Università
per Stranieri
di Perugia

Come riconoscere un’e-mail di phishing

Il phishing è una pratica fraudolenta che consiste nell'invio di messaggi per indurre i destinatari a rivelare informazioni personali come password e numeri di carta di credito. Esistono diversi modi per individuare un tentativo di phishing e misure da adottare quando ci si trova di fronte a un tentativo di phishing.

Come riconoscere un’e-mail di phishing

Può essere **difficile** riconoscere se un’e-mail è legittima o un tentativo di phishing, ma ci sono alcuni **segnali** a cui devi fare attenzione:

1. **Linguaggio insistente o minaccioso**
   Le e-mail di phishing spesso creano un senso di urgenza o di paura per farti reagire rapidamente. Potrebbero affermare che il tuo account è in pericolo o che dovrai affrontare delle conseguenze se non rispondi immediatamente.
2. **Mittente sospetto**
   Controlla l'indirizzo e-mail del mittente. Le e-mail di phishing utilizzano spesso indirizzi e-mail ingannevoli che somigliano a quelli di organizzazioni legittime, ma che contengono lievi variazioni o errori ortografici.
3. **Saluti generici**
   Le e-mail di phishing spesso utilizzano formule di saluto generiche come "Gentile cliente" invece di rivolgersi a te per nome. Le organizzazioni legittime di solito personalizzano le proprie e-mail con il tuo nome.
4. **Errori grammaticali e di ortografia**
   Le e-mail di phishing spesso contengono errori di ortografia, errori grammaticali o un uso maldestro della lingua. Le organizzazioni legittime inviano solitamente comunicazioni professionali, ben scritte e prive di errori.
5. **Link o allegati sospetti**
   Diffida di link o allegati inaspettati nelle e-mail, soprattutto se non conosci il mittente. Questi possono portare a siti web dannosi o scaricare malware sul tuo dispositivo.
6. **Richiesta di informazioni personali**
   Fai attenzione alle e-mail che ti chiedono di fornire informazioni personali o sensibili come password, numeri di previdenza sociale o dati della carta di credito. Raramente le organizzazioni legittime richiedono questo tipo di informazioni via email.

Cosa devo fare se ricevo un’e-mail di phishing?

Se hai identificato un’e-mail di phishing, puoi adottare alcune **misure**:

- **Evita** di cliccare su qualsiasi **link** sospetto e non scaricare nessun **allegato** dall'email.

- **Non fornire** informazioni personali.
- **Segnala** l'e-mail come spam.
- **Elimina** l'e-mail.
- **Attiva** l'autenticazione a due fattori (**2FA**) su tutti i tuoi account, se possibile. Se la tua password viene violata, l'autenticazione a due fattori garantisce comunque la sicurezza del tuo account.
- **Aggiorna** le **password** di qualsiasi account compromesso, se hai fatto clic su un link o hai fornito informazioni. Se utilizzi la stessa password per più siti web, aggiorna anche quelle. Ti consigliamo di utilizzare una password forte e univoca, memorizzata in un **gestore di password**.

Queste azioni garantiranno la sicurezza dei tuoi dati personali.