

---

# PHISHING: per non abboccare.

---

## COSA È

Il **phishing**, termine coniato dalla storpiatura del vocabolo inglese "fishing" (pescare) associato a "phreaking" (una sorta di intrusione nei sistemi telefonici), è entrato nel vocabolario informatico per indicare una tecnica fraudolenta che punta principalmente ad ottenere i dati personali di clienti di banche, servizi finanziari e servizi on-line (codici, password, dati della carta di credito, ecc), convincendo l'utente a fornirglieli con falsi pretesti. Con la stessa tecnica è possibile ottenere a scopo fraudolento qualunque altro dato *sensibile* (dati relativi a origine razziale o etnica, religione, politica, filosofia, stato di salute, vita sessuale, ecc.).

## COME RICONOSCERE IL PHISHING

Un servizio di home banking, e-commerce, ecc. non chiederà mai i codici di accesso, numeri di carta di credito, codici bancomat o password inviando e-mail o lettere o telefonicamente. Chi gestisce questi servizi conosce bene quali sono i pericoli di furto dei dati dei propri utenti e non farà mai richieste del genere. Quindi **non rispondere a richieste di informazioni personali ricevute tramite posta elettronica, lettera o telefono**. Ma se ancora si avessero dubbi rivolgersi direttamente al fornitore del servizio per verificare l'attendibilità del messaggio ricevuto. Se oltretutto risultasse autentica la richiesta dei vostri dati per e-mail, dovrete allarmarvi sulla serietà di chi gestisce il servizio.

## PER NON ABBOCCARE

**Entrare nella pagina digitando l'indirizzo (url) direttamente nel browser** (Explorer, Netscape, Firefox, ecc.). Non accedere mai al sito di un servizio di home banking, e-commerce, sanitario, postale, INPS, ecc. che chiede di autenticarsi da un link inserito in un messaggio (e-mail, instant messaging,...) Anche se il link nella e-mail o la barra degli indirizzi Web risulta (apparentemente) corretto, non dimenticare che esistono delle tecniche, per mascherare l'indirizzo fasullo con uno corretto. Questi collegamenti potrebbero condurre la vittima a connettersi al sito pirata.

Non fidarsi ciecamente dei *perferiti* o *segnalibri*. Purtroppo potrebbe accadere anche che da una pagina apparentemente innoqua qualcuno possa avere modificato il vero indirizzo del servizio di home banking o del negozio online preferito con uno falso col quale rubare i dati di autenticazione. **Controllare sempre l'indirizzo sulla barra del browser**.

## SE SI CADE IN TRAPPOLA

Se per errore si sono inseriti i codici sulla pagina di un sito sospetto, **contattare immediatamente l'assistenza clienti** del servizio in questione. Se è possibile entrare nella pagina digitando l'indirizzo (url) direttamente nel browser internet (Explorer, Netscape, Firefox, ecc.) e **cambiare almeno la propria password**. Denunciare alle autorità eventuali usi illeciti delle proprie informazioni e notificare, eventuali sospetti relativi al furto d'identità.

**Polizia di Stato** [www.poliziadistato.it/pds/informatica/contatti.html](http://www.poliziadistato.it/pds/informatica/contatti.html)