



## Phishing: attenzione ai "pescatori" di dati personali La scheda informativa del Garante privacy

Cosa è il phishing? Quali rischi comporta? Come riconoscerlo? Quali sono le piccole accortezze quotidiane che è possibile mettere in campo per evitare che malintenzionati si impossessino dei nostri dati personali?

A queste e ad altre domande punta a dare risposta la nuova [scheda informativa](#) sintetica (infografica) del Garante per la protezione dei dati personali, da oggi diffusa sul sito web [www.garanteprivacy.it](http://www.garanteprivacy.it) e sui canali social in cui sono presenti account istituzionali dell'Autorità ([LinkedIn](#) e [Google+](#)).

La scheda è parte di una serie di [nuovi prodotti informativi](#) ideati dal Garante per sensibilizzare gli utenti sulle varie tematiche connesse alla protezione dei dati personali.

**IL PHISHING: Attenzione ai «pescatori» di dati personali**

Il phishing è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito - con l'intento di compiere operazioni fraudolente.

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità», si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc.

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 carpati 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.

### ALCUNI CONSIGLI PER DIFENDERSI

- 1. IL BUON SENSO PRIMA DI TUTTO**  
Dati, codici di accesso e password personali **non** dovrebbero mai essere comunicati a sconosciuti. E' bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita **non** richiedono informazioni personali attraverso e-mail, sms, social media o chat: quindi, meglio evitare di fornire dati personali, soprattutto di tipo bancario, attraverso tali canali. Se si ricevono messaggi sospetti, è bene **non** cliccare sui link in essi contenuti e **non** aprire eventuali allegati, che potrebbero contenere virus o programmi *trojan horse* capaci di prendere il controllo di pc e smartphone. Spesso dietro i nomi di siti apparentemente sicuri o le URL abbreviate che si trovano sui social media si nascondono link a contenuti non sicuri. Una piccola accortezza consigliata è quella di posizionare sempre il puntatore del mouse sul link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.
- 2. 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.
- 3. PROTEGGERSI MEGLIO**  
E' utile installare e tenere aggiornato sul pc o sullo smartphone un programma antivirus che protegga anche dal phishing. Programmi e gestori di posta elettronica hanno spesso sistemi di protezione che indirizzano automaticamente nello spam la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni. Meglio non memorizzare dati personali e codici di accesso nei browser utilizzati per navigare online. In ogni caso, è buona prassi impostare password alfanumeriche complesse, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato: banca online, e-mail, social network, ecc. (vedi anche la scheda del Garante con i consigli per gestire le password in sicurezza), a meno di disporre di sistemi di autenticazione forte (*strong authentication*).
- 4. ACQUISTI ONLINE IN SICUREZZA**  
Se si fanno acquisti online, è più prudente usare carte di credito prepagate o altri sistemi di pagamento che permettono di evitare la condivisione di dati del conto bancario o della carta di credito.
- 5. LA PRUDENZA NON E' MAI TROPPIA**  
Per proteggere conti bancari e carte di credito è bene controllare spesso le movimentazioni e attivare sistemi di alert automatico che avvisano l'utente di ogni operazione effettuata. Nel caso si abbia il dubbio di essere stati vittime di phishing è consigliabile contattare direttamente la banca o il gestore della carta di credito attraverso i canali di comunicazione conosciuti e affidabili.

Per segnalazioni e richieste di ulteriori informazioni: [urp@gpdp.it](mailto:urp@gpdp.it)