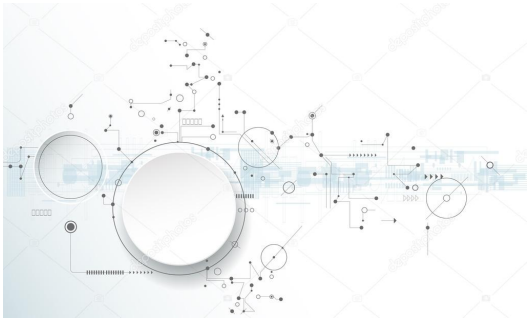


Siete stati chiamati da un'azienda di nome Epicodesecurity, questa azienda ha un sito web suo personale con il nome di dominio www.Epicodesecurity.it. un server email con l’email aziendale Epicodesecurity@semoforti.com

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.

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

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

Gli attacchi di ingegneria sociale, in particolare quelli basati sul **phishing**, rappresentano una minaccia significativa per la sicurezza online, 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 e la manipolazione.

Il phishing è una forma di attacco di ingegneria sociale in cui gli attaccanti cercano di indurre le persone a rivelare informazioni sensibili, come nomi utente, password e dettagli finanziari.

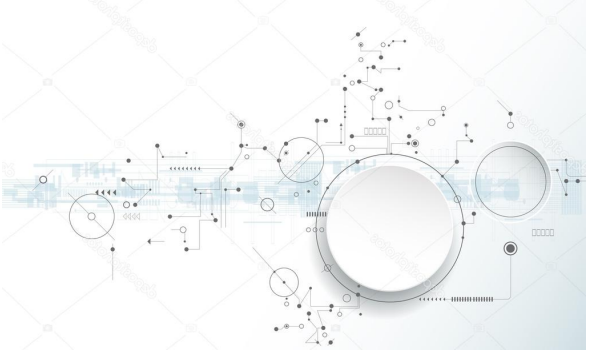
Le tecniche di phishing possono includere phishing email, siti web, telefonico, social e messaggi istantanei.

Come in ogni cosa la miglior difesa è la prevenzione, essere consapevole e adottare pratiche di sicurezza online. Verificare sempre l'autenticità di comunicazioni e siti web, evitare di cliccare su link sospetti, usare l'autenticazione a due fattori quando possibile e mantenere il software aggiornato.

Strumenti progettati per rilevare e bloccare tentativi di phishing sono i cosiddetti filtri anti - phishing:

- **SPF** → l'obiettivo principale è consentire ai destinatari delle email di verificare che un determinato messaggio sia stato inviato da un server autorizzato per il dominio dichiarato nel campo "Indirizzo Mittente" dell'email, confrontandolo con l'elenco di indirizzi IP autorizzati nel record SPF del dominio del mittente. Se l'indirizzo IP non è autorizzato, il destinatario potrebbe decidere di marcare il messaggio come sospetto o rifiutarlo;

- **DKIM** → l'obiettivo principale è garantire che il contenuto di un'email non sia stato alterato durante il trasporto e che l'email provenga da un mittente autenticato. Il mittente firma digitalmente il contenuto dell'email con una chiave privata, e il destinatario può verificare l'autenticità utilizzando la chiave pubblica associata.
- **DMARC** → è uno standard di autenticazione delle email che si basa su SPF e DKIM, l'obiettivo è fornire una politica di autenticazione e un meccanismo di reporting per garantire che le email inviate da un dominio siano conformi alle politiche di autenticazione del dominio. Consente di specificare le azioni da intraprendere per le email che non superano l'autenticazione che, ad esempio, possono essere contrassegnate come spam o rifiutate.



Il direttore vi da il permesso di creare un phishing controllato:

4 - Descrivere come agireste.(Usare dei programmi è opzionale).

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

Sotto autorizzazione del direttore possiamo impostare una dimostrazione creando un e-mail falsa con un link che invita a cliccare per ottenere un bonus vacanza, il cui indirizzo è uguale a quello aziendale a cui sono abituati se non per il finale **Epicodesecurity@semoforti.com → Epicodesecurity@semoforsi.com**, e il cui sito di destinazione è la perfetta copia di un noto sito di viaggi.

Si inviteranno i dipendenti a notare che prima di tutto l'indirizzo e-mail può già mettere in allarme e, in ogni caso, di utilizzare sempre **"mostra originale"** per rendersi conto che tale indirizzo non possiede le autorizzazioni dei filtri di phishing; mettendo caso che si arrivi sul sito, si focalizza l'attenzione sull'url del sito internet che non risulta sicuro, cosa che deve mettere in allarme perché, ovviamente, qualora si andrà a cliccare per avere il fatidico bonus, si rischia seriamente di essere derubati dei propri dati sensibili.

Come è ovvio si tratta di una dimostrazione a scopo informativo, quindi nessuno rischia nulla, ma è fondamentale per cambiare la mentalità comune e far in modo di essere sempre informati e preparati per non cadere in tranelli, o quantomeno di non rendere ai criminali informatici la cosa così semplice.