Come difendersi da una e-mail phishing

Sono sempre di più le e-mail phishing ricevute dagli utenti: ecco cosa fare per riconoscerle e quali sono i pericoli

> **Che cosa sono gli attacchi phishing**. *Si tratta di un attacco informatico che viene perpetuato tramite SMS ed e-mail. Il malvivente invia a un utente (nella maggior parte dei casi le vittime sono casuali, vengono inviati gli stessi messaggi a centinaia di migliaia di persone) un'e-mail nella quale lo invita a* ***cliccare su un link per cambiare la password*** *del proprio conto corrente o a inviare i propri dati personali per ritirare un premio. Per rendere più veritiero il messaggio,* **l'e-mail del mittente** *sembra essere quella di una vera azienda (Poste, banca, catena di elettrodomestici) e* **la URL del sito** *che andiamo ad aprire sembra identica a quella del portale originale.*

Come riconoscere una *e-mail phishing*

Partiamo dalle basi. Per riconoscere un messaggio-truffa basta effettuare dei semplici check. Se riceviamo un'e-mail nella quale apparentemente la nostra banca ci avvisa che dobbiamo cambiare la password a causa di problemi generali di sicurezza, controlliamo attentamente l'indirizzo di posta elettronica del mittente. I pirati informatici sono abili nel costruire degli ***indirizzi molto simili a quelli originali, ma si differenziano per un paio di lettere***. Se notiamo qualcosa di strano già nel primo controllo, possiamo essere abbastanza sicuri che si tratta di un **messaggio phishing**.

Altro controllo da fare è la **URL del link** presente nel messaggio (in una e-mail phishing c'è sempre un link che porta su una piattaforma esterna). Anche in questo caso, ***la URL sembra essere identica a quella di un vero sito, ma si differenzia sempre per una o due lettere***. Basta un po' di attenzione per capire che si tratta di un sito falso creato appositamente per truffare gli utenti.

Che cosa fare quando si riceve una *e-mail phishing*

La prima cosa da fare quando si riceve una e-mail phishing è ***NON cliccare sui link presenti all'interno del messaggio.*** L'infezione potrebbe iniziare proprio cliccando il link.

Altra cosa da non fare è ***NON rispondere a questo tipo di e-mail***. I truffatori inviano ogni giorno milioni di messaggi di posta elettronica nella speranza che qualche utente abbocchi alla truffa. Rispondendo all'e-mail si dà la conferma al truffatore che il nostro indirizzo di posta sia "vivo e vegeto" e continuerà a inviare messaggi ogni giorno.

Segnalare la *e-mail* al provider di posta elettronica

Con la crescita degli attacchi phishing tutti i principali provider di posta elettronica hanno implementato degli strumenti per **bloccare i messaggi-truffa**. Se un'e-mail phishing riesce a superare i filtri di protezione, gli utenti possono SEGNALARE L'INDIRIZZO DI POSTA ELETTRONICA DEL MITTENTE IN MODO CHE VENGA BLOCCATO DAL PROVIDER.

La procedura da seguire cambia a seconda dell'app e del provider di posta elettronica che utilizziamo, ma i passaggi da seguire sono molto simili tra di loro. Nella maggior parte dei casi bisogna entrare all'interno del messaggio-truffa, cliccare sulle impostazioni e poi su "Segnala phishing". In questo modo il provider farà partire un'indagine per capire se si tratta realmente di un messaggio falso.

Segnalare la *e-mail* alle forze dell'ordine

Ove si cada nella **trappola di in attacco phishing** si deve SEGNALARE IMMEDIATAMENTE L'ACCADUTO ALLE FORZE DELL'ORDINE. La Polizia Postale può far partire un'indagine per risalire al mittente del messaggio e cercare di bloccare la truffa.

Segnalare la *e-mail* all'azienda vittima della truffa

Ogni **messaggio phishing** sfrutta il nome di una vera azienda: un servizio di home banking, un brand famoso, una catena di elettrodomestici. Queste aziende sono anche loro delle vittime della truffa: i malviventi utilizzano impropriamente il loro nome.

Se ricevete **una e-mail phishing** AVVERTITE IMMEDIATAMENTE L'AZIENDA COINVOLTA, in modo che anch’essa possa far partire una sua denuncia.

Cancellare la *e-mail*

Una volta seguiti tutti questi passaggi, cancellate l'e-mail.

Non avere paura

Ricevere un messaggio phishing non è pericoloso. E non vuol dire che il proprio PC è infetto. I messaggi-truffa stanno diventando sempre più frequenti e può capitare di riceverne un paio. L'importante è seguire tutti i passaggi illustrati nella nostra guida ed essere sempre attenti a non cliccare su nessun link.