

## **-1 Il vostro ruolo è quello di spiegare e informare i dipendenti dell'azienda Epicodesecurity sui rischi di attacchi di ingegneria sociale, in particolar modo contro il phishing.**

Gli attacchi di ingegneria sociale possono portare a gravi conseguenze, come il furto di dati sensibili, danni finanziari, perdita di reputazione aziendale e violazioni della privacy.

L'ingegneria sociale è una tecnica utilizzata dagli hacker per manipolare le persone al fine di ottenere informazioni riservate o accesso non autorizzato a sistemi informatici.

Perché è pericolosa?

- fiducia e autorità: gli attaccanti sfruttano la tendenza dell'uomo a fidarsi di autorità o persone visibilmente affidabili, creando situazioni che sembrano legittime.
- difficoltà nella difesa tecnologica: si ha difficoltà a difendersi contro tali attacchi perché l'ingegneria sociale si basa sulla manipolazione del personale e non su quanto il sistema di sicurezza è avanzato
- scarsa consapevolezza: molte persone non sono consapevoli delle tecniche usate nell'ingegneria sociale

Tra le varie tecniche di ingegneria sociale abbiamo il phishing, tra i più diffusi e pericolosi.

Il phishing serve per rubare informazioni personali, passando per qualcosa di affidabile (che può essere un messaggio o un email) contenente di solito link di login oppure file da scaricare.

## **-2 Come impostate la formazione? (spiegare cos'è il phishing ).**

1) Gli obiettivi principali sono:

- spiegare i concetti fondamentali e i rischi dell'ingegneria sociale
- sensibilizzare i dipendenti sull'importanza della sicurezza informatica e sulla protezione dei dati aziendali
- fornire tecniche e strumenti per riconoscere e prevenire le varie tattiche di attacco di ingegneria sociale

2) Contenuti della formazione:

- definizioni, tipologie di attacchi e obiettivi degli hacker
- esempi pratici di attacchi utilizzando scenari realistici
- pratica sulle comunicazioni online, che sarebbe l'utilizzo di siti web, email e social media

3) Verifica e monitora l'apprendimento:

- Verifica l'apprendimento attraverso test e domande.
- Raccolta di feedback per migliorare e aggiornare la formazione.

## **-3 Cosa devono vedere, in particolar modo, i dipendenti per non cadere nel phishing?( quali parametri vedere per identificarlo.Esempio: SPF).**

Il phishing è una tattica usata per truffare online, dove i criminali informatici cercano di rubare le informazioni personali fingendosi autorità legittime, che possono essere per esempio la propria banca o un social media che usiamo. L'attacco phishing è basato sul chiedere all'utente di effettuare l'accesso o di verificare le informazioni personali, quindi rilevando le proprie informazioni private dato che le andremo ad inserire su link fittizi, che sembrano quelli originali ma sono stati invece usati dai criminali informatici.

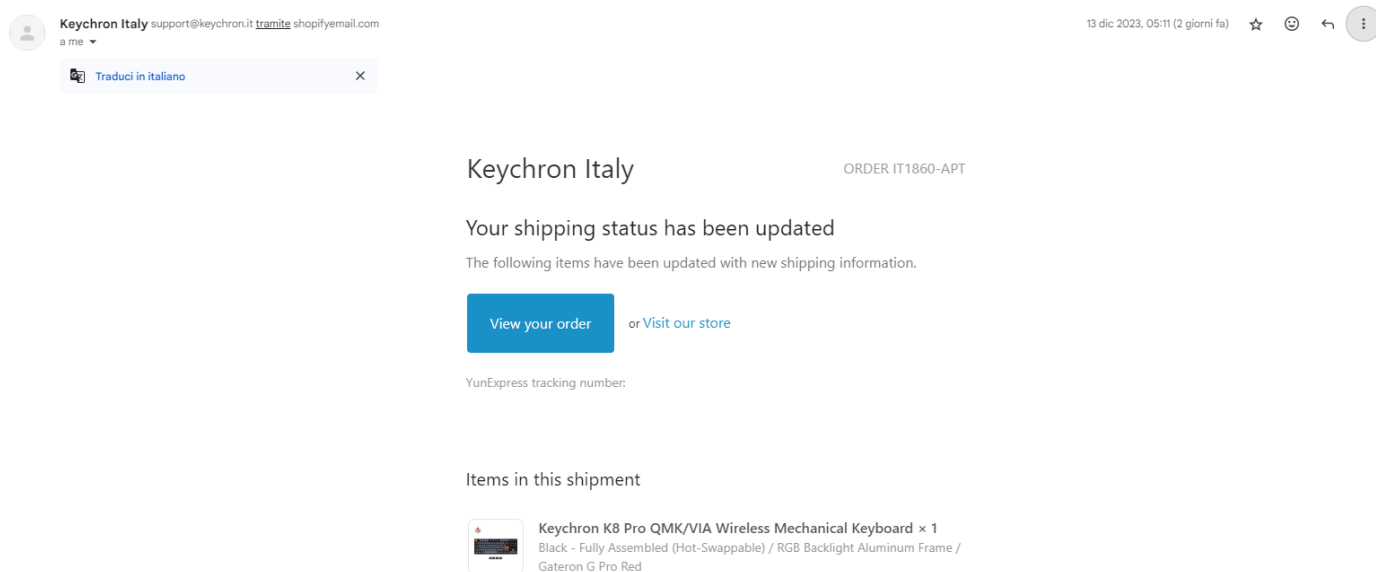
Abbiamo diversi standard di autenticazione per verificare se si tratta di phishing, essi sono:

- SPF(Sender Policy Framework): verifica che l'indirizzo ip sia autorizzato per conto del dominio specificato.
- DKIM(DomainKeys Identified Mail): garantisce l'integrità e l'autenticità del contenuto di email grazie alla firma digitale.
- DMARC (Domain-based Message Authentication, Reporting and Conformance): unisce SPF e DKIM, se le email non superano le autenticazioni consente di specificare le azioni da intraprendere che sono per esempio contrassegnate come spam o rifiutate.

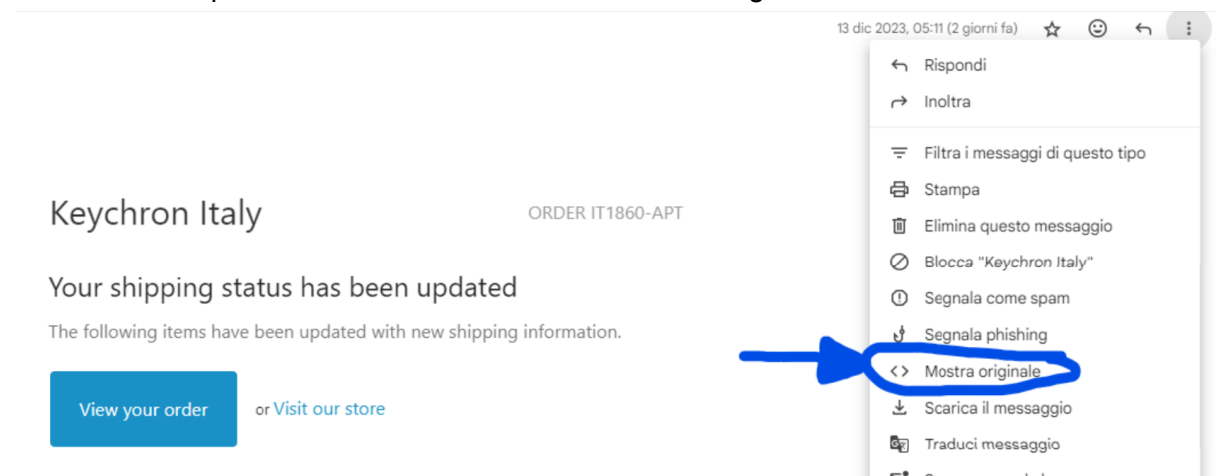
Esempio di email phishing:

I parametri da vedere per identificare il phishing sono diversi, per esempio su gmail dobbiamo seguire i seguenti passaggi:

Apriamo un email



Cliccare sulle opzioni dell'email e cliccare "< > Mostra originale"



Ci aprirà una schermata e per prima cosa andremo a leggere queste informazioni

## Messaggio originale

ID messaggio	<E1030004-17A048CF610A88C2-A32AF9BC@shopify.com>
Creato alle:	13 dicembre 2023 alle ore 05:11 (consegnato dopo 0 secondi)
Da:	Keychron Italy <support@keychron.it>
A:	d80281439@gmail.com
Oggetto:	Shipping update for order IT1860-APT
SPF:	PASS con l'IP 149.72.90.155 <a href="#">Ulteriori informazioni</a>
DKIM:	'PASS' con il dominio shopifyemail.com <a href="#">Ulteriori informazioni</a>

Dobbiamo controllare che su SPF, DKIM e DMARC ci sia scritto 'PASS' e non 'FAIL', questi standard di autenticazione ci dicono se l'email passa o no la verifica, quindi in questo caso l'email passa l'autenticazione.

Se scendiamo un poco più in giù troveremo scritto tutto il codice dell'email e troveremo in questo punto preciso l'email del mittente e l'indirizzo ip del percorso che fa l'email.

```
dkim=pass header.i=@shopifyemail.com header.s=s1 header.b=jjVLgc4l;  
dkim=pass header.i=@sendgrid.info header.s=smtapi header.b=KSQpLUIE;  
spf=pass (google.com: domain of bounces+22662670-0628-d80281439@gmail.com@mailer.shopifyemail.com designates 149.72.90.155 as permitted sender) smtp.mailfrom="bounces+22662670-0628-d80281439@gmail.com@mailer.shopifyemail.com"  
Return-Path: <bounces+22662670-0628-d80281439@gmail.com@mailer.shopifyemail.com>  
Received: from o12.mailer.shopify.com (o12.mailer.shopify.com. [149.72.90.155])  
  by mx.google.com with ESMTPS id az37-20020a05620a172500b0077f5a4b743fsl10237680qkb.119.2023.12.12.20.11.55  
  for <d80281439@gmail.com>  
    (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);  
    Tue, 12 Dec 2023 20:11:55 -0800 (PST)  
Received-SPF: pass (google.com: domain of bounces+22662670-0628-d80281439@gmail.com@mailer.shopifyemail.com designates 149.72.90.155 as permitted sender) client-ip=149.72.90.155;  
Authentication-Results: mx.google.com;
```

Così possiamo controllare semplicemente leggendo l'email del mittente che sia conforme a il nome del sito o applicazione che ci ha inviato l'email, inoltre troviamo anche un indirizzo ip vicino all'email del mittente che possiamo andare a controllare tramite il sito <https://exchange.xforce.ibmcloud.com> , che ci permette di controllare il rischio e la sicurezza di un indirizzo ip.

Rischio

1

Report IP X-Force

149.72.90.155

Esporta come STIX 2

Suggerisci modifica

Segui

Questo report non contiene tag. Aggiungere tag tramite la casella commento.

Dettagli

Classificazione in categorie

Non sospetto

Applicazione

Nessuna applicazione conosciuta

Ubicazione

United States

Record WHOIS

Creato

05 set 2017

Aggiornato

18 apr 2023

Organizzazione registrante

SendGrid, Inc.

Paese o regione del registrante

United States

Nome registrar

ARIN

E-mail

abuse@sendgrid.com

15

Sequenza temporale

Visualizza tutto

Categoria	Motivo	Ubicazione	Data
	Regional Internet Registry	United States	27 dic 2021 08:52
	Regional Internet Registry	United States	26 dic 2021 08:52
	Regional Internet Registry	United States	29 mar 2020 08:52
	Regional Internet Registry	United States	28 mar 2020 08:52

2

DNS passivo

Nome	Categoria	Tipo	Ubicazione	Data
URL shopify.com	Shopping	A		19 mag 2021 10:43

Come possiamo vedere nell'immagine l'indirizzo ip dell'email ha rischio 1 quindi nessun rischio di phishing o di qualche tecnica di ingegneria sociale.

Un email che può essere esempio di phishing si presenterà così

d80281439

Hai (1) un messaggio da parte nostra. Clicca qui sotto per aprirlo.

Spam x

BRT

noreply@service.brtzfi8.it tramite cianjay.com

a me

Perché questo messaggio si trova nella cartella Spam? Sembra essere una risposta automatica a un messaggio che fingeva di essere stato inviato dal tuo indirizzo email.

Segnala come non spam

Segnalazione di phishing

Traduci in italiano

X

BRT

Hai (1) un messaggio da parte nostra. Clicca qui sotto per aprirlo.

N.ID:



6778533020

Ti informiamo che il tuo indirizzo dovrà essere confermato per confermare la spedizione del pacco.

CONTROLLA QUI >

Infatti notiamo che lo standard di autenticazione DKIM non l'ha passato, infatti ci dice 'FAIL'

Messaggio originale

ID messaggio	<20230325195746.decxfopz@mail.vpsnet.it>
Creato alle:	6 dicembre 2023 alle ore 06:09 (consegnato dopo 4 secondi)
Da:	 BRT  ™ <noreply@service.brtzfj8.it>
A:	d80281439@gmail.com
Oggetto:	d80281439  Hai (1) un messaggio da parte nostra. Clicca qui sotto per aprirlo. 
SPF:	PASS con l'IP 212.83.186.194 <a href="#">Ulteriori informazioni</a>
DKIM:	'FAIL' con il dominio service.brtzfj8.it <a href="#">Ulteriori informazioni</a>

**-4 Il direttore vi da il permesso di creare un phishing controllato. Descrivere come agireste.(Usare dei programmi è opzionale).**

**-5 L'obiettivo è cercare di ingannare le persone nel miglior modo possibile.**

Per prima cosa definire il tipo di phishing, quindi in questo caso andiamo ad utilizzare un email falsa. Aspetterei un po' di settimane dalla formazione che hanno ricevuto i dipendenti per agire, nel mentre io creo un email finta da inviare a tutti i dipendenti, clonando un sito per esempio google forms, dove l'email chiede di compilare questo modulo personale per dare una valutazione all'azienda. Quando il dipendente vede l'email, dovrà cliccare su pulsante per accedere al modulo di google, dove per prima cosa verrà richiesto di fare l'accesso a google con il proprio account, e poi nel modulo verrà chiesto di inserire il proprio nome e cognome e l'email per poi mandare una copia del modulo. Dopo aver mandato l'email a tutti i dipendenti facciamo un resoconto di quanti sono stati attenti a controllare che fosse un email di phishing e quanti invece sono cascati nella truffa.