



# PHISHING: ATTENZIONE AI «PESCATORI» DI DATI PERSONALI

## Occhio agli indirizzi

I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue.

E' utile anche prestare attenzione al mittente (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali).

Meglio diffidare dei messaggi con toni intimidatori, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole strategie per spingere il destinatario a fornire informazioni personali.

In genere, i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un form da compilare. I dati così carpiri possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

## Allegati

 [Phishing attenzione ai pescatori di dati personali. Infografica](#) 297 KB