

## Difendersi è facile

Bastano pochi, semplici accorgimenti per mettersi al riparo dai pirati informatici ed evitare le loro pericolose incursioni sul conto corrente on line o sulla carta di credito.

Un messaggio di posta elettronica apparentemente inviato dalla tua BCC, che chiede il numero della tua carta di credito o la parola chiave per accedere al tuo conto corrente elettronico, ti deve subito insospettire: la tua BCC, come ogni altra banca, non chiederebbe mai questi dati personali e riservati per posta elettronica.

Non rispondere mai a queste richieste e informa subito la tua BCC: contro questa difesa neanche il più temibile frodatore può fare niente.

# Phishing



## Non abboccare!

Con la tua BCC  
contro le truffe informatiche  
che colpiscono carte di credito  
e conti on line

## Phishing, phisher, e-mail, link, password... Piccolo vocabolario della sicurezza informatica

Le frodi informatiche chiamate "phishing" sono sempre più diffuse: colpiscono i titolari di conti correnti on line e carte di credito che navigano su internet ed hanno un indirizzo di posta elettronica, anche se possono avvenire pure via telefono fisso o cellulare.

Il phishing consiste nell'invio da parte di un truffatore informatico (phisher) di un messaggio di posta elettronica (e-mail) ad un gran numero di ignari utenti di internet.

Il messaggio di posta elettronica sembra in tutto e per tutto provenire dalla tua BCC: a volte riporta anche il marchio della BCC. In alcuni casi al suo interno c'è un allegato o il collegamento (link) a quello che appare proprio il sito internet della tua BCC.

Il truffatore tenta di conquistare la tua fiducia in vari modi: il messaggio può fare riferimento all'esigenza di cambiare la password, che si sostiene essere scaduta, oppure si indicano non meglio precisati "motivi tecnici" o ancora si adducono presunti problemi sul conto corrente che vanno risolti immediatamente. Il linguaggio quasi sempre è gentile, ci si scusa persino dell'incomodo,

in altri casi è più imperioso, si minaccia la sospensione del servizio on line in caso di mancata risposta.

Il vero cuore della frode è la richiesta di rispondere al messaggio – di aprire l'allegato o di collegarsi al link riportato in esso – scrivendo dati riservati inerenti al conto corrente o alla carta di credito. Ad esempio, le coordinate bancarie, la parola chiave (password) per accedere al proprio conto corrente on line, oppure il numero della carta di credito o un altro analogo codice segreto.



## Che vuol dire phishing


Phishing deriva da una deformazione del verbo inglese "to fish", ovvero "pescare". Si potrebbe tradurre con "gettare l'esca" ... per vedere chi abbocca.

Una volta venuto in possesso di queste delicate informazioni, il truffatore informatico potrà agire sul conto corrente o utilizzare la carta di credito, con grave danno per i clienti colpiti.

## Le regole d'oro anti phishing

**1. Non rispondere mai alle e-mail** che chiedono dati riservati. Già solo il dubbio che possa trattarsi di una truffa è sufficiente a sconsigliare l'invio di dati così importanti. Come detto, la tua BCC non te li richiederebbe mai via e-mail. Contattare subito la BCC per segnalare l'accaduto.

**2.** Se nel messaggio di posta elettronica c'è un allegato o il collegamento a quello che in apparenza è il sito internet della BCC, ma probabilmente è solo un sito internet contraffatto, **non aprire l'allegato e non cliccare sul link**. Per accertarti che il sito sia veramente quello della BCC, digita l'indirizzo internet della BCC manualmente sul programma di navigazione internet (browser).

**3.** Prima di digitare qualsiasi dato personale su internet, **verifica se il sito è garantito dal certificato di professione**: si tratta di un'icona che rappresenta un piccolo lucchetto giallo . Se pre-

sente, questo simbolo indica che il sito è protetto da un sistema di crittografia.

**4. Fai attivare** dalla tua BCC, ove possibile, un sistema di **avviso immediato dell'utilizzo** di carta di credito e bancomat. È il cosiddetto Sms alert, che consiste nell'invio automatico di un messaggio sul cellulare non appena la carta o il bancomat sono utilizzati.

**5.** Invia alle **competenti autorità di polizia** una segnalazione con il messaggio di phishing ricevuto.

**6.** Se pensi di aver subito una frode e rilevi una transazione non autorizzata, procedi immediatamente al **blocco della carta** e rivolgiti subito alla tua BCC. Se anche a seguito di una verifica effettuata con la tua BCC risulta confermata la frode a tuo danno, rivolgiti alle autorità di pubblica sicurezza competenti, che sono a tua disposizione 24 ore su 24, anche tramite un apposito sito internet, [www.commissariatodips.it](http://www.commissariatodips.it)