ADICONSUM
Associazione Difesa Consumatori e Ambiente
promossa dalla CISL

GERI HDP

Guida al Furto d'Identità

Informativa per il Consumatore sui rischi e le tutele da adottare a difesa dei propri dati personali

Premessa

Il furto d'identità è un reato subdolo e sconosciuto.

Subdolo perché difficile da combattere e, in alcune forme, anche particolarmente difficile da prevenire.

Sconosciuto perché è ancora troppo scarsa l'informazione in merito, spesso limitata al phishing, che rappresenta solo una delle possibili forme in cui può manifestarsi il furto d'identità.

L'Italia è un paese molto esposto; secondo gli ultimi dati disponibili (CRIF), nel nostro Paese si sono verificati oltre 25.000 casi di furto d'identità, per un valore complessivo di oltre 200 milioni di euro.

Nel corso degli ultimi anni sono state adottate nuove misure di prevenzione rispetto alle frodi d'identità. Lo stesso sistema bancario ha incrementato i presidi di sicurezza attraverso l'utilizzo dei cosiddetti "alert". Pur tuttavia, molto ancora deve essere fatto a tutela del consumatore, al quale troppo spesso viene attribuito ogni tipo di responsabilità, come ad esempio: non aver conservato correttamente la carta, aver aperto una mail potenzialmente pericolosa, aver cestinato senza prima distruggerli documenti contenenti dati sensibili, ecc.

Fondamentale in tal senso è la collaborazione internazionale tra Forze di Polizia, trattandosi spesso di reati transnazionali, nonché l'aggiornamento del Codice Penale, che ancora non prevede molti dei reati che vengono quotidianamente compiuti in rete.

Si tratta di un percorso difficile, perché l'ingegnosità dei criminali è enorme, ed è conseguentemente impossibile prevederne con esattezza le mosse; tuttavia, se la lotta al furto d'identità e ai reati informatici sarà posta in primo piano, sarà possibile ricondurre il fenomeno quantomeno ad un livello "fisiologico", con significativi vantaggi per tutti, imprese e consumatori.

Vista l'importanza sempre maggiore del fenomeno, nell'ottica di adoperarsi per poter fornire un'opportuna e adeguata informazione a tutela del consumatore, nonché di denunciare quanto ancora non funziona in modo corretto, Adiconsum e Geri hanno concordato, nell'ambito delle attività previste dall'Accordo siglato, di realizzare un'informazione condivisa, nonché di creare un Osservatorio congiunto sul credito, in grado anche di monitorare criticità e specifici fenomeni.

Le forme del furto d'identità

La normativa definisce il furto d'identità (*Id-theft*) come una condotta criminale attuata attraverso l'impersonificazione totale (in altre parole, "l'occultamento totale della propria identità mediante l'utilizzo indebito di dati concernenti l'identità e il reddito di un altro soggetto" che può "riguardare l'utilizzo indebito di dati riferibili sia a un soggetto in vita che a uno deceduto") oppure attraverso l'impersonificazione parziale (in altre parole "l'occultamento parziale della propria identità" attraverso

"l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi a un altro soggetto").

In linea generale, si verifica un furto d'identità ogni qualvolta un'informazione individuale, relativa a una persona fisica o a un'impresa, è ottenuta in modo fraudolento da un criminale, il quale agisce con l'intento di assumerne l'identità altrui per compiere atti illeciti.

Il furto d'identità provoca alla vittima sia un danno economico/finanziario sia un danno morale/psicologico, correlato allo stress emotivo causato dalla sensazione di impotenza, che a sua volta genera rabbia e paura, nonché un danno "per sacrificio di tempo libero", ovvero l'impegno di tempo ed energie necessari per risolvere i problemi scaturiti dalla frode (ad esempio, la necessità di dover ricostruire il proprio profilo digitale).

Il furto d'identità può colpire anche le imprese, con conseguenze non solo economiche, ma anche reputazionali (basti pensare alla possibilità che il truffatore offra beni e servizi di livello inferiore agli standard dell'impresa cui è stata rubata l'identità).

Le imprese, inoltre, hanno anche il diritto-dovere di tutelare, oltre a sé stesse, i propri dipendenti, clienti e fornitori.

Per questo motivo sono tenute ad adottare particolari misure di sicurezza a tutela delle proprie informazioni aziendali (ad es., elenco clienti), in primo luogo attraverso una corretta gestione e archiviazione dei documenti. E' inoltre fondamentale la corretta conservazione degli stessi e la distruzione dei documenti che riportano dati sensibili propri o di terzi.

L'impresa è responsabile, civilmente e penalmente, per i danni causati a terzi in caso di trattamento non corretto dei dati sensibili. In proposito è importante ricordare che in tema di trattamento dei dati è prevista l'inversione dell'onere della prova (art. 2050 c.c.): ciò significa che è il responsabile del trattamento dei dati che deve dimostrare di avere gestito correttamente i dati stessi, pena l'irrogazione di sanzioni, anche pesanti.

Per evitare di incorrere in rischi del genere, lo strumento più adatto è la previsione di una corretta formazione dei dipendenti dell'impresa, in modo tale da informarli adeguatamente sui possibili rischi e sulle modalità con le quali il furto d'identità e le altre tipologie di frode possono verificarsi, nonché sui rimedi da adottare.

Infine, come per qualsiasi altro soggetto, anche per le imprese è fondamentale utilizzare un sistema informativo dotato di adeguate misure di prevenzione e costantemente aggiornato.

Le tipologie di frode

Le diverse tipologie di frode d'identità sono:

Identity Cloning: clonazione dell'identità, ossia la sostituzione di una persona con l'obiettivo di creare una nuova identità e una nuova vita;

Financial Identity Theft: furto dell'identità allo scopo di utilizzare i dati identificativi di un individuo o di un'impresa per ottenere crediti, prestiti finanziari, aprire conti correnti in nome della vittima;

Criminal Identity Theft: uso dei dati della vittima per compiere, in sua vece, atti pubblici illeciti di varia natura (ad es., attivazione di nuove carte di credito);

Synthetic Identity Theft: uso dei dati personali di soggetti diversi, combinati per costruire "in laboratorio", completamente o parzialmente, una nuova identità in base alle proprie necessità;

Medical Identity Theft: avvalersi dei dati personali altrui per ottenere prestazioni sanitarie;

Gosthing: costruzione di una nuova identità, diversa da quella originaria, appropriandosi dei dati di una persona defunta;

Cyber Bullismo - Impersonation: impersonificazione, tramite cellulari o servizi web 2.0, in una persona diversa, allo scopo di inviare messaggi e/o testi, dal contenuto solitamente reprensibile.

Tutte le forme di furto d'identità sono possibili attraverso determinate modalità:

Skimming: clonazione di una carta di credito, attraverso un'apparecchiatura elettronica, durante l'uso in un esercizio commerciale o in occasione di un prelievo di denaro presso uno sportello elettronico (Atm); l'apparecchiatura consente di conoscere tutti i dati necessari e di utilizzare la carta senza necessità di appropriarsi interamente dell'identità della vittima. Il kit di montaggio dello *skimmer* (apparecchiatura elettronica che immagazzina i dati contenuti nella banda magnetica del bancomat, per memorizzarne il pin) può addirittura essere acquistato in internet;

Siti internet: richiesta di fornire informazioni personali durante la navigazione in internet per accedere a determinati siti e per acquistare beni; spesso tali informazioni viaggiano sulla rete in chiaro e non in modalità protetta;

Phishing: furto via posta elettronica. L'organizzazione criminale invia una mail dichiarando di essere un incaricato e/o di appartenere a enti/società/organizzazioni con le quali, plausibilmente, può esservi un rapporto, inducendo la vittima a fornire informazioni personali. Normalmente la mail contiene la richiesta di utilizzare un determinato link per accedere ai dettagli del proprio conto, adducendo esigenze di sicurezza; cliccando sul link l'utente sarà reindirizzato in un sito web parallelo e fraudolento. In tal modo i criminali riescono ad utilizzare i dati inseriti nel sito fittizio per prelevare denaro dai conti correnti delle vittime, o per effettuare acquisti o transazioni a loro nome;

Vishing o voice phishing: si tratta di un'evoluzione del phishing. Il primo contatto avviene via mail, chat o sms; in questo caso non si chiede di cliccare su un link, bensì di contattare un (falso) recapito telefonico dell'istituto di credito, al quale normalmente risponde un disco o un finto operatore del call center, il

quale chiede alla vittima la comunicazione dei dati per accedere al conto corrente;

Spamming: nato come nuova forma pubblicitaria, è spesso sfruttato per indurre a cliccare su link o scaricare file che, all'insaputa dell'utente, installano automaticamente sul pc collegato software malevoli;

Keylogging: è uno strumento che infetta il computer con un malware, senza danneggiare i programmi, ma intercettando quanto viene digitato sulla tastiera, in particolar modo le password. Il keylogger hardware è installato tra la tastiera e il pc, e ha le sembianze di un adattatore o di un semplice cavo (ne esistono tuttavia anche di invisibili, inseriti nella tastiera);

Spoofing: tecnica basata sull'utilizzo della posta elettronica (e-mail mime spoofing) di ignari cybernauti;

Pharming: connessione telematica reindirizzata su un sito clone di quello dell'istituto di credito, attraverso il quale vengono rubate le chiavi di accesso al conto on line di un cliente dell'intermediario. Il furto avviene inserendo nel computer un virus che modifica la lista dei siti "preferiti" presente nel browser del cybernauta. Una forma di difesa fondamentale consiste nel non inserire tra i siti preferiti l'indirizzo internet utilizzato per collegarsi al sito della propria banca senza dover impostare ogni volta la password;

Sniffing: attività di monitoraggio e intercettazione dei pacchetti di dati che transitano in una rete telematica. È utilizzata non solo per il monitoraggio della rete da parte dei sistemisti (attività lecita), ma anche per l'acquisizione di account, password e qualsiasi altro tipo di dato sensibile (attività illecita);

Download di video, brani musicali e foto da siti web dei quali non si conosce la natura: all'interno di presunti brani o video musicali possono nascondersi programmi che, una volta nel computer, si espandono e prendono possesso del contenuto dello stesso. Il criminale, introducendosi nel computer, avrà libero accesso a qualsiasi dato che riguardi l'utente;

Trashing o bin raiding: utilizzo dei dati personali di una persona, "rubando" dalla sua spazzatura la documentazione personale buttata via (ricevute, bollette, estratti conto, documenti assicurativi, lettere personali, ecc.), spesso contenente dati riservati come codice fiscale o numero di conto corrente, la quale non sia stata prima resa illeggibile, tagliuzzandola o utilizzando una macchina distruggi documenti;

Dumpster diving: si tratta di un'evoluzione del trashing, consistente nel "furto" di quanto viene gettato nei cassonetti e nelle discariche;

Indirizzo di posta: i criminali sono in grado di recuperare le informazioni personali della vittima in caso di trasferimento di residenza, laddove questa dimentichi di comunicare la variazione del proprio indirizzo alle Poste Italiane;

Furto: vengono sottratti dalla borsa o dal portafoglio della vittima bancomat, carte di credito e documenti di identità quali ad esempio la patente di guida o le tessere di iscrizione a partiti e associazioni. La vittima, seppure si accorge relativamente presto di essere stata derubata, spesso realizza troppo tardi il valore effettivo delle informazioni contenute nel bene sottratto;

Contatti indesiderati: il criminale prende contatto con la vittima, presentandosi in nome dell'istituto di credito o dell'azienda con la quale la stessa intrattiene rapporti di tipo commerciale. E' importante fare molta attenzione nel comunicare le proprie informazioni personali, ed è inoltre opportuno recarsi di persona presso la sede dell'organizzazione dalla quale si dovessero ricevere determinate richieste, in modo tale da essere certi di non cadere nella trappola dei criminali.

Come avvengono il furto di identità e la frode informatica

Le modalità con cui avviene il furto di identità si possono suddividere in due macro categorie:

1) sottrazione di denaro (90% del totale dei casi di furto d'identità);
2) danneggiamento della reputazione della persona.

Un sistema sperimentato di "furto" è rappresentato dall'offerta su internet o sui social network di posti di lavoro, piuttosto che di condizioni particolarmente vantaggiose per l'apertura di conti correnti, così come di altre offerte (apparentemente) remunerative, a condizione di fornire i propri dati identificativi. Spesso è sufficiente l'indicazione di nome e data di nascita, del proprio posto di lavoro o di altre informazioni (ritenute innocue) sulla propria famiglia, per consentire ai truffatori di ricostruire il profilo personale della vittima e di sostituirsi ad essa con nuovi documenti di identità, arrivando perfino a saccheggiarle il conto in banca.

Particolare attenzione va inoltre posta nell'utilizzo dei telefoni cellulari e del wi-fi, che rendono ancora più semplice "attaccare" i pc degli ignari internauti.

Una volta compiuto il furto, i criminali, con la nuova identità, possono aprire un conto corrente bancario, emettere assegni contraffatti fino a prosciugare il conto della vittima, acquistare auto, elettrodomestici e altri beni di consumo, anche a rate, oppure scrivere alla filiale di banca e modificare le coordinate bancarie. Gli estratti conto saranno quindi inviati al nuovo indirizzo, rendendo difficile scoprire il reato che si sta perpetrando con l'identità della vittima, la quale sarà poi l'unica a pagare.

Legislazione

La lotta al furto d'identità e alle frodi informatiche si interrompe in assenza di una normativa specifica.

Il primo aspetto importante riguarda la querela sporta da parte del soggetto che subisce il furto d'identità, chiave di accesso per contrastare il reato: il giudice, infatti, non può agire d'iniziativa propria.

La legislazione sul furto d'identità e sulle frodi informatiche si limita a:

Codice Penale, art. 494, impersonificazione (sostituzione di persona), pena massima un anno;
Decreto legislativo n. 231/2007, art. 55.9, di recepimento della Direttiva europea 2005/60/CE;
Codice della Privacy (D.lgs. n. 196/2003, art. 1), che prevede che i dati personali sono diritti inviolabili;
Legge 15 febbraio 2012, n. 12, "Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica", relativa alla confisca e alla destinazione dei beni informatici o telematici utilizzati per la commissione di reati informatici.

In ragione della scarsità di fonti normative, nonché in assenza di riferimenti specifici, frequentemente la Magistratura si è vista costretta a dover ricondurre la fattispecie del furto d'identità ad altre tipologie di reati, quali: diffamazione (art. 595 c.p.), falsità materiale in scrittura privata (art. 485 c.p.) o sostituzione di persona (art. 494 c.p.).

La mancanza di una normativa specifica crea poi posizioni paradossali per cui, ad esempio, ai sensi dell'art. 485 (falsità in scrittura privata), chi falsifica un cedolino di assicurazione è punito a seguito di querela dell'assicurazione frodata, mentre chi inventa il nome di un'assicurazione e si autoproduce un cedolino non è invece sanzionabile, dal momento che, non esistendo la compagnia, non esiste chi può sporgere querela.

In altri Paesi quali la Gran Bretagna, solo per citare un esempio, il *Fraud Act* del 2006 descrive con precisione il reato di frode.

La legislazione manca inoltre di coordinamento internazionale. Avanzare una rogatoria internazionale è una questione che può durare mesi, a fronte di un reato che invece può essere realizzato, senza peraltro lasciare più traccia, in tempi molto rapidi.

Si stanno invece facendo alcuni passi in avanti sotto il profilo della prevenzione dei reati.

Le leggi dedicano particolare attenzione al furto di identità per evitare le frodi nel settore del credito al consumo, uno dei più colpiti.

È pienamente operativa la banca dati sulle carte di credito, che offre un diverso approccio da parte delle banche nelle convenzioni, nei rapporti con i dealer e la rete. La norma prevede l'istituzione, presso l'Ucamp (Ufficio centrale antifrode mezzi di pagamento) del Ministero dell'Economia, di un archivio informatico per rafforzare la sicurezza del circuito di utilizzo dei mezzi di pagamento informatici, e l'espulsione dal circuito stesso degli esercenti che accettano mezzi di pagamento clonati o contraffatti.

Una protezione per tutti i cittadini utilizzatori di carte di credito e mezzi di pagamento analoghi.

Per evitare tali avvenimenti è stato inoltre creato, presso il Ministero dell'Economia e delle Finanze, un archivio unico (D.lgs. n. 141/2010 – V-bis – Credito al consumo – "Sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore creditizio").

L'archivio consente di verificare l'identità dei cittadini attraverso i seguenti documenti:

- documenti d'identità e di riconoscimento, comunque denominati o equipollenti, anche se smarriti o rubati, rilasciati dal Ministero dell'Interno;
- le informazioni sulle partite iva;
- il codice fiscale;
- i documenti relativi al reddito dei cittadini, trattati dall'Agenzia delle Entrate;
- le posizioni contributive, previdenziali e assistenziali, gestite dai vari Enti previdenziali.

Al sistema di prevenzione possono aderire le banche, gli intermediari finanziari, i fornitori di servizi di comunicazione elettronica e i fornitori di servizi interattivi, i gestori di sistemi di informazioni creditizie e le imprese che già offrono servizi assimilabili alla prevenzione.

Tutela

La prima difesa contro il furto di identità è l'autotutela del consumatore.

In molti casi vengono inseriti sui social network i propri dati personali, consentendo alla criminalità di utilizzarli, oppure si gettano documenti, anche importanti (ad es., la dichiarazione dei redditi), senza averli prima distrutti, rendendo semplice per i criminali ricostruire tutte le informazioni relative alle persona che sarà poi frodata, oppure, ai fini di ottenere una tessera sconto, si rilasciano i propri dati identificativi, pur non essendo assolutamente obbligatorio.

Per quanto riguarda l'utilizzo del pc, la prima difesa possibile è la navigazione solo su siti sicuri; è poi necessario curare l'aggiornamento continuo degli antivirus e utilizzare firewall hardware o software; fondamentale è inoltre non aprire in automatico le mail, neppure le anteprime, né inserire i propri dati personali o partecipare a catene di Sant'Antonio inoltrate via mail.

Nell'ambito dell'autotutela è opportuno conservare in casa o, comunque, in un luogo sicuro, una fotocopia di tutti i documenti personali, quali il passaporto, la patente di guida, il porto d'armi, il tesserino professionale, ecc.; non conservare tutti i documenti d'identità nello stesso posto, specialmente se si è in viaggio, quando è anche inutile portarli tutti con sé. Mai comunicare i propri dati se non si è sicuri di fornirli ad una persona affidabile e, qualora siano richiesti, ad esempio, dalla società emittente la carta di credito o da un fornitore, verificare l'attendibilità della fonte contattando telefonicamente la società.

È importante fare attenzione alla ricezione degli estratti conto e delle bollette delle utenze; è necessario contattare immediatamente la banca o la società di servizio se non si riceve regolarmente l'estratto conto o la bolletta (un estratto conto o una bolletta mancante possono significare che un frodatore è venuto a conoscenza del conto della carta di credito o di altri dati personali, modificando la residenza della vittima).

Inoltre, mai lasciare incustodite giacca o borsa contenenti il portafoglio o i documenti. I criminali sono veloci e possono essere anche persone apparentemente insospettabili, perfino, ad esempio, i colleghi della stanza accanto.

Nel caso di spedizione di documenti personali è poi opportuno scegliere il mezzo più sicuro, piuttosto che quello più economico.

E' importante utilizzare password e codici pin diversi e non facilmente decifrabili. Gli stessi siti internet, ormai, indicano se la password prescelta ha un livello di sicurezza basso, medio o alto. Password e pin vanno memorizzati, piuttosto che scritti, e non vanno mai comunicati a nessuno.

Se l'autotutela non è sufficiente, anche in caso di semplice sospetto di essere stati vittima di furto di identità, è **essenziale**:

attivare i filtri di protezione della privacy;

verificare se l'utilizzo di internet è stato effettuato secondo le modalità sicure sopra descritte;

bloccare ogni sistema di pagamento (carte di credito) utilizzato sul web.

Quando il furto d'identità sia accertato, è **indispensabile:**

bloccare immediatamente ogni mezzo di pagamento (bancomat, carta di credito, conto corrente), e farsi rilasciare dalla banca numero e ora del blocco;

presentare denuncia circostanziata alle Autorità, possibilmente alla Polizia Postale (www.poliziapostale.it) e alla Guardia di Finanza (www.gat.gdf.it). La denuncia può essere presentata anche attraverso il commissariato virtuale della pubblica sicurezza: attraverso tale mezzo i cittadini possono denunciare immediatamente un comportamento illecito subìto, oltre che segnalare fenomeni sospetti in cui ci si dovesse essere imbattuti navigando in rete. Sempre attraverso il commissariato virtuale, è inoltre possibile ottenere informazioni sulle questioni più spinose o controverse del mondo di internet;

con riguardo ai minori, le segnalazioni e tutte le altre attività necessarie devono essere effettuate a cura di chi esercita la patria potestà dell'utente.

E' **opportuno** inoltre segnalare i fatti a:

Autorità Garante per la Protezione dei dati personali (www.garanteprivacy.it);

Autorità delle Comunicazioni (www.agcom.it);

Associazione dei consumatori (www.adiconsum.it).

Le iniziative del sistema bancario

Per combattere le frodi e rendere più sicuro l'utilizzo delle carte di credito, i vari intermediari creditizi e finanziari e gli emittenti di carte di credito (IMEL), hanno previsto alcuni servizi utili per i possessori delle carte di credito.

CartaSi, ad esempio, ha previsto l'invio all'utente di un Sms che comunica l'importo speso e l'esercizio commerciale presso il quale è stato effettuato l'acquisto; se il reale possessore della carta non si riconosce in tali informazioni, è sufficiente chiamare il numero verde 800.15.16.16, per bloccare immediatamente la transazione, evitando così l'addebito in estratto conto. Il servizio è totalmente gratuito.

Visa utilizza il sistema di protezione "Verified by Visa". Il servizio è gratuito, e prevede l'abbinamento alla carta di credito di una password da utilizzare ogni volta che si deve effettuare un acquisto on line.

Mastercard utilizza invece il sistema "SecureCode MasterCard". La procedura è sostanzialmente identica a quella di Visa.

Sono iniziative importanti, che tuttavia non possono sostituire un'informazione dettagliata sui comportamenti da adottare per proteggersi, la quale deve sempre essere fornita prima della sottoscrizione per il rilascio della carta di credito o di debito.

Frodi informatiche

Molte frodi informatiche avvengono attraverso le carte di credito e di debito.

Il rischio di frode si ha durante tutto il ciclo di vita di una carta di credito: richiesta (furto 'identità), produzione (frode interna), invio (intercettazione), utilizzo (clonazione).

E' comunque possibile adottare alcuni accorgimenti per difendersi.

Spesso, ma non sempre, le carte di pagamento false possono essere riconosciute da disordini e imperfezioni nei particolari grafici, dall'illeggibilità di microscritture riprodotte attraverso "scannerizzazioni" e dall'assenza di iscrizioni e loghi grafici luminescenti, visibili, nelle carte autentiche, soltanto attraverso l'esposizione alla luce ultravioletta.

Per evitare possibili frodi è utile, prima di utilizzare l'Atm, controllare che i componenti dello sportello siano ben saldi, e attivare il servizio sms alert, offerto ormai da quasi tutti i principali circuiti.

Per quanto riguarda i Pos, è fondamentale che gli esercenti verifichino frequentemente l'integrità dei sigilli di sicurezza, perché è soltanto manomettendoli che è possibile procedere alla clonazione delle carte.

Sempre per i pagamenti a mezzo Pos, è importante non perdere mai di vista la propria carta, evitando, ad esempio, che l'esercente la porti via insieme al conto da pagare o, addirittura, vada nel retrobottega per "strisciare" la carta stessa.

Per evitare frodi on line è necessario fare attenzione, oltre ai sistemi di pagamento, anche ai prodotti acquistati, spesso non conformi a quanto pubblicizzato, se non addirittura "taroccati"; per questo è importante navigare sempre e soltanto su siti sicuri.

Dieci regole per difendersi dallo spam e dai furti di identità

1. **Usare un software antivirus e tenerlo sempre aggiornato.** E' importante disporre di un sistema in grado di aggiornare il computer tempestivamente e regolarmente: il malware può diffondersi con estrema rapidità. Inoltre, vanno installati regolarmente gli aggiornamenti del sistema operativo utilizzato, in modo da poter evitare eventuali vulnerabilità che possono esporre il pc al pericolo di attacchi di virus.
2. **Non effettuare mai acquisti suggeriti da mail non richieste.** Il pericolo è di veder inserito il proprio indirizzo mail in liste che vengono poi vendute agli spammer,

con il duplice svantaggio di ricevere ulteriori mail spazzatura e di aumentare il rischio di finire vittime di frodi.

3. **Utilizzare un client firewall sui computer collegati a internet.** Un client firewall protegge i computer collegati con il mondo esterno; anche chi utilizza un portatile e/o lavora da casa, quindi, ha bisogno di una protezione firewall.
4. **Non rispondere allo spam e ignorare i link contenuti nelle mail.** Rispondere ai messaggi spam, anche semplicemente per cancellare l'abbonamento alla mailing list, non fa altro che confermare la validità dell'indirizzo mail allo spammer, che spedirà di conseguenza una maggiore quantità di messaggi.
5. **Non usare la modalità anteprima nel client di posta.** L'opzione "anteprima" apre il messaggio e comunica agli spammer che la loro mail è andata a buon fine. Quando si controlla la posta, è possibile capire, anche solo in base all'oggetto e al mittente, se si tratta o meno di un messaggio spazzatura.
6. **Utilizzare indirizzi secondari e fornirli solo a persone fidate.** Si consiglia di comunicare il proprio indirizzo principale solo ad amici e colleghi, e di utilizzare gli indirizzi secondari per i moduli web. Non pubblicare mai il proprio indirizzo principale su forum, newsgroup o altri siti pubblici. Gli spammer potrebbero facilmente intercettarli con l'utilizzo di programmi che navigano in internet alla ricerca di indirizzi mail.
7. **Non rispondere mai ai messaggi che chiedono informazioni finanziarie personali.** Diffidate delle mail che richiedono di inserire password e dettagli relativi a conti bancari o che includono link per effettuare tali operazioni. Le banche e le società di e-commerce, normalmente, non spediscono messaggi di questo genere.
8. **Visitare i siti internet delle banche digitando l'indirizzo nell'apposita barra.** Non selezionare i link presenti nei messaggi di posta indesiderata. I "phisher" possono utilizzare questi collegamenti per reindirizzare l'utente su siti web fantasma: meglio digitare l'indirizzo del sito nell'apposita barra degli indirizzi, per essere sicuri di navigare all'interno della pagina autentica.
9. **Non cliccare sui pop up.** Se appaiono pop up inattesi, come quelli che avvertono della presenza di virus sul computer e che offrono “soluzioni”, non selezionate il link e non autorizzate nessun download. Potrebbero scaricarsi e installarsi software potenzialmente dannosi.
10. **Non salvare le password sul computer o su dispositivi online.** Gli hacker potrebbero essere in grado di accedere al vostro computer e trovare le password.