CONSEGNA S3/L5
DIGITAL CITIZENSHIP LESSON

PHISHING 101

Pensa prima di Clickare!

STRUTTURA DELLA FORMAZIONE

Le lezioni saranno di 1 ora ogni mattina per un totale di 6 giorni lavorativi

1. Cos’è l’ingegneria sociale?
2. Cos’è il phishing?
3. Tipologie comuni di phishing
4. Come funziona?
5. Come evitarlo?
6. Formazione pratica
7. Riepilogo finale

OBIETTIVI

Alla fine di questa formazione i dipendenti sapranno:

1

Cos’è l’ingegneria sociale e come viene messa in atto

2

Il significato e come riconoscere il Phishing

3

Cosa fare e non fare quando si ha davanti un presunto tentativo di Phishing

COS’È L’INGEGNERIA SOCIALE?

L’ingegneria sociale non è altro che una tecnica che si basa principalmente sulla manipolazione delle persone, al fine di ottenere informazioni, dati sensibili, vantaggi. Quest’ ultima può essere utilizzata in molti contesti tra cui anche la sicurezza informatica. Essendo una pratica che si basa su tattiche psicologiche come inganno e persuasione il miglior modo per affrontarla è la consapevolezza.

Quali sono i campanelli di allarme quando si riceve una mail o un messaggio?

COS’È IL PHISHING?

Il Phishing è un’applicazione reale dell’Ingegneria Sociale, ovvero una tecnica utilizzata per rubare credenziali, codici di carte di credito e in generale dati sensibili.
Potresti essere incoraggiato ad effettuare il login su siti “cloni” (ad esempio di Amazon o servizi di cui ci avvaliamo) che potrebbero sembrare in un primo momento i siti ufficiali, ma in realtà staremo inviando i nostri dati ad un criminale informatico.

Cosa rende sospetto un sito che ti chiede di fare login?

TIPOLOGIE DI PHISHING

I più comuni tentativi sono:

EMAIL PHISHING

Si basa sull’invio di email false spacciandosi per una fonte attendibile (es. Amazon, Bartolini)

SMS PHISHING

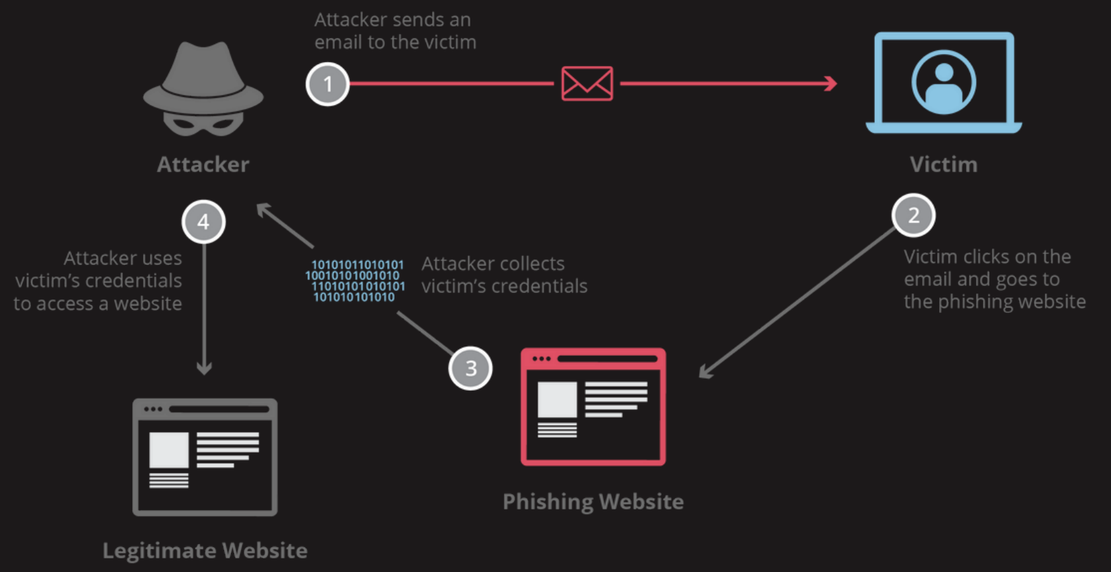
Si basa sull’invio di messaggi con link malevoli o richiesta di informazioni personali

SOCIAL MEDIA PHISHING

Si basa sull’invio di contenuti, link malevoli o richieste di dati sensibili attraverso profili falsi

COME FUNZIONA IL PHISHING?

I criminali informatici per eseguire un tentativo di email Phishing, per prima cosa, creano dei cloni dei siti web che vogliono utilizzare per ottenere i dati personali delle vittime (a oggi è una procedura molto semplice clonare un sito). Dopodiché, tramite degli indirizzi mail simili a quelli ufficiali, invieranno un messaggio che possa indurre la vittima ad aprire il link allegato, spesso convincendola che è necessaria un'azione repentina. Il messaggio, per sembrare attendibile, potrebbe riportare loghi o testo simile agli originali; nella maggior parte dei casi ci si trova di fronte a una schermata di login uguale a quella del servizio che ci aspettavamo, solo che le informazioni che andremo ad inserire arriveranno direttamente al criminale informatico.



SEGNALI DI AVVERTIMENTO DEL PHISHING

Per capire se ci troviamo davanti ad un tentativo di Phishing tra le prime cose che possono catturare la nostra attenzione ci sono:

1. Linguaggio urgente o minaccioso
2. Mittente della email sospetto
3. Richiesta di informazioni personali
4. Errori ortografici o grammaticali
5. Link o allegati sospetti

COME PROTEGGERSI DAL PHISHING?

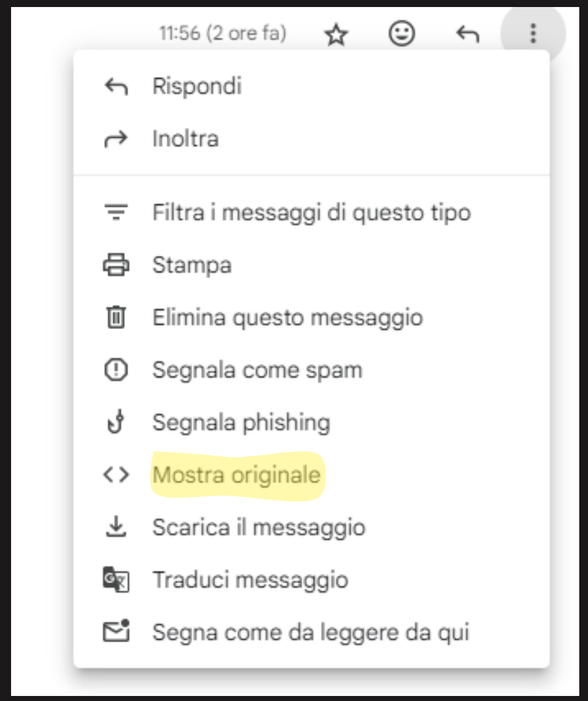
Come abbiamo detto in precedenza, il miglior modo per prevenire il Phishing è la consapevolezza. Per questo oggi vedremo i parametri più utili da verificare per sapere se ci si trova davanti a un presunto tentativo di Phishing

Tra i parametri più importanti da controllare abbiamo:

- SPF (SENDER POLICY FRAMEWORK)
- DKIM (DOMAIN KEYS IDENTIFIED MAIL)
- DMARC (DOMAIN-BASED MESSAGE AUTHENTICATION REPORTING AND CONFORMANCE)

COME PROTEGGERSI DAL PHISHING?

Andiamo a vedere cosa sono e dove trovare questi fondamentali parametri.
Quando ci troviamo davanti ad una mail, di presunto Phishing, la cosa migliore che possiamo fare è cliccare i puntini in alto a destra nel corpo della mail e selezionare la voce “mostra originale” come nell’esempio qui riportato



COME PROTEGGERSI DAL PHISHING?

La schermata che ci ritroveremo sarà la seguente

Messaggio originale

ID messaggio	<vylz5fixbDFBuSLDYxuknw@notifications.google.com>
Creato alle:	15 dicembre 2023 alle ore 11:56 (consegnato dopo 1 secondo)
Da:	Google <no-reply@accounts.google.com>
A:	mpalozza@gmail.com
Oggetto:	Avviso di sicurezza
SPF:	PASS con l'IP 209.85.220.73 Ulteriori informazioni
DKIM:	'PASS' con il dominio accounts.google.com Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

Da qui avremo già una visione più chiara della situazione: infatti, non è necessario sapere cosa indichino questi parametri, in quanto se dovesse trattarsi di una mail di Phishing queste voci saranno del tutto assenti o comunque non saranno tutte presenti. Tuttavia è sempre importante esaminare l'intero contesto della mail.

A:	matteopalozza@yahoo.it
Oggetto:	Siamo alla ricerca di nuovi clienti, lasciati premiare!
SPF:	SOFTFAIL con l'IP 0.0.0.0 Ulteriori informazioni

Scarica messaggio originale

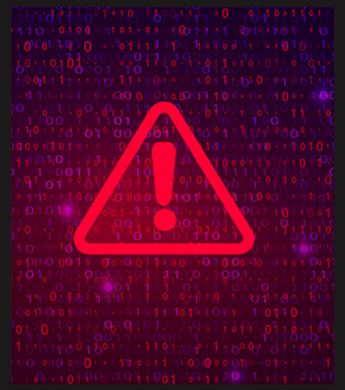
Tentativo di Phishing via mail

FORMAZIONE PRATICA

Dopo aver parlato con il direttore dell’azienda e aver ricevuto il permesso di creare un Phishing controllato, ho agito nel seguente modo:

- Raccolta di informazioni: dopo aver raccolto informazioni generali sull’azienda, il direttore mi fornirà tutti gli indirizzi email dei dipendenti di Epicodesecurity

- Creare le basi del Phishing: ho creato un sito clone della piattaforma di login hostato dal dominio www.Eplcodesecurity.it il quale assomiglia molto all’originale



- Progettare una mail credibile: ho ipotizzato di far inviare una mail a nome del direttore che esortasse i dipendenti ad entrare nella nuova piattaforma aziendale tramite un link, preoccupandomi di rendere la mail quanto più uguale alle originali
- Infine ho inviato le mail ai dipendenti per verificare la loro interazione con le email di phishing a seguito della formazione

CONCLUSIONI

A seguito della informazioni ricevute dal direttore ho appreso che ci sono 250 dipendenti nella società

Prima della formazione circa il 20% dei dipendenti ha dichiarato di aver subito danni dagli attacchi di Phishing

Dopo circa un mese dalla fine della formazione ho chiesto ai dipendenti come fosse cambiato il loro rapporto con le email, ricevendo un responso perlopiù positivo, con solo il 2% dei dipendenti che risulta avere ancora problemi di phishing

Contro gli attacchi informatici non esiste una difesa sicura al 100%, però la consapevolezza ci aiuta a contenere le possibilità

PENSA PRIMA DI CLICKARE!

PROTEGGI TE STESSO CONTRO IL PHISHING

Non divulgare le tue informazioni personali!