



# Phishing e truffe informatiche: ecco come dormire sonni tranquilli

Dai media a volte arrivano allarmi sui furti di dati elettronici. Ma per godersi in sicurezza la comodità dei servizi online, bastano poche precauzioni

**P**hishing. Ovvero “pescare” (dall’inglese to fish) navigatori di Internet inducendoli a **rivelare i propri codici segreti** utilizzati per effettuare operazioni dispositive online. Negli ultimi anni il phishing (qualcuno lo traduce con “spillaggio”) ha conosciuto un’escalation anche nel nostro paese. Confermandosi – rileva l’ultimo rapporto dell’Assintel (l’associazione italiana delle imprese informatiche e tecnologiche) – fra le truffe più diffuse.

## “INGEGNERI” DEL MALAFFARE

Ma come agiscono i cybercriminali? I truffatori si ispirano ai principi della cosiddetta “ingegneria sociale”, vale a dire lo studio del comportamento altrui per carpire informazioni riservate. C’è chi lo fa spacciandosi

al telefono per un operatore di call centre (vishing), rovistando nelle cassette della posta dei condomini (boxing), perfino frugando nell’immondizia alla ricerca di ricevute ed estratti conto (trashing). Ma **lo strumento preferito rimane la posta elettronica**: un messaggio e-mail nel quale il phisher sollecita ai correntisti le password di accesso ai rispettivi conti online, magari dichiarandosi un tecnico della banca incaricato di aggiornare il sistema informatico.

## QUANDO LA MAIL È SOSPETTA

Un tempo bastava un pizzico di ragionevolezza per smascherare il carattere fraudolento delle richieste: agli albori del phishing, l’italiano stentato delle mail (molti pirati

agiscono dall’estero) e la grafica rudimentale ne tradiva la falsità a una prima occhiata.

Oggi molti phisher si sono fatti agguerriti: le **mail fraudolente** possono includere il logo e l’impostazione grafica abitualmente utilizzate dai mittenti legittimi e quasi sempre rimandano, con un collegamento, a una pagina di accesso uguale in tutto al sito dell’organizzazione presa di mira. Insomma, si tratta di **contraffazioni di primissimo livello**.

## PRIMA REGOLA: NESSUNA RICHIESTA

Per difendersi dal phishing basta aver presente un’evidenza: nessuna organizzazione seria, né tantomeno BankAmericard, chiede ai propri clienti di comunicare i dati di accesso. Per nessun motivo. La semplice regola anti-truffa elencata al primo punto del riquadro qui a fianco recepisce questo assunto. Ed è sufficiente a tenere alla larga buona parte degli aspiranti phisher. Senza contare che, sul web come nella vita quotidiana, chi ha in tasca una BankAmericard beneficia della tranquillità aggiuntiva dei **numerosi servizi di sicurezza**: dalle notifiche via Sms delle spese alla garanzia in caso di uso fraudolento, fino al servizio Fast Claim, per verificare gli addebiti dubbi direttamente dal portale [www.bankamericard.it](http://www.bankamericard.it).

## Cinque mosse per difendersi dalle frodi

**1 Non assecondare le richieste di codici segreti**, qualunque sia il pretesto e il mezzo con cui arrivano.

Per accedere alle aree riservate dei siti (come quella del portale BankAmericard), **non seguire il collegamento** che compare in una mail o in una pagina di internet, anche se appare corretto; digitare per esteso l’indirizzo (come [www.bankamericard.it](http://www.bankamericard.it)) nella finestra del programma di navigazione. Oppure memorizzarlo fra i segnalibri.

**3 Scaricare regolarmente gli aggiornamenti per il computer.** Con Windows, basta avviare “Windows Update” dal menu Start.

**Usare un programma antivirus.** Ce ne sono anche di gratuiti, come l’ottimo Avast che si scarica su [www.avast.com/ita/download-avast-home.html](http://www.avast.com/ita/download-avast-home.html)

**5** Se si è vittima di una frode, **fare denuncia** alla Polizia postale. Si può fare anche online, con un clic su [www.denunceviaweb.poliziadistato.it/polposta](http://www.denunceviaweb.poliziadistato.it/polposta).