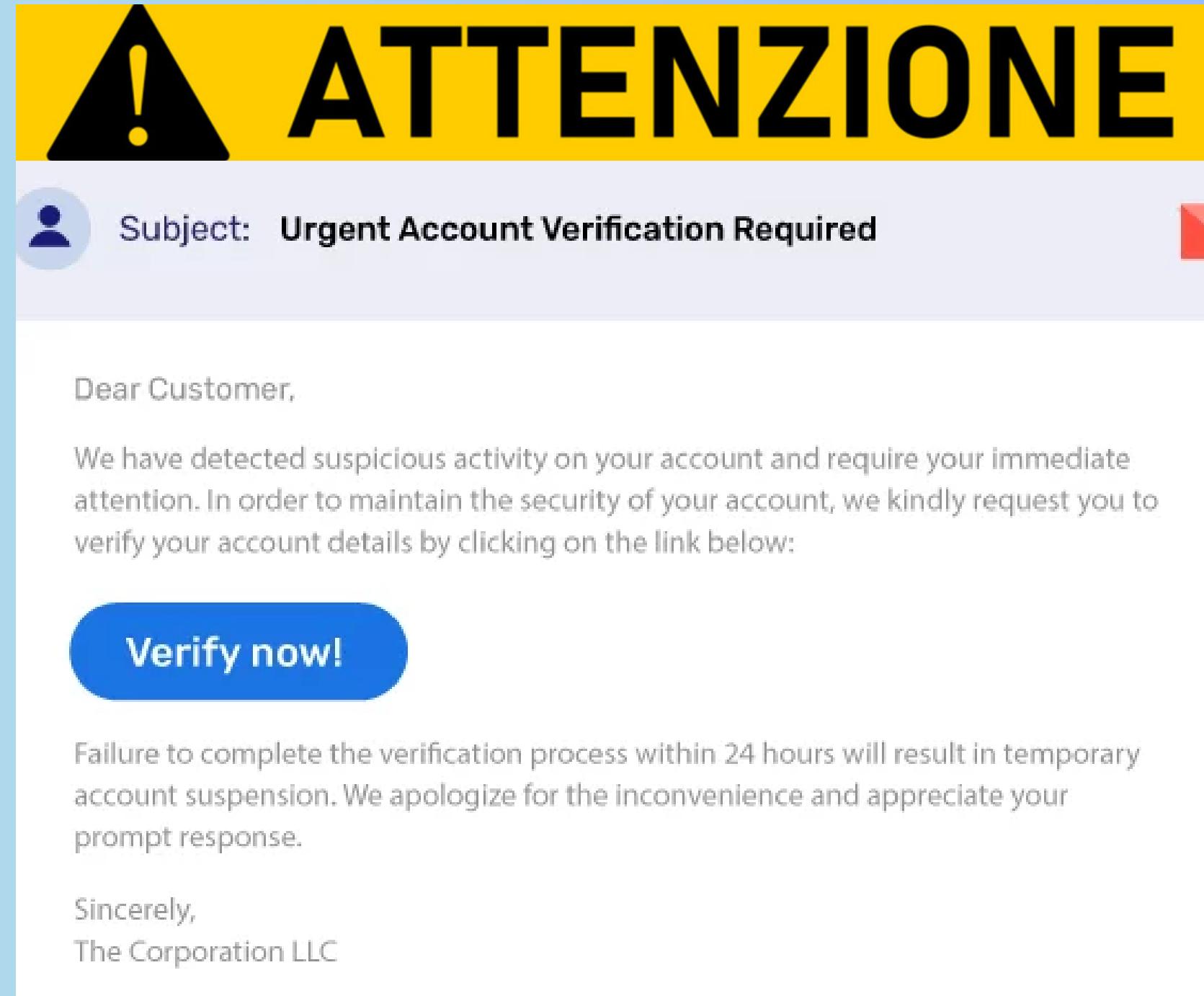
2. **Errori di ortografia.** Leggi bene il testo del messaggio, le email di phishing spesso contengono errori di ortografia oppure sono scritte con una grammatica scadente.



Come ci si difende dal phishing?

3. Oggetto della mail. Se l'oggetto della email ti indica la comunicazione come urgente, e la comunicazione arriva in modo inaspettato, potrebbe trattarsi di una minaccia informatica.

4. Allegati e link. Quando ricevi una email che ti chiede con insistenza di aprire un allegato o fare clic su un link e inserire le tue credenziali, fai molta attenzione. Le comunicazioni ufficiali da enti o aziende difficilmente ti chiederanno con tanta leggerezza di inserire i tuoi dati.



Come ci si difende dal phishing?

Misure di prevenzione:

1. Autenticazione

Multifattore (MFA).

L'implementazione di MFA può aggiungere uno strato di sicurezza, anche se le credenziali vengono compromesse.



Protected PIN



Bluetooth*



Phone Proximity



Fingerprint

Logical Location



Facial Recognition



Come ci si difende dal phishing?

2. Uso di Filtri Anti-Phishing. L'utilizzo di filtri anti-phishing può aiutare a bloccare e-mail sospette prima che raggiungano le caselle di posta degli utenti.



Come ci si difende dal phishing?

In particolare è consigliato l'uso di filtri **SPF, DKIM, DMARC**

- SPF (Sender Policy Framework);
 - DKIM (DomainKeys Identified Mail);
 - DMARC (Domain-based Message Authentication, Reporting, and Conformance).
- Essi sono standard di autenticazione e sicurezza utilizzati per mitigare il rischio di spam, phishing e spoofing nelle comunicazioni via email. Ogni standard svolge un ruolo specifico nel rafforzare l'autenticazione delle email e nel proteggere i destinatari da potenziali minacce.

RECOMMENDED
SPF, DKIM,
DMARK

Cosa fare se hai cliccato sul link di phishing? Non disperare!

Può capitare a tutti di non riconoscere per tempo un'email sospetta e non riuscire a difendersi dal phishing. In questi casi, però, non devi disperare ma passare all'azione! Il primo consiglio è quello di **cambiare subito la password** dei propri account, che potrebbero essere stati compromessi. Se i dati condivisi coi cybercriminali riguardano il proprio conto corrente bancario o le carte di credito, dovrai rivolgerti alla tua **banca**, verificare che non ci siano spese sospette e chiedere il blocco delle transazioni non autorizzate.

Infine, puoi denunciare l'accaduto alla **Polizia Postale**, che attraverso un sistema di segnalazioni online ti permette di indicare il sito che è stato contraffatto e su cui hai inserito i tuoi dati, e denunciare l'attacco di phishing subito.



Esempio di phishing controllato

Il direttore di Epicodesecurity mi ha dato il permesso di creare un phishing controllato, con l'obiettivo di ingannare le persone nel miglior modo possibile e vedere se sono vulnerabili a potenziali attacchi.

Ho deciso di prendere come obiettivo della mia scam email il Manager del Dipartimento di Sicurezza, per puntare ai suoi privilegi di accesso alle informazioni riservate dell'azienda. Tipico esempio di Whaling!

La prima cosa che faccio è cercare informazioni su questa persona: conosco il suo nome e il suo cognome, posso cercarla sui social media? Assolutamente sì. In questo modo posso facilmente reperire informazioni sui suoi interessi, sul suo stile di vita, ecc.

Kyle Meyer

Friends Message Call

Timeline About Friends 19 Mutual Photos 47 More

About

Product Designer at Facebook.
Facebook, Big Cartel and Clickworker, Active Media Systems

Studied Interactive Media Design at The Art Institute International Minnesota
West De Pere High School

Lives in San Francisco, California
From West De Pere, Wisconsin

Followed by 3,627 people

Friends 442 (19 Mutual)

Mike Murphy, Jason Fatinus and 7 others like this.

Like Comment Share

Jay Bumbers I even sent some emails on my phone from the chairlift. 22 hours ago - Like · 42

Adam Michael nice shot! I can confirm that I see work-related chair lifts / comments. Now, back to the slopes. 20 hours ago via mobile - Like · 41

Write a comment...

Vi presento il Manager del Dipartimento di Sicurezza, Kyle Meyer!

Dal suo profilo riesco a capire che è una persona avventurosa, che ama le escursioni e gli sport di montagna.

Posso utilizzare in qualche modo questa informazione per i miei scopi?
Assolutamente sì!

Da: trivagoo@gmail.com

A: KyleMeyer@episecurity.it

Gentile Kyle Meyer,
Congratulazioni! Sei stato scelto come vincitore di un soggiorno nello Chalet Super Deluxe Magie d'Inverno in Trentino Alto Adige!



Il tuo pacchetto comprende visite guidate sulle bellissime montagne nei pressi dello chalet, spa e sauna presso il centro benessere [SentirsiMeglio](#) del paese vicino, colazione a letto e cena offerta nei migliori ristoranti dei dintorni!

Ma affrettati! L'offerta scade alle [23:59](#) di oggi! Per confermare la tua presenza, accedi a questo link www.trivagoo/chalet-magie-inverno-deluxe.it e immetti le seguenti credenziali: documento d'identità, codice fiscale, dati della carta di credito.

Non preoccuparti, il soggiorno è gratuito! I dati verranno usati solo in caso di danni dolosi alla proprietà e saranno cancellati una volta terminato il soggiorno!

Affrettati! Il Trentino ti aspetta!

Cordialmente
Trivago s.p.a.

Il povero Signor Meyer ha appena ricevuto una email scam che simula una comunicazione dell'agenzia di viaggi Trivago, che a quanto pare gli ha offerto un soggiorno gratuito in un bellissimo chalet di montagna.

Kyle, essendo un cliente abituale di Trivago, non si chiede se l'email sia vera o falsa, non fa i controlli dovuti e clicca sul link, immettendo tutti i suoi dati personali. Non appena lo fa, i dati della sua carta di credito entrano in mio possesso.

Ma non è finita qua per il povero Kyle! Il mio link conteneva anche un Trojan Horse, un tipo di malware che mi permette di prendere possesso del dispositivo della vittima. Questo vuol dire... che ho accesso al computer aziendale di Kyle, con tutte le informazioni sensibili sul suo dipartimento!

Il direttore non sarà contento del suo manager, ma per fortuna era solo un attacco simulato!

**Grazie per l'attenzione e
attenti al phishing!**