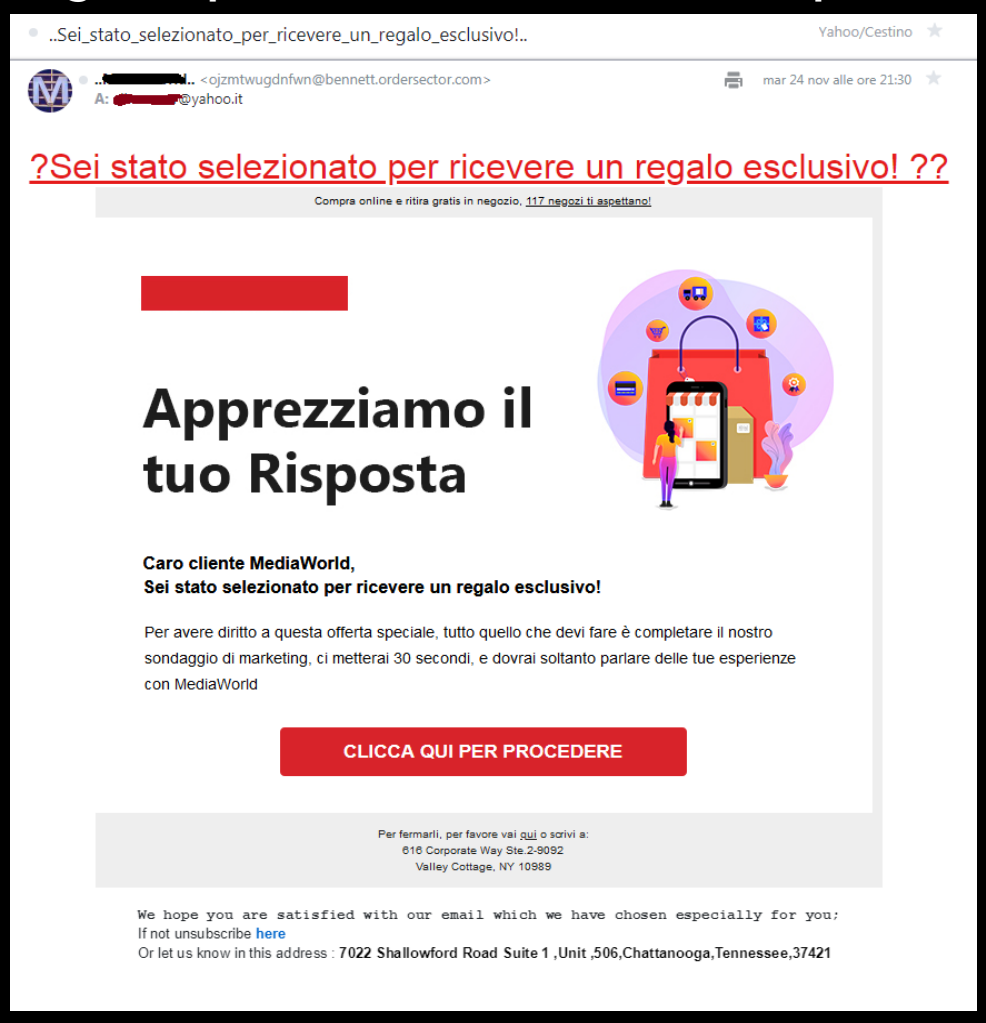
Security

Prevenzione attacchi di ingegneria sociale Epicodesecurity.

L’arte della difesa: Educazione al Phishing

Partiamo subito definendo cos’è il Phishing, si tratta di una tecnica di ingegneria sociale utilizzata da criminali informatici, attraverso l’inganno dell’individuo, con lo scopo di ottenere informazioni sensibili.
Immaginate questa scena, vi svegliate la mattina, andate in bagno a sciacquare la faccia e vi sedete in cucina a fare colazione.

Prendete il telefono e notate una notifica da parte della vostra casella di posta elettronica, aprite e vi accorgete di una mail da parte del vostro negozio preferito (Mediaworld in questo caso):



“Fantastico!
Non vedo l’ora di rispondere al questionario e recarmi immediatamente in negozio!”

Cliccate per compilare il sondaggio e qualcosa non va…
Vi accorgerete ben presto che non si tratta di mediaworld.
Chiudete la vostra casella di posta elettronica sconsolati per non aver vinto nessun regalo esclusivo…
Cosa è successo? L’email in questione si tratta di Phishing, un’email falsa.

Quali sono le conseguenze? Molto probabilmente i vostri dati sensibili come informazioni personali, credenziali di accesso ai vostri socials, siti online e nel

peggiore dei casi applicazioni riguardanti le vostre finanze, sono finite nelle mani del criminale che vi ha mandato l'email.

Conseguenze all'interno di un'azienda

Il bersaglio principale di questi attacchi sono proprio le aziende.
Le conseguenze potrebbero essere particolarmente pericolose se una di queste email malevole raggiunge il suo scopo all'interno di esse, per farvi un esempio possiamo citarne alcune:
-Furto di dati sensibili: Compromissione dei dati finanziari, informazioni personali dei dipendenti, dati dei clienti, segreti aziendali.
-Perdite finanziarie dirette: Tramite frodi o trasferimenti di denaro non autorizzati.
-Installazione malware: I link di queste email possono installare potenziali malware che danneggiano i sistemi interni.
-Danni alla reputazione: La perdita di fiducia dei clienti e partner a seguito di questa violazione della sicurezza.

Capite bene che la gravità delle conseguenze può essere molto elevata, si potrebbe incorrere alla chiusura definitiva di un'azienda.

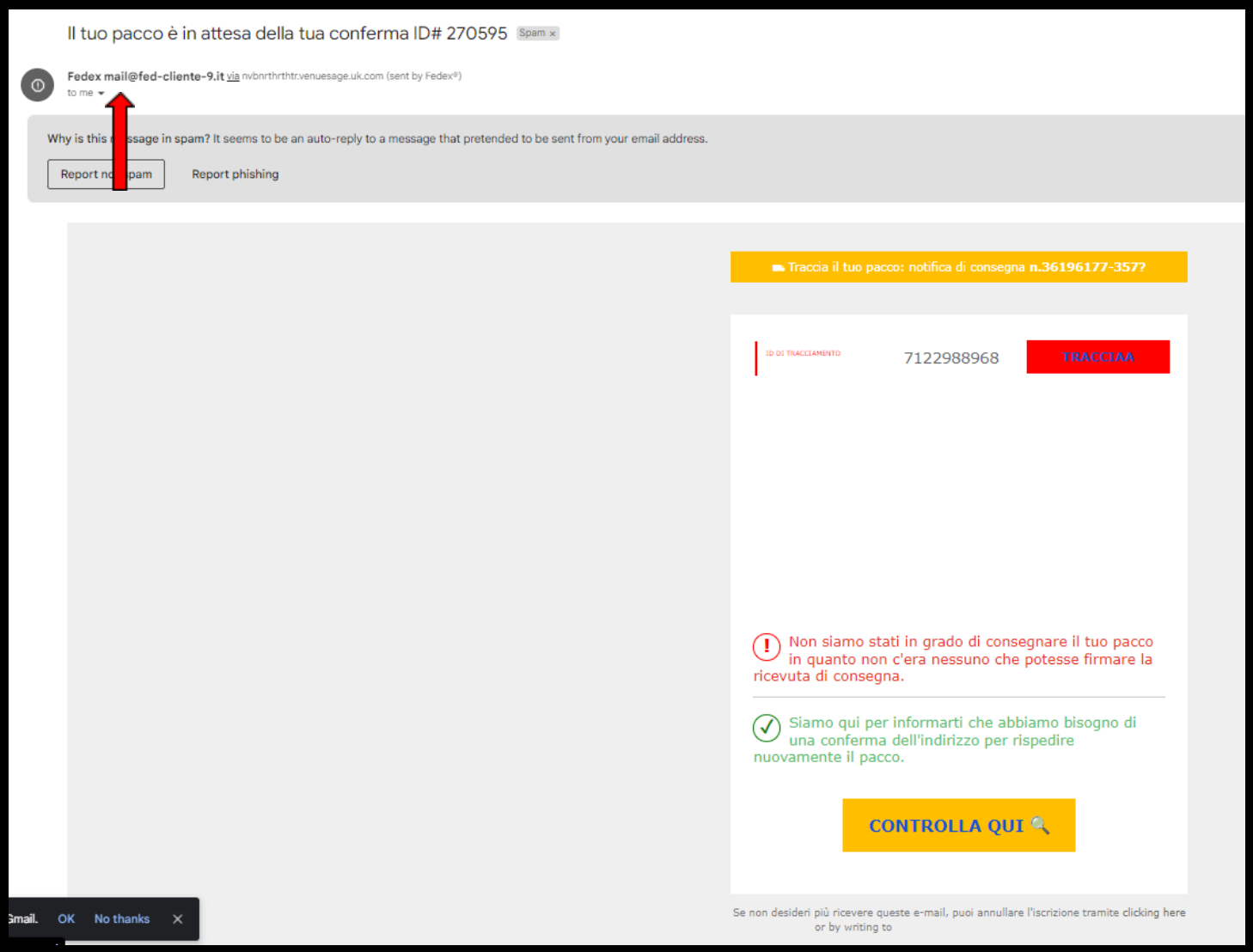
Come posso difendermi?

Proprio come i software informatici, anche il cervello umano presenta delle vulnerabilità, rendendoci suscettibili a tattiche di ingegneria sociale come il Phishing.
Ma questo non vuol dire che, attraverso l'educazione, non possiamo prevenire questo tipo di attacchi.

Come riconoscere un attacco di phishing

Una volta ricevuta un'email nella nostra casella aziendale, procediamo con alcuni metodi per verificarne l'autenticità, accorgimenti attuabili anche per chi non conosce il campo informatico.
Procediamo con i seguenti passaggi:

1. Verifica della fonte: Attraverso le impostazioni del provider aziendale, verifichiamo se l'indirizzo email dell'emittente corrisponde al contenuto della mail. Vediamo un esempio pratico:



Come possiamo notare in questo esempio, l’emittente si identifica come fedex, richiedendo la conferma del tuo pacco.
Controllando però l’indirizzo email, ci accorgiamo che non corrisponde all’originale.

2. Richieste di informazioni personali: Diffidate da email che chiedono dati sensibili, soprattutto se non avete iniziato voi la comunicazione.

3. Errori di ortografia e grammaticali: Email professionali sono solitamente ben scritte. Errori del genere possono essere segno di phishing.

4. Controllare i filtri: Se non doveste capire l’autenticità dell’email attraverso i passaggi precedenti, si possono controllare i filtri SPF, DKIM, DMARC per verificarne ulteriormente la veridicità.
Comprendo che entriamo in termini più avanzati, per questo non vi è richiesto di saperne il funzionamento, ma di essere consapevoli di questi strumenti.

SPF: Immaginalo come un elenco di invitati per una festa, se il mittente è si trova in questo elenco può considerarsi quasi sicuro, al contrario, potrebbe essere un impostore

DKIM: Consideralo come una sigillatura di cera su una lettera. Questo filtro aggiunge una firma digitale alle email inviate, mostrandola diversa se il contenuto dell'email è stato modificato durante il tragitto.

DMARC: Si tratta di un'istruzione per gestire le lettere sospette. Questo filtro utilizza i precedenti per verificare se un'email è autentica. Se un'email non supera i controlli, esso dice al server come gestirla.

Per verificare questi filtri potreste recarvi nelle impostazioni della mail e verificarne la presenza per essere sicuri che abbia superato questi controlli. Se è autentica, risulterà questo:

SPF:	PASS with IP 204.135.8.93 Learn more
DKIM:	'PASS' with domain fedex.com Learn more
DMARC:	'PASS' Learn more

Nel caso in cui avete seguito tutti i passaggi e non siete ancora sicuri dell'autenticità di un'email, rivolgetevi ad un esperto di sicurezza informatica interno.

Programmazione del test

Un mese dopo la conclusione della fase formativa, con il consenso esplicito del direttore, procederò a un test pratico delle conoscenze acquisite dai dipendenti. Questo test si articolerà in una simulazione di attacco phishing controllato e altamente sofisticato.

L'obiettivo principale di questa simulazione è valutare l'efficacia della formazione ricevuta dai dipendenti e la loro capacità di applicare le conoscenze apprese per identificare tentativi di phishing.

L'email di phishing creata per il test sarà particolarmente sofisticata e ingannevole, comprenderà:
1. Un design e layout che imita fedelmente quello di un mittente legittimo.
2. Un linguaggio e tono coerenti con le comunicazioni autentiche.
3. Link falsificati ma credibili, che reindirizzano a una pagina sicura di nostra creazione, dove verrà spiegato il contesto del test.
4. Nessuna raccolta di dati sensibili: La simulazione sarà completamente sicura.