



**“Osservatorio Nazionale  
Permanente sulla Sicurezza” O.N.P.S.**

**Centro Studi e Ricerche  
www-onps.org**

## **Il Phishing**

**Dedicate 5 minuti per la Vs. sicurezza.**

**Alcune semplici regole per navigare ed utilizzare i servizi on line in sicurezza.**

**Con questo servizio intendiamo fornire ai ns. soci e visitatori alcuni consigli per essere maggiormente sicuri, relativi agli account ed alcune applicazioni gratuite per combattere il software dannoso.**

### **Innanzitutto: Che cos'è il Phishing:**

**È una rielaborazione di fishing, cioè pescare, attraverso un'e-mail fraudolenta che viene inviata a vari ignari destinatari**

Ci si riferisce all'atto del raccogliere dati privati del malcapitato di turno. Si spera che chi riceve le e-mail abbocchi, cliccando su qualche link non sicuro ma ben camuffato o inserisca la sua password in qualche form.

Nelle prime settimane di giugno del 2005, alcune Banche segnalavano casi di **mail fraudolente** che richiedevano ai loro clienti dati personali, in particolare i codici per accedere ai servizi on line.

Queste e-mail sono realizzate utilizzando il logo, il nome e il layout tipico della Banca imitata e invitano il destinatario a collegarsi tramite un link ad un sito Internet del tutto simile al quello della società e ad inserirvi, generalmente attraverso una finestra pop-up, le informazioni riservate quali codici d'accesso o altri dati personali.

Il phishing è una tipologia sempre più diffusa di spam che ha per obiettivo il furto dei dati personali: sensibili: numeri delle carte di credito o le password per l'Internet banking.

Negli attacchi di phishing l'artefice della truffa invia delle e-mail da "mittenti falsificati", le quali sembrano provenire da un sito web legittimo con il quale il destinatario intrattiene regolari rapporti, per esempio la propria banca, la società che ha emesso la carta di credito o il provider Internet, e per accedere al quale gli utenti necessitano di un account personale. Il messaggio e-mail potrebbe richiedere al destinatario di rispondere fornendo i propri dati personali al fine di "aggiornarli", o per altre ragioni.

L'e-mail fraudolenta potrebbe anche reindirizzare l'utente in un sito web fasullo o in una finestra a comparsa identica al sito web legittimo, creata ad hoc per sottrarre informazioni personali dell'utente.

Le ignare vittime vengono quindi spesso indotte con l'inganno a fornire il proprio numero di carta di credito, le password o altri dati sensibili.

Vista la diffusione del phishing vi invitiamo a tenere conto di questi pochi semplici accorgimenti per tutelarvi da possibili frodi informatiche

### **Segnalazioni di sospetto phishing**

Se avete ricevuto una e-mail fraudolenta, vi **invitiamo a contattare subito la vs. Banca o Posta e, se desiderate comunque segnalarci il problema** potete inviarci una e-mail al seguente indirizzo: [info@onps.org](mailto:info@onps.org)

### **Come avviene un attacco di phishing**

**Innanzitutto ricordate che la vostra Banca o La Posta non hanno alcun motivo di richiedervi l'invio, via e-mail, di informazioni personali, in quanto le ha già ed userebbe il canale che solitamente usa, della comunicazione o convocazione tramite posta riservata:**

- password per intero
- nome e cognome
- numero della carta di credito
- numero del conto bancari

**Alcune indicazioni per difendersi dal phishing Controllate sempre l'indirizzo del sito della vs. Banca o Posta**

1) Accedete ai servizi dispositivi della vs. Banca o della Posta sempre e solo digitando direttamente l'indirizzo della banca nella barra degli indirizzi del browser (esempio MS Explorer, Netscape, ecc.).

2) Non inserire i codici di accesso al sito della vs. Banca o della Posta da un link inserito in un messaggio (posta elettronica, instant messaging,...).

3) Non inserite i codici di accesso al sito della vs. Banca o della Posta da un link inserito in un sito terzo.

4) Verificate il certificato di protezione del sito: ogni sezione del sito della vs. Banca o della Posta è protetto da un certificato (visibile accedendo sull'icona a forma di lucchetto in basso a destra nella finestra vostro browser che garantisce, oltre alla riservatezza delle informazioni scambiate, anche l'identità del sito.

Attendete quindi la conferma della Vs. Banca o Posta che siete effettivamente collegati con loro.

**Chiedete sempre comunque, in dettaglio, alla vs. Banca o Posta quali sistemi di sicurezza contro il phishing hanno adottato per garantire maggiore sicurezza ai propri clienti.**

**Sede operativa:** 00142 Roma Via Badia di Cava,36 - Fax 067911292 Cell. 3357356664

E-mail: [info@onps.org](mailto:info@onps.org) . Sito Internet: [www.onps.org](http://www.onps.org)

**Sedi Territoriali:** Napoli . Padova . Torino - Palermo . Vibo Valentia . Bari . Milano.