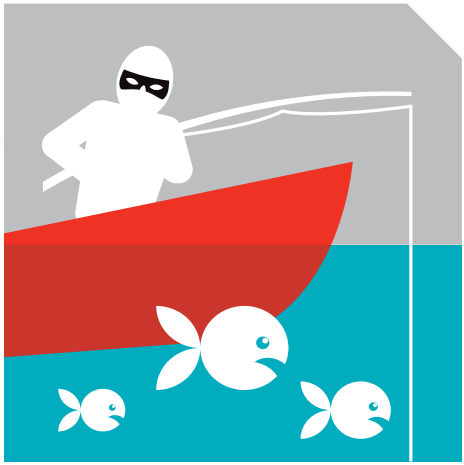
bsi. Phishing

Pensa prima di cliccare!



Se sembra troppo bello per essere vero, probabilmente non è vero
Le email di phishing sono progettate appositamente per contenere stimoli psicologici che inducano a cliccare.

Stai allerta sugli argomenti delle mail di phishing
Gli attaccanti lanciano campagne di phishing basandosi su eventi attuali e reali. Per esempio, periodi come scadenze fiscali, grandi eventi sportivi e la corrente pandemia hanno visto un incremento del traffico phishing.

Tono dell'email
Le email di phishing sono scritte per stimolare le emozioni. Avidità, urgenza, curiosità e paura sono solo alcuni dei principali stimoli contenuti in un'email di phishing efficace.

Non cliccare...
...su link contenuti in email inaspettate o sospette, e non aprirne i file allegati. Verifica sempre con il mittente via telefono.

Sii particolarmente attento...
...quando i file o i link nell'email indirizzano a siti che richiedono username e password: anche se sono molto realistiche sono spesso comunicazioni fraudolente.

Frasi impersonali?
La mail contiene saluti generici?

L'indirizzo del mittente è strano?
L'indirizzo del mittente corrisponde al nome dell'azienda rispettabile di cui si parla?

URL troppo corto?
È importante prestare attenzione agli URL troppo corti, usati dai criminali al posto dell'URL originale per far sembrare plausibile la mail di phishing. Fai scorrerei il mouse sopra il link nell'email per verificare la correttezza dell'URL.

Consapevolezza sul phishing
Campagne regolari di sensibilizzazione dei dipendenti sono molto utili.

Configura la tua casella di posta...
...così che le email dall'esterno siano segnalate come "Email esterna"

Doppio controllo con i tuoi contatti
Nel caso di un attacco BEC (Business Email Compromise), è importante verificare richieste di pagamento e aggiornamenti sulle informazioni di pagamento.

Hai ricevuto una mail sospetta?

Se si riceve una qualsiasi email da una fonte non affidabile, è importante avvisare il dipartimento IT e seguire le loro indicazioni. Se si clicca su un link o si scaricano software sospetti è necessario allertare il dipartimento IT, che attiverà le procedure di sicurezza e i protocolli in essere per risolvere il problema e rimuovere la minaccia.