Phishing via email: i segnali e le regole per smascherare i falsi messaggi

LETTURA: 6 MINUTI | TARGET: CONSUMATORI E UTENTI WEB | FONTE: NOTIZIARIO.NET



Immagine generata con supporto AI - Trasparenza Reg. UE 2024/1689 (Fonte: NOTIZIARIO.NET)

S SINTESI DELLA NOTIZIA

Il fenomeno del phishing via email continua a mietere vittime a causa di tecniche sempre più raffinate. In questa guida completa analizziamo i segnali d'allarme principali e le strategie per difendersi efficacemente da truffe informatiche e furti di identità.

R REGOLE D'ORO E SICUREZZA

- Non cliccare mai su link o pulsanti contenuti in email che richiedono aggiornamenti urgenti di dati.
- Verificare sempre l'indirizzo email completo del mittente e non soltanto il nome visualizzato.
- Attivare l'autenticazione a due fattori (2FA) su tutti gli account bancari e personali.
- Non scaricare o aprire allegati inattesi con estensioni sospette (.exe, .zip, .scr).

P COSA C'E DA SAPERE IN SINTESI

- I tentativi di phishing via email sfruttano l'urgenza e la contraffazione di marchi noti per ingannare la vittima.
- L'analisi attenta del mittente reale e dei link tramite il controllo del dominio rivela la natura fraudolenta del messaggio.
- In caso di inserimento di dati riservati, è necessario bloccare subito le carte e contattare la Polizia Postale.

C IL CONSIGLIO DELLA REDAZIONE

Mantenere sempre un approccio prudente: di fronte a comunicazioni che richiedono interventi urgenti sui propri dati bancari o personali, non utilizzare mai i link forniti nell'email ma accedere al servizio digitando manualmente l'indirizzo ufficiale nel browser.