

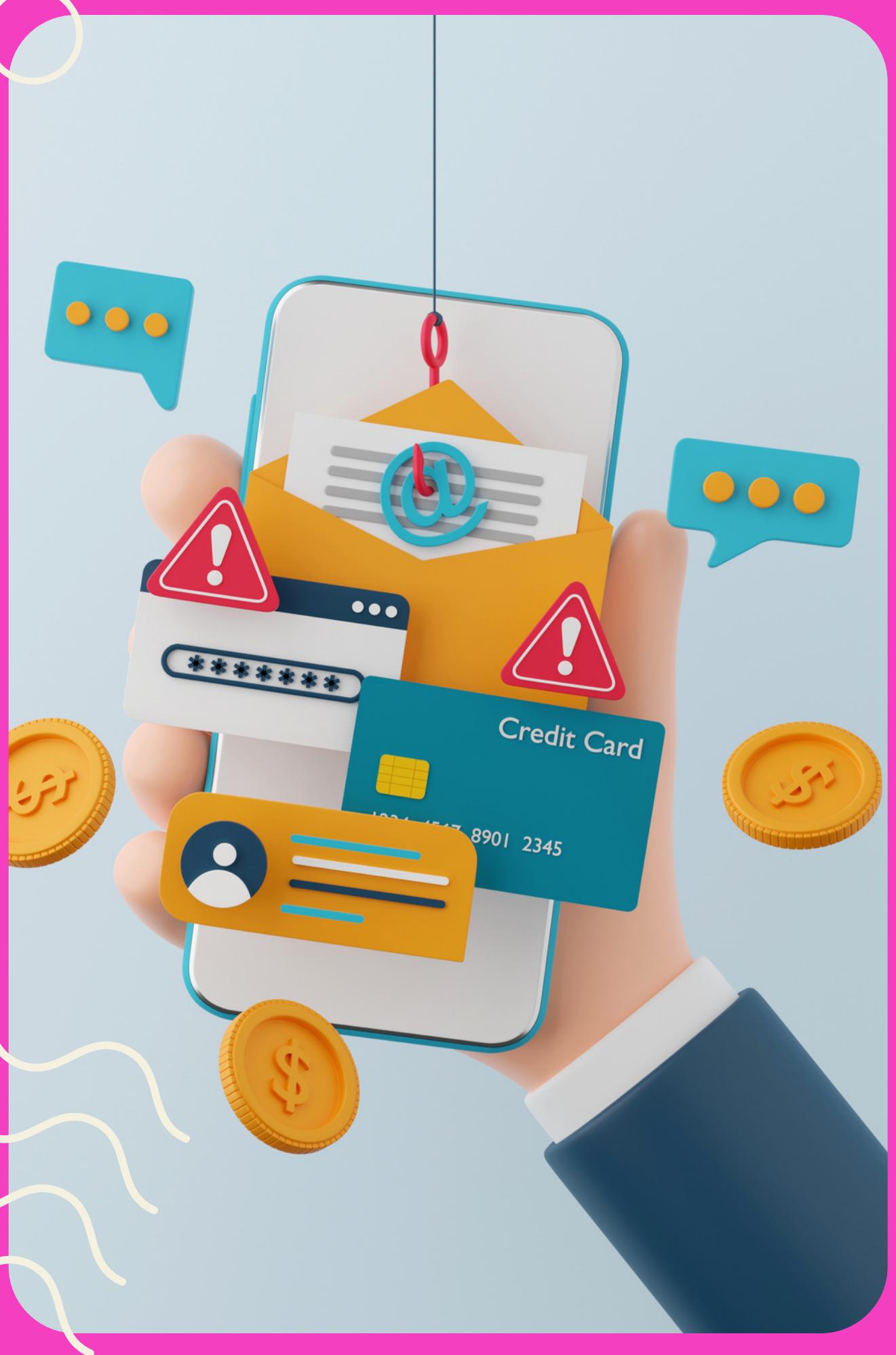


INGEGNERIA

SOCIALE

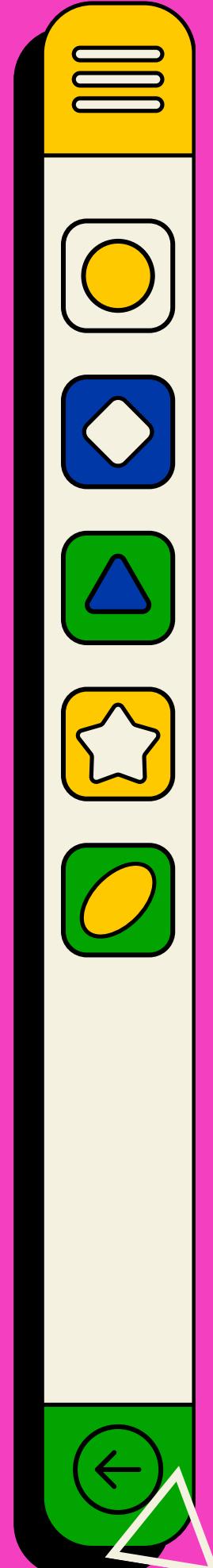
PER TUTTI

by MATTIA PASTORELLI



Indice giornata

- 1 Introduzione Ingegneria Sociale
- 2 Cos'è il Phishing e Rischi Associati
- 3 Come riconoscere il Phishing (indicatori)
- 4 Esercitazioni pratiche e Simulazioni
- 5 Feedback e Miglioramenti
- 6 Politiche di Sicurezza Aziendale e Azioni Consigliate
- 7 Domande e risposte, Conclusioni





Introduzione

La sicurezza informatica è il complesso di pratiche, tecnologie e comportamenti progettati per proteggere i dati, i sistemi e le reti informatiche da accessi non autorizzati, danni o furti.



Proteggere le informazioni è cruciale nell'era digitale



Nell'era digitale, dove la nostra vita quotidiana è sempre più interconnessa e dipendente dalla tecnologia, proteggere le informazioni è cruciale per diversi motivi. Le informazioni personali e aziendali sono diventate risorse preziose e, di conseguenza, sono diventate un obiettivo primario per i criminali informatici.



Ingegneria Sociale

L'ingegneria sociale è una forma di manipolazione psicologica in cui gli attaccanti cercano di ottenere informazioni sensibili o indurre le persone a compiere determinate azioni attraverso l'inganno, la manipolazione e l'uso delle relazioni umane.

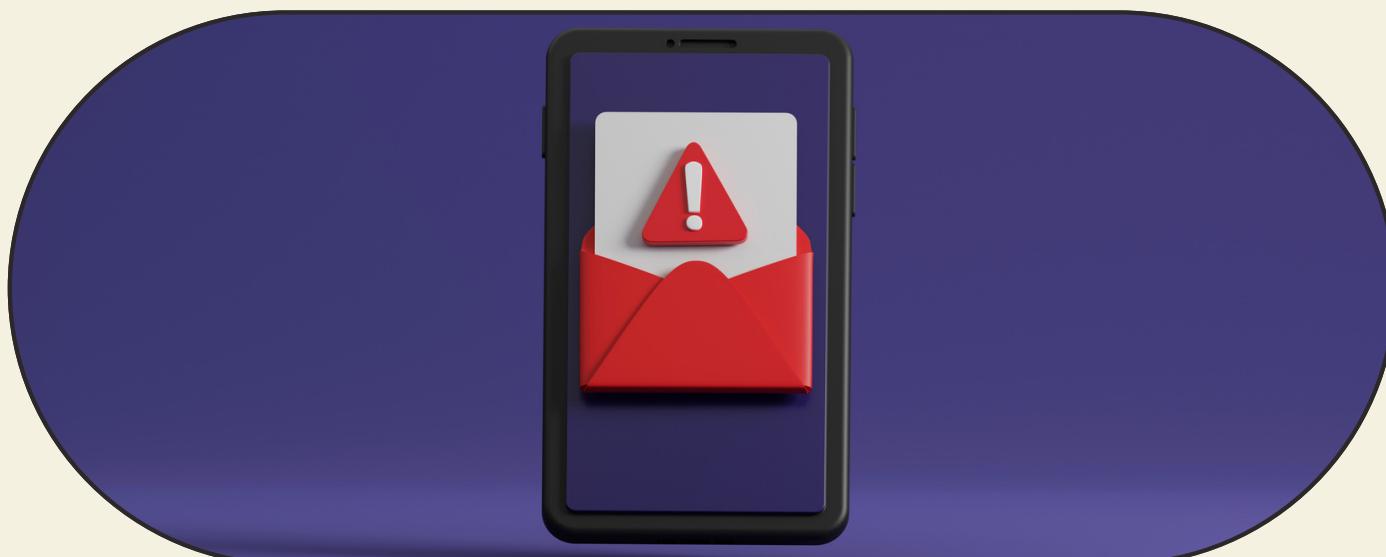
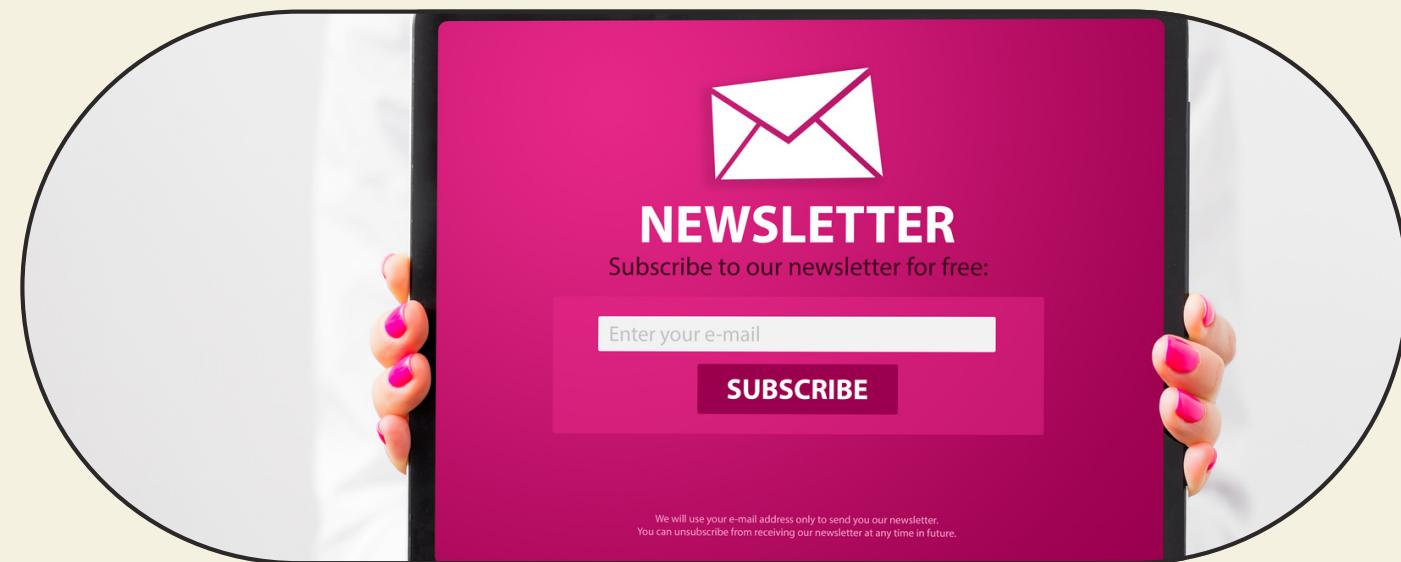




Tipologie di attacchi

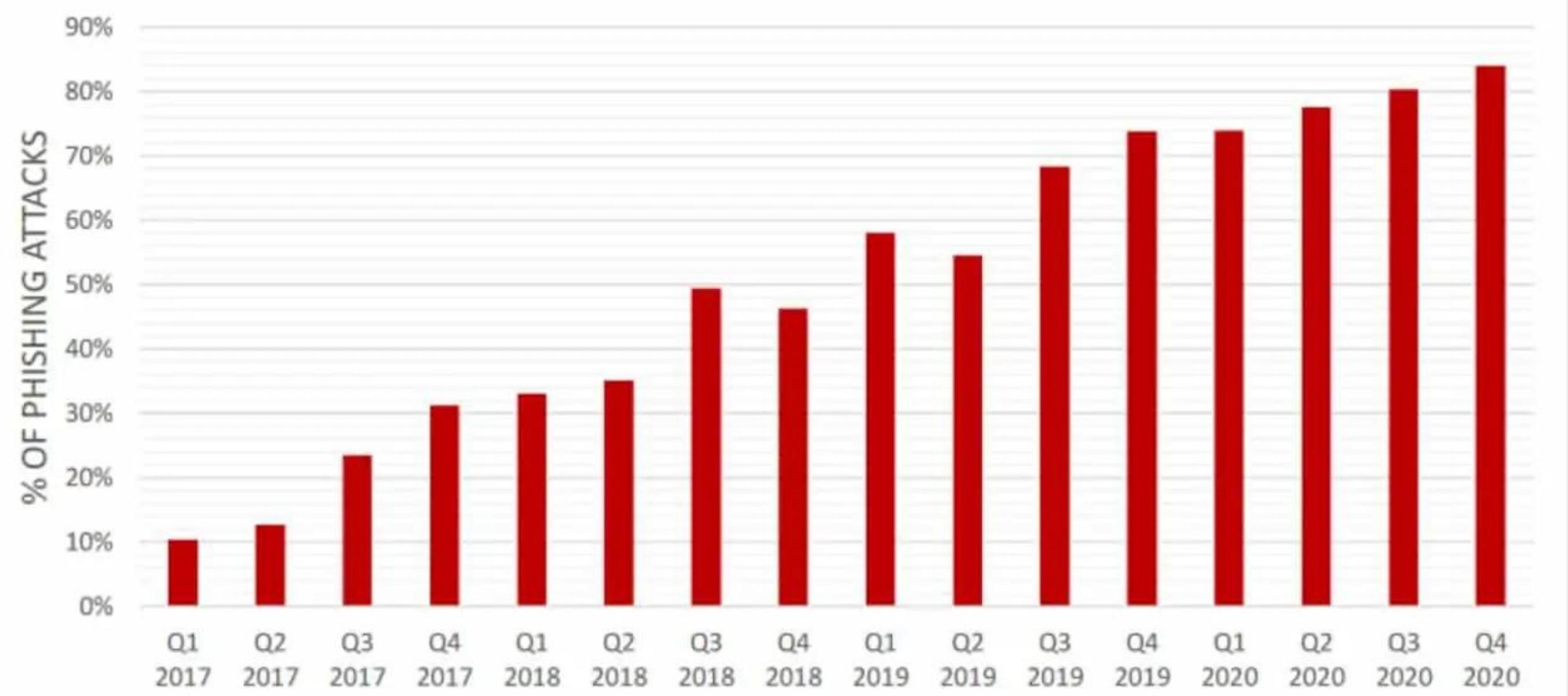
PHISHING:

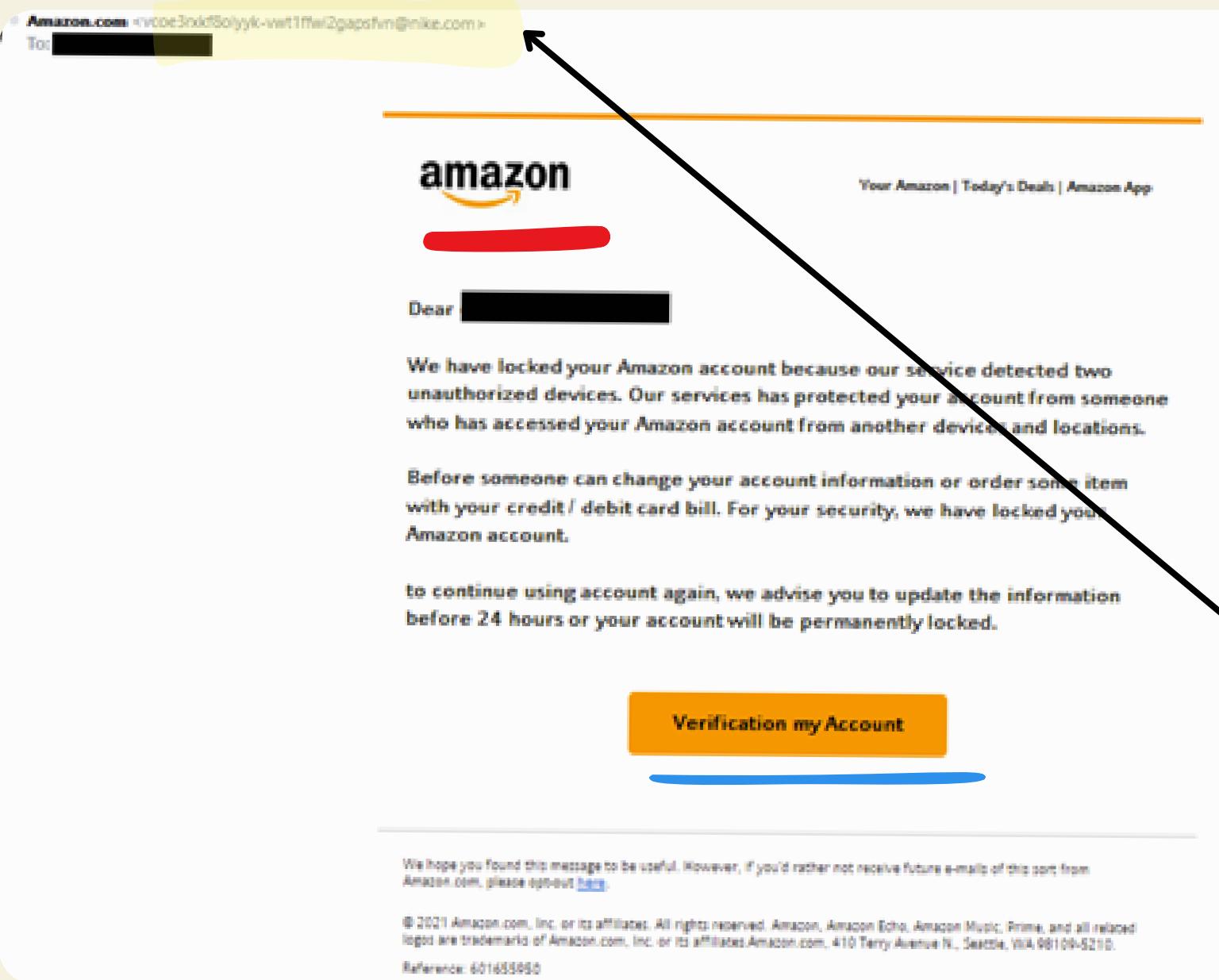
Il phishing è una forma di truffa online in cui i truffatori cercano di ingannare le persone facendosi passare per entità affidabili al fine di ottenere informazioni personali. Ciò avviene attraverso l'invio di e-mail che sembrano provenire da fonti legittime, come banche o servizi online, con l'obiettivo di indurre le vittime a rivelare informazioni sensibili.



SMISHING: Lo smishing è una forma di phishing che avviene attraverso messaggi di testo (SMS). Gli attaccanti inviano messaggi che sembrano provenire da fonti attendibili, cercando di indurre le persone a fornire informazioni personali o cliccare su link malevoli.

Phishing in aumento





Esempio di Phishing

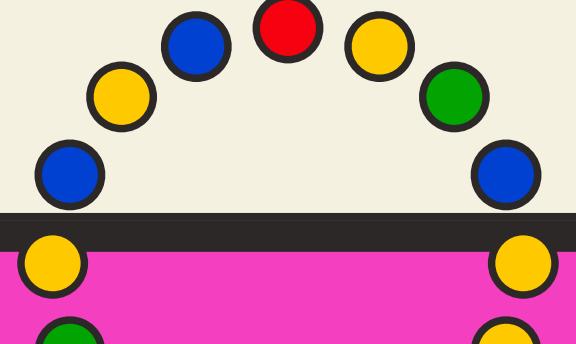
Nell'immagine possiamo notare un'e-mail da parte di Amazon, nella quale ci viene detto che il nostro account è stato bloccato a causa di un conflitto di 2 dispositivi non autorizzati. Ci viene richiesto di verificare la nostra identità, premendo sul tasto arancione presente in immagine.

- A prima vista può sembrare tutto lecito, ma guardiamo attentamente l'email di provenienza del messaggio (evidenziato in giallo). Possiamo notare che c'è qualcosa di errato, dato che ci aspetteremo un email del tipo: **amazon.services@amazon.com**

Possibili danni del Phishing

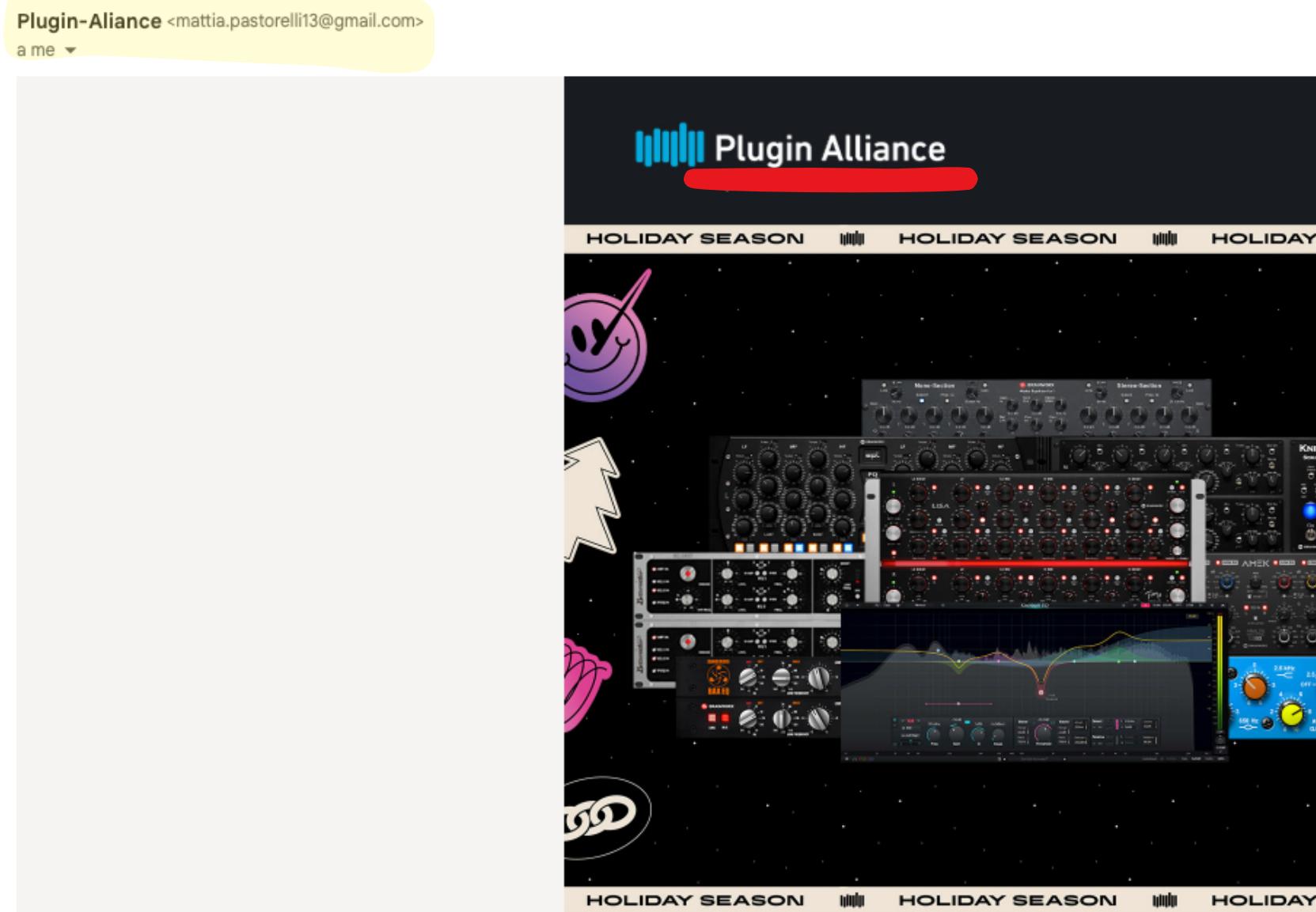
Esistono molteplici danni se si cade in un attacco di questo tipo:

- Furto delle credenziali
- Accesso non autorizzato
- Furto identità
- Perdita finanziaria
- Danni alla Reputazione
- Danni all'Azienda
- Distribuzione di Malware
- Violazione della Privacy





Come riconoscere un attacco Phishing?



Vediamo un esempio di un'altra e-mail poco attendibile. Questa volta l'email è da parte di un sito web che fornisce servizi per la produzione musicale. Cosa bisogna guardare per riconoscere se l'e-mail è attendibile o meno?

- Per prima cosa NON bisogna guardare il contenuto dell'e-mail, in quanto è facilmente replicabile
- Seconda cosa: Guardare l'email di provenienza. Si può notare che il nome prima dell'email e la stessa sono completamente diversi. (evidenziato in giallo). Soprattutto si può notare che "Plugin Aliance" è scritto solamente con una "L", a differenza della scritta sottolineata in rosso.
- Sono le prime cose che possono dare una rapida attendibilità o meno.



Come riconoscere un attacco Phishing?

ID messaggio	<1702646957041750800.17200.3287070085996620190@LAPTOP-M3JSPV3P>
Creato alle:	15 dicembre 2023 alle ore 14:29 (consegnato dopo 0 secondi)
Da:	Plugin-Alliance <mattia.pastorelli13@gmail.com> Tramite gophish
A:	Mattia Pastorelli <mattia.pastorelli13@gmail.com>
Oggetto:	Save up to 88% on premium EQs

Phishing

ID messaggio	<0B.6B.39017.E6A1B756@gv.mta3vrest.cc.prd.sparkpost>
Creato alle:	14 dicembre 2023 alle ore 16:08 (consegnato dopo 1 secondo)
Da:	Plugin Alliance <newsletter@news.plugin-alliance.com>
A:	mattia.pastorelli13@gmail.com
Oggetto:	Save up to 88% on premium EQs
SPF:	PASS con l'IP 137.22.229.218 Ulteriori informazioni
DKIM:	'PASS' con il dominio news.plugin-alliance.com Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

Reale

C’è un terzo modo, per poter aver un riscontro immediato di attendibilità o meno di un e-mail.

Premendo sui pallini sul lato email e andando su “Mostra Originale”, ci apparirà quest’immagine. Dalle due possiamo notare la differenza totale nell’e-mail del mittente, ma soprattutto la mancanza delle voci “SPF,DKIM,DMARC” nell'email phishing.



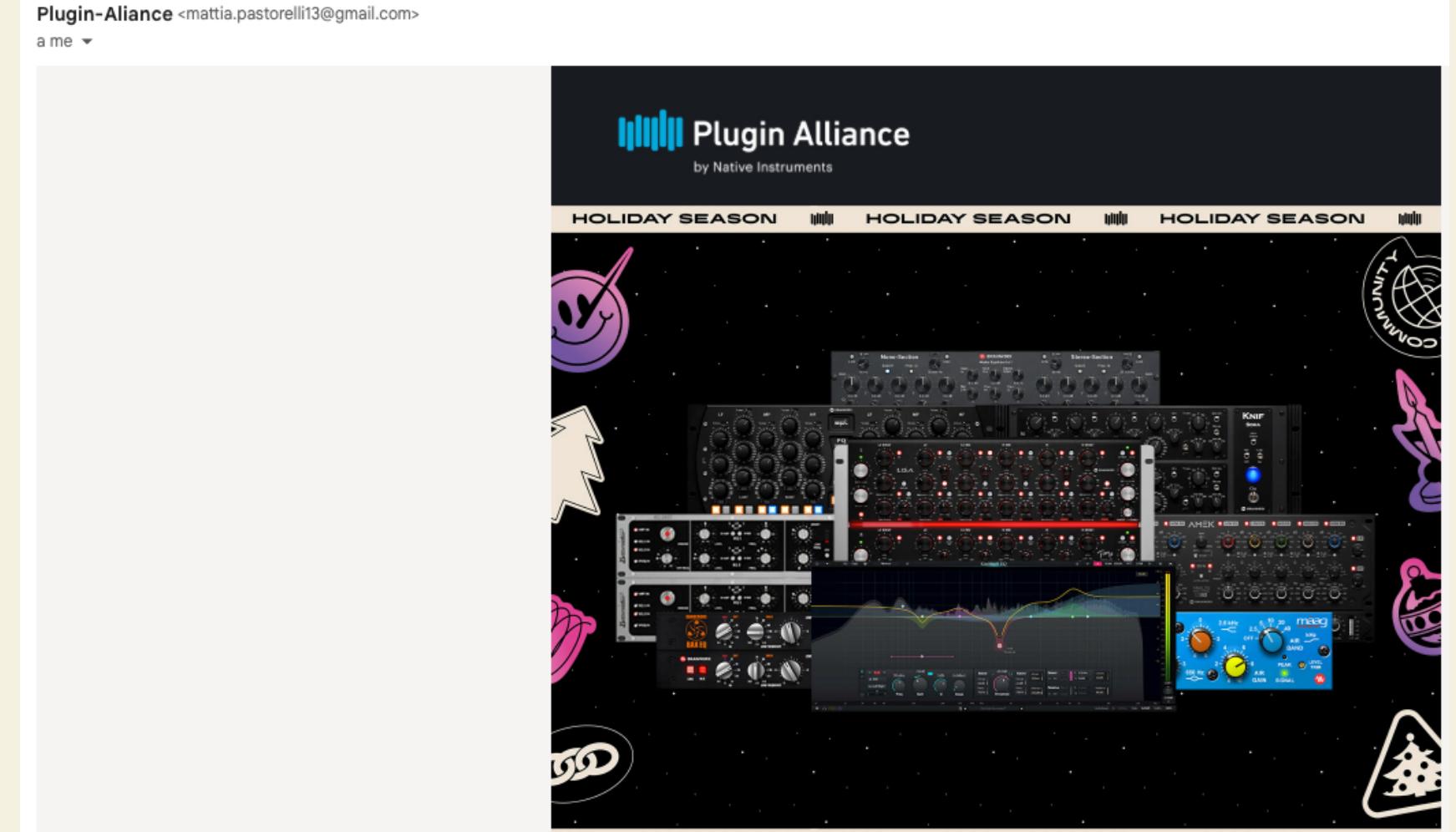
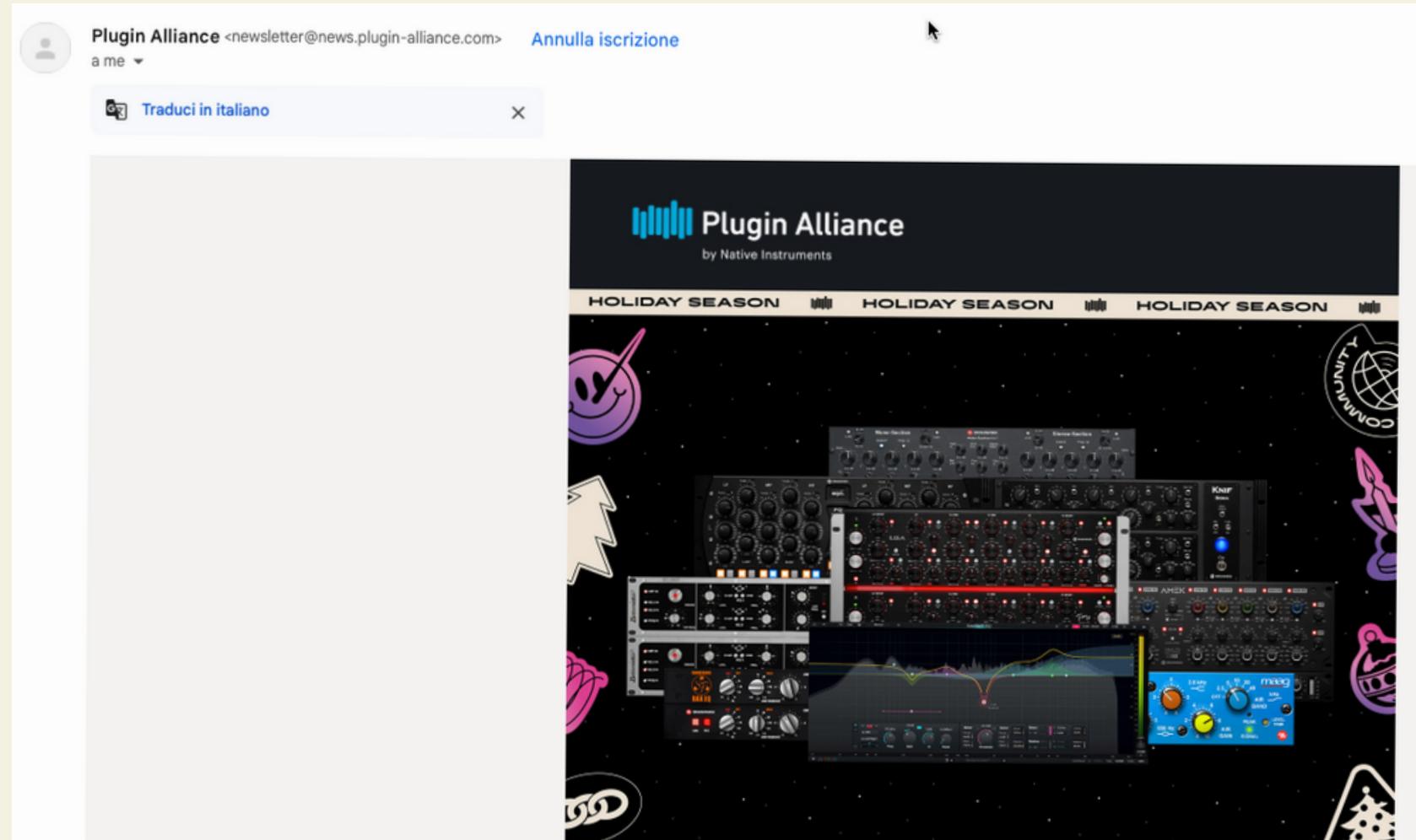
SPF, DKIM, DMARC

ID messaggio	<0B.6B.39017.E6A1B756@gv.mta3vrest.cc.prd.sparkpost>
Creato alle:	14 dicembre 2023 alle ore 16:08 (consegnato dopo 1 secondo)
Da:	Plugin Alliance <newsletter@news.plugin-alliance.com>
A:	mattia.pastorelli13@gmail.com
Oggetto:	Save up to 88% on premium EQs
SPF:	PASS con l'IP 137.22.229.218 Ulteriori informazioni
DKIM:	'PASS' con il dominio news.plugin-alliance.com Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

- **SPF:** è una tecnologia di autenticazione email che verifica che il server di invio di un'email sia autorizzato a inviare messaggi a nome di un determinato dominio.
- **DKIM:** è un sistema di autenticazione email che consente di verificare l'integrità e l'autenticità del messaggio, garantendo che non sia stato alterato durante il trasporto.
- **DMARC:** è un protocollo che unifica SPF e DKIM, fornendo un meccanismo per consentire ai proprietari di domini di dichiarare le proprie pratiche di autenticazione email
- Ogni voce è viene accompagnata da una parola “**PASS**”, ciò vuol dire che tutti i passaggi sono stati correttamente eseguiti ed il contenuto dell'email non è stato variato in corso di spedizione.



Riuscite a vedere le differenze?





Simulazione di Phishing Controllato

opo S.p.A <info@kosqvery.com> ★
aggiornamento obbligatorio
★

 **INTESA**  **SANPAOLO**

Gentile Cliente,

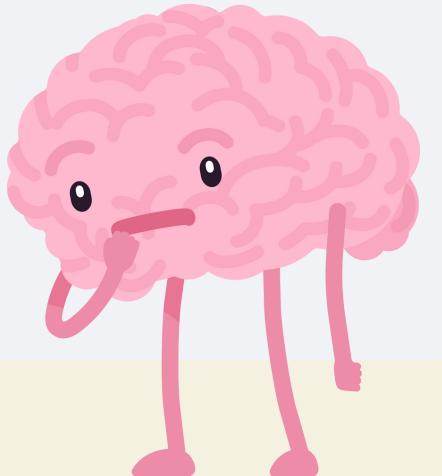
Mastercard Identity Check™ è il nuovo servizio gratuito che rende i tuoi pagamenti online più smart. Ogni volta che confermi un acquisto online, la tua identità è verificata in automatico e in tempo reale per essere sicuri che sia veramente tu a effettuare il pagamento. Solo se necessario, ti sarà richiesto di confermare il pagamento con il metodo di autenticazione adottato dalla tua banca come impronta digitale, riconoscimento facciale o SMS OTP (One Time Password).

Registrati ora in pochi passaggi alle nuove procedure di sicurezza Visa Secure e Mastercard® Identity Check™

Partita IVA IT11991500015

CLICCA QUI E ACCEDI ALLA TUA BANCA ONLINE

Copyright 2022, Intesa Sanpaolo. Tutti i diritti riservati.



Nelle scorse settimane, dopo il consenso dell'amministratore delegato, siete stati sottoposti ad una simulazione di Phishing Controllato durante l'orario lavorativo.

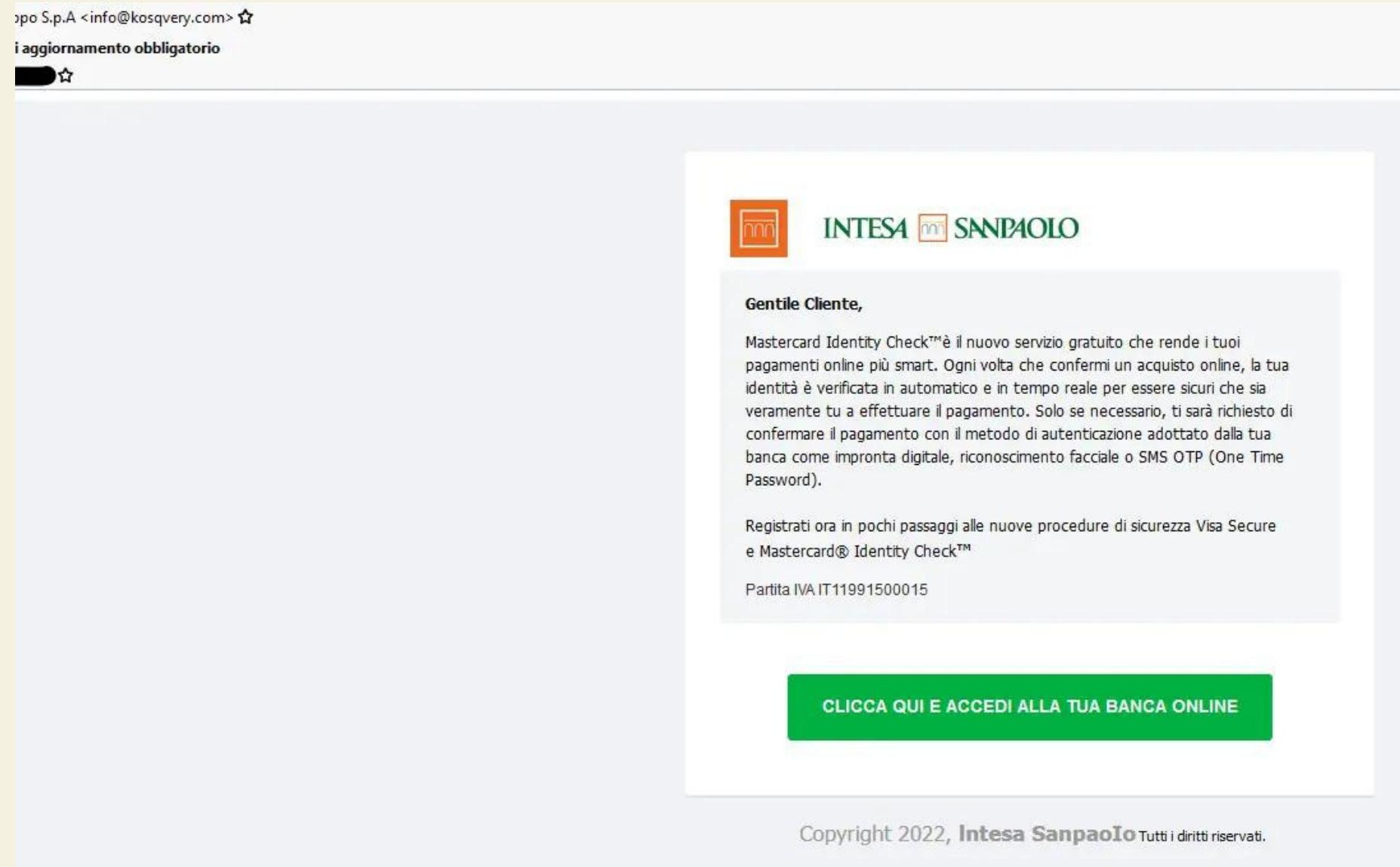
Ricordate quest'email?

Notato niente di strano?

Usate i concetti appresi prima per trovare cosa rende questo messaggio



Simulazione di Phishing Controllato

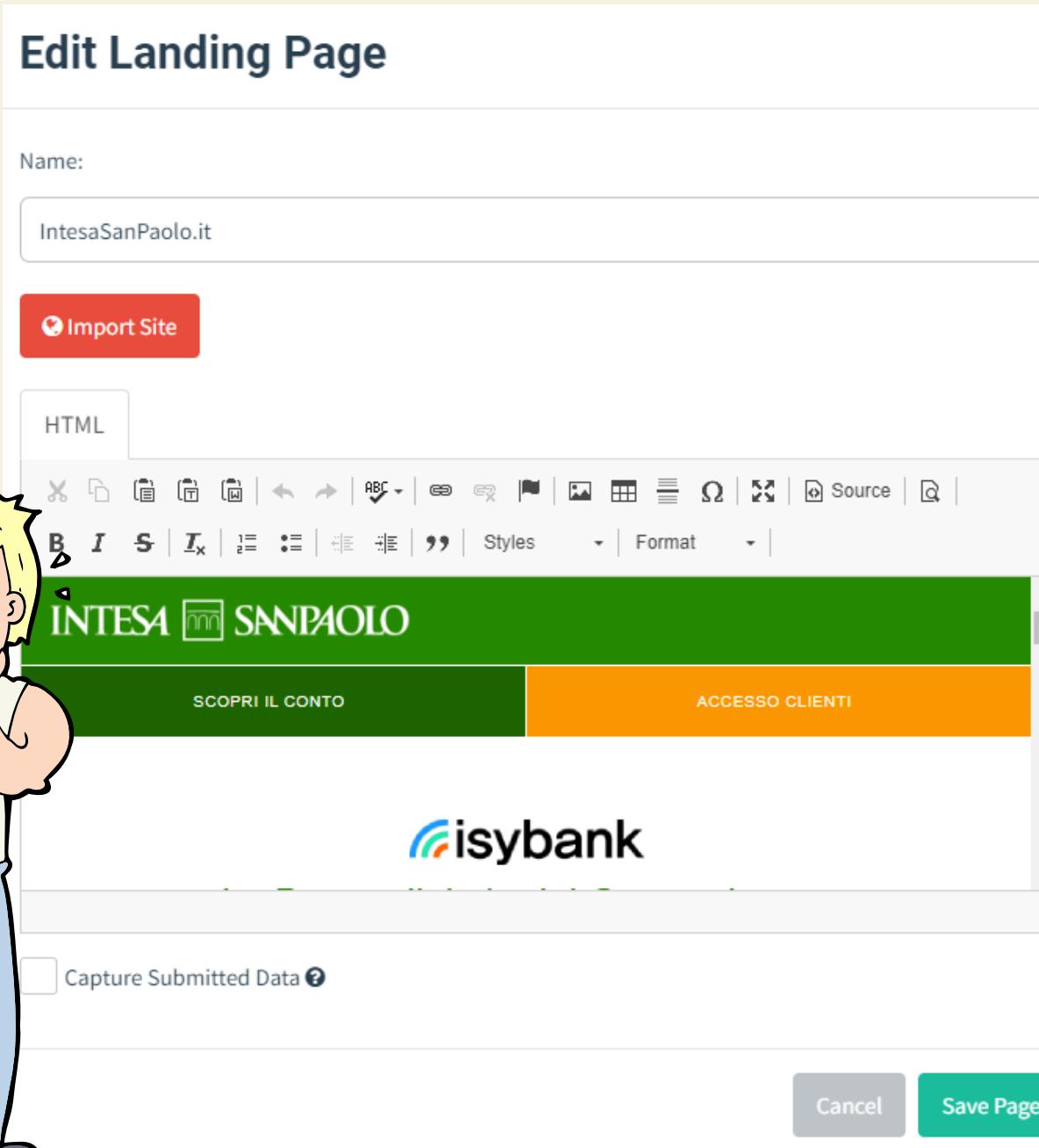


Quest'esperimento è stato effettuato per puro scopo statistico prima di questa formazione.

Al termine di tale test, è emerso che il 50% di voi è cascato in quest'inganno, però niente PAURA, è stato svolto tutto in un ambiente sicuro!
Ciò è stato dato dalla mancanza di esperienza e dalla varietà di età presente in azienda.



Simulazione di Phishing Controllato



Com'è stato possibile?!

Abbiamo utilizzato un programma chiamato GoPhishing. Il quale ha la funzionalità di immettere una campagna di phishing in un ambiente totalmente sicuro.

Con questo programma possiamo andare ad emulare perfettamente un'email da parte di un particolare ente/persona. (come in figura). Dopodiché abbiamo inserito quest'email nel server di EpicodeSecurity, il quale ha smistato ad ognuno di voi il contenuto di tale messaggio

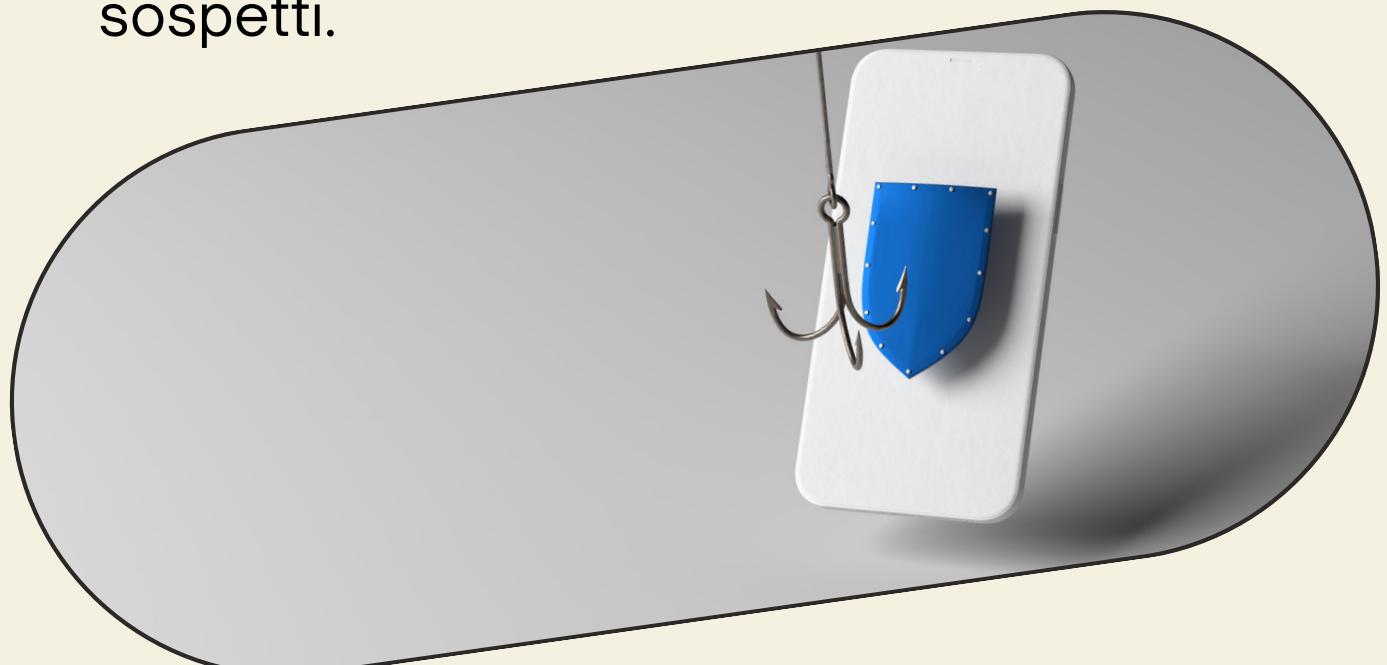
Come difendersi dal Phishing?

1. Verifica dell'Indirizzo Email:

- Verifica SEMPRE attentamente l'indirizzo email del mittente. Gli attaccanti spesso utilizzano indirizzi simili a quelli ufficiali, ma con piccole variazioni.

2. Attenzione agli URL:

- Prima di cliccare su link in email o messaggi, passa il cursore sopra di essi per vedere l'URL reale. Evita di inserire informazioni personali su siti web sospetti.



• Autenticazione a Due Fattori (2FA):

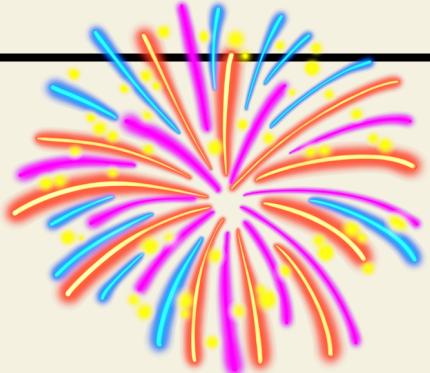
- Abilita l'autenticazione a due fattori quando possibile. Aggiunge un livello extra di sicurezza richiedendo un secondo passo di verifica oltre alla password.

• Formazione sulla Consapevolezza:

- Partecipa a programmi di formazione sulla sicurezza informatica per riconoscere segnali di phishing. Mantieni una consapevolezza costante e segnala immediatamente eventuali sospetti.



Conclusioni



Vi ringraziamo per l'attenzione!

Nelle prossime settimane/mesi, chi lo sa, verranno effettuati altri test di phishing per valutare la vostra conoscenza in materia.

Ricordate, l'arma più potente per arginare tali attacchi è la consapevolezza!



GO EPICODE



Seguendo questi suggerimenti sulla sicurezza digitale, puoi contribuire a proteggere te stesso e le tue informazioni personali online.
Stay safe!