

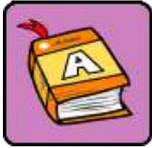


IDENTITÀ E FRODI

I RISCHI CONNESSI AL FURTO DI IDENTITÀ
IN INTERNET
PHISHING, PHARMING E I MODI
PER DIFENDERSI

Di cosa parleremo

- ➔ Il **furto d'identità**: caratteristiche e rischi concreti.
- ➔ Cos'è il **phishing**.
- ➔ Cos'è il **pharming**.
- ➔ Come **difendersi** dal furto d'identità.
- ➔ Come **documentarsi**.



Cos'è il furto d'identità

- ➔ Il **furto d'identità** è un reato finanziario: i ladri si fingono le vittime appropriandosi di informazioni personali importanti come numeri della previdenza sociale, numeri della patente, indirizzi, numeri di carte di credito e di conti correnti.

- ➔ Il furto d'identità avviene fondamentalmente attraverso strumenti informatici e sottraggono agli utenti informazioni personali, quali ad esempio:
 - identificativo di un account
 - password
 - numeri di carta di credito
 - ...



Come viene attuato il furto d'identità

- ➔ Con la diffusione della **posta elettronica** e del **Web** e l'aumento dei sistemi di pagamento **on line**, gli autori dei furti di identità hanno adottato nuove tecniche e nel mondo virtuale possiamo constatare l'esistenza di numerosi tipi di attacchi che hanno ripercussioni nel mondo reale, in particolare:
- il **phishing**
 - il **pharming**



Cos'è il phishing

- ➔ Il **phishing** (possiamo tradurre in italiano il termine con "abboccamento") viene messo in atto da un utente malintenzionato che invia false e-mail che sembrano provenire da siti Web noti o fidati, come il sito della propria banca o della società di emissione della carta di credito.
- ➔ Le false e-mail e i siti Web in cui l'utente viene indirizzato sembrano sufficientemente ufficiali da trarre in inganno sulla loro autenticità. Ritenendo queste e-mail attendibili, gli utenti spesso rispondono ingenuamente a richieste di "verifica" o "messa in sicurezza" dell'accesso alla propria banca on line, o alla richiesta di singoli dati per completare un account (data di nascita, Comune di nascita, tessera sanitaria...).



Cos'è il pharming

- ➔ Il **pharming** è una forma di **phishing avanzato** che altera la connessione Internet e fa sì che, ogni volta che gli utenti cercano di connettersi al sito ufficiale di un'azienda, anche se digitano l'indirizzo corretto, vengono segretamente dirottati su un sito apparentemente autentico, ma che di fatto è un sito **contraffatto**.
- ➔ Una volta all'interno di uno di questi siti falsificati, è possibile immettere involontariamente informazioni personali trasmesse direttamente all'autore del sito, che le utilizzerà per acquistare prodotti, richiedere una nuova carta o rubare l'identità del malcapitato.



I rischi concreti

Elenchiamo solo alcuni dei possibili rischi concreti connessi al furto d'identità:

- ➔ perdere la propria identità e quindi farsi sottrarre parte del conto in banca;
- ➔ perdere importanti dati personali su siti o su piattaforme che usiamo per lavoro;
- ➔ impossibilità di concludere una transazione o un'attività.



Precauzioni generali

Teniamo a mente alcune semplici norme di buon senso:

- ➔ i "dati personali" devono restare tali sia nella vita reale sia nel Web;
- ➔ custodire nickname, password e numeri di accesso in luoghi sicuri, e fra loro separati;
- ➔ distruggere estratti conto, carte di credito o tessere scaduti: da questi i ladri di identità potrebbero trarre informazioni preziose;
- ➔ denunciare smarrimento o furto di tali documenti con sollecitudine.



Precauzioni sul Web

Per le **e-mail**:

- ➔ Mai aderire a richieste di dati riservati: cestinare l'e-mail senza esitazione!
- ➔ Mai seguire i link nelle e-mail: eventualmente posizionarvi il mouse sopra, per verificarli nell'etichetta gialla che appare o nella barra di stato.



Precauzioni sul Web

- ➔ Instant messaging, profili web, chat possono offrire ghiotte occasioni agli usurpatori di identità! Usare "nick" generici e non fornire dati personali a nessuno.
- ➔ Utilizzare **browser aggiornati**: aiuta a riconoscere i siti fasulli.
- ➔ Utilizzare il **firewall**: permette di evitare le occasioni di intrusione e di proteggere i dati immagazzinati nei file del tuo PC.
- ➔ Verificare sempre la **sicurezza** di un **sito Web**.



Precauzioni sul Web

Quando si forniscono dati personali a un sito Web commerciale o al sito di una banca occorre verificare la presenza di segnali che ne garantiscano la sicurezza:

- ➔ l'icona di un **lucchetto** sulla barra di stato del browser;
- ➔ un URL che inizi con "**https://**" (la "s" vuol dire "sicuro").

Questi segnali non garantiscono però una certezza del 100%, perché tutte le icone di sicurezza possono essere falsificate.



Alcuni dati

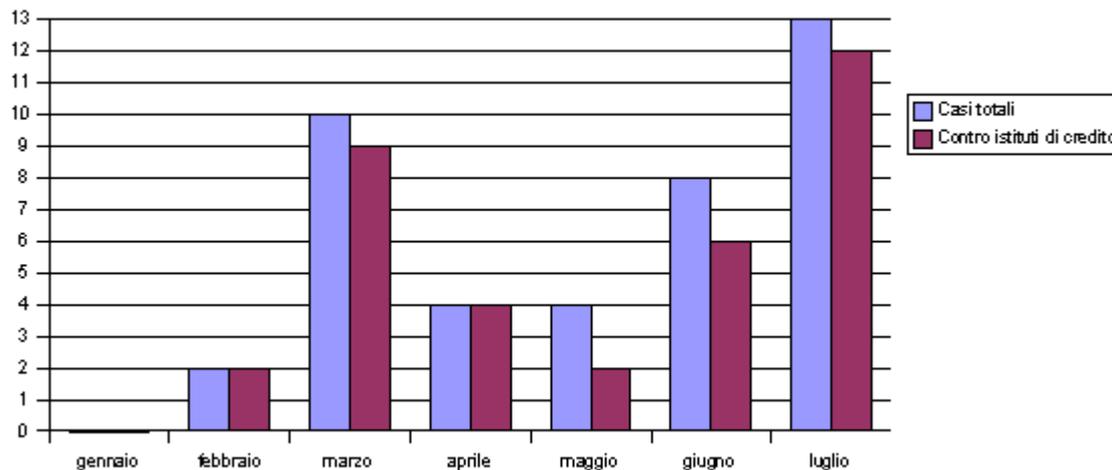
Il furto d'identità negli USA

- Il fenomeno del furto d'identità, secondo le stime della FTC (*Federal Trade Commission*, un organo governativo preposto alla tutela dei consumatori americani), soltanto nel 2003 ha portato a quasi **215.000** furti.
- Gli Stati Uniti sono stati i primi a dotarsi di una legislazione specifica contro il furto digitale d'identità, con l'*Identity Theft Penalty Enhancement Act*, varato nel 2004.



Alcuni dati Il phishing in Italia

Casi di phishing contro obiettivi italiani - Anno 2006



Fonte: Anti-Phishing Italia - www.anti-phishing.it



Documentiamoci

- ➔ Microsoft dà numerosi consigli per non incappare nelle truffe e nel furto di identità.
<http://www.microsoft.com/italy/athome/security/email/phishing.mspix>
<http://www.microsoft.com/italy/mscorp/twc/privacy/default.mspx>
- ➔ Sito specializzato, ricco di notizie sul fenomeno del phishing.
<http://www.anti-phishing.it/>
- ➔ Attenzione alle truffe, ma anche agli allarmi eccessivi: sembrano più pericolose le truffe reali di quelle on line!
<http://www.apogeeonline.com/webzine/2005/02/21/01/200502210101>



Documentiamoci

- ➔ È possibile sfruttare Internet per farsi una cultura sui problemi relativi all'identità personale. Ad esempio, proviamo a cercare in un motore di ricerca questi termini:
 - Identità e persona
 - Identità multiple
 - Identità europea
 - Multiculturalità e identità

- ➔ Può essere istruttivo anche condurre una ricerca sui termini **ingegneria sociale** - "social engineering" - evidenziando le implicazioni per il nostro tema:
 - fingere identità **false** per impossessarsi di identità **vere**;
 - conoscere i fatti degli altri per sfruttarne i comportamenti.



Link utili

- ➔ <http://www.sicuramenteweb.it/>
- ➔ <http://www.ilwebperamico.it/>
- ➔ <http://www.poliziadistato.it/pds/informatica/>
- ➔ http://www.commissariatodips.it/stanze.php?st_rparent=10
- ➔ <http://www.lionsinterneteminori.org/default.asp>
- ➔ <http://www.ilfiltro.it/>