ADICONSUM
associazione difesa consumatori e ambiente

LA GUIDA DEL CONSUMATORE

Il furto di identità

Come tutelare i propri dati personali

Test noi consumatori - periodico settimanale di informazione e studi su consumi, servizi, ambiente - Anno XX - Supplemento al numero 8 - 22 febbraio 2008
Spedizione in abbonamento postale D.L. 353/2003 (conv. in L. 46/2004) art. 1, comma 2, DCB Roma

ECC-Net
www.ecc-netitalia.it

In collaborazione con

ANSSAIF
Associazione Nazionale Specialisti Sicurezza e Analisi di Informazioni Finanziarie

LA GUIDA DEL CONSUMATORE

Il furto di identità

Come tutelare i propri dati personali

ADICONSUM
associazione difesa consumatori e ambiente

TEST noi consumatori - anno XX - supplemento al numero 8 - 22 febbraio 2008

Direttore: Paolo Landi • Direttore responsabile: Francesco Guzzardi • Comitato di redazione: Paolo Landi, Angelo Motta, Fabio Picciolini • Progetto grafico e impaginazione: Claudio Lucchetta • Amministrazione: Adiconsum, Via Lancisi 25, 00161 Roma • Registrazione Tribunale di Roma n. 350 del 9.06.88 • Spedizione in abbonamento postale D.L. 353/2003 (conv. in L. 46/2004) art. 1, comma 2, DCB Roma • Stampa: Arti Grafiche S.Lorenzo s.r.l., Via dei Reti 36 - 00185 Roma • Finito di stampare in febbraio 2008

Associato all'Unione Italiana Stampa Periodica

Premessa

Il furto d'identità, dei dati personali, non nasce oggi. Esiste da sempre. La storia ci presenta numerosi episodi in cui qualcuno si è sostituito a qualcun altro per ottenere un vantaggio o un guadagno.

Ricordate Giacobbe che, per entrare in possesso dei beni del padre Isacco, si sostituì al fratello maggiore, Esaù? Mise una pelle di pecora al braccio in modo che il padre, cieco e morente, toccandolo, lo scambiasse per Esaù, il quale, essendo il maggiore di età, godeva del diritto di primogenitura e, quindi, sarebbe succeduto ad Isacco.

E Alì Babà il quale, nascosto dietro un masso, udì la frase che, se pronunciata, permetteva l'accesso alla grotta dove era nascosto il tesoro e, andati via i ladroni, la utilizzò per impossessarsi del bottino?

Potremmo andare avanti ancora a lungo citando tanti episodi di scambi di persona o di furto di informazioni "chiave" carpite ed utilizzate per trarne illegittimi vantaggi.

Oggi, in presenza di mercati finanziari molto articolati e di un mondo che viaggia sempre più veloce, l'informatica offre innumerevoli opportunità. Anche la criminalità si è adeguata ed ha trovato nuovi sistemi per raggiungere i suoi scopi. Di conseguenza, le Aziende investono continuamente in sistemi di sicurezza e di protezione dei dati personali al fine di proteggerli ed evitare che estranei possano venirne a conoscenza ma, soprattutto, investono nella formazione e nell'informazione degli utenti dei sistemi informatici.

Facciamo la nostra parte!

Non dobbiamo avere paura delle nuove tecnologie e di sfruttare le opportunità che ci offrono. Piuttosto dobbiamo guardare con sospetto alcuni episodi alquanto anomali: una email che ci invita ad inserire i nostri dati personali in una griglia; un SMS che ci arriva sul telefonino e sembra essere stato inviato da una persona amica; l'incapacità del Bancomat di leggere la carta magnetica; il computer che non risponde ai comandi da quando ci si è connessi ad Internet; ecc..

Inoltre dobbiamo **cercare di adeguare le nostre conoscenze riguardo ai nuovi rischi ed ai nuovi metodi usati dai criminali per impossessarsi dei nostri dati personali.** *Dobbiamo farlo non solo per noi stessi - anche per la nostra cultura personale - ma soprattutto per proteggere le persone a noi vicine che non conoscono adeguatamente i nuovi strumenti informatici e tecnologici e non hanno coscienza dei rischi che corrono.*

Non stiamo dicendo che, per il solo fatto di possedere un computer, si debbano conoscere tutti i sistemi e le tecnologie adottate per portare a termine una frode. Assolutamente no! A questo ci pensano gli specialisti - e le banche ne hanno tanti che si tengono aggiornati continuamente -.

Dobbiamo conoscere quali cautele adottare per ridurre la probabilità di cadere vittima di un furto d'identità.

A tal fine, **ANSSAIF** *(Associazione Nazionale Specialisti di Sicurezza in Aziende di Intermediazione Finanziaria) e* **ADICONSUM***, in linea con la propria missione di tutela ed informazione del Consumatore, hanno realizzato questo volumetto, sintetico e di facile lettura.*

Sommario

Un caso reale: la storia di Paolo

Arriva un plico da una Finanziaria

Un giorno il signor Paolo M., dipendente di un'impresa, riceve un plico da una Finanziaria del Nord. Nella lettera di accompagnamento ai bollettini di conto corrente postale, la Finanziaria afferma: «siamo lieti di comunicarLe di aver accettato la sua domanda di finanziamento di 6.000 euro, che può saldare in comode rate mensili di 190 euro l'una».

Paolo, esterrefatto, controlla i dati per verificare che la lettera sia realmente indirizzata a lui. È così. Paolo, però, non ha chiesto finanziamenti a nessuno! Cosa può essere accaduto?

Chiede chiarimenti alla moglie Carla ed al figlio Rosario, pensando ad un loro coinvolgimento nella questione. «Stai a vedere che Carla ha fatto di testa sua e ha comprato a Rosario qualcosa senza che io fossi d'accordo?» – pensa –. Carla e Rosario negano decisamente e si offendono del fatto che abbia potuto pensare una cosa simile!

È sabato, Paolo telefona alla Finanziaria ma non risponde nessuno. Trascorre un fine settimana d'inferno, pensando a cosa possa essere successo. Il lunedì successivo chiama la Finanziaria e finalmente riesce a parlare con una signora molto gentile dalla quale apprende che il finanziamento riguarda l'acquisto di una moto. La signora, di fronte allo stupore di Paolo, afferma che potrebbe trattarsi di un errore: gli faranno sapere.

Paolo non lo sa, ma è proprietario di una moto!

Trascorrono due giorni e nessuno si fa vivo. Paolo telefona e gli viene comunicato che l'Amministrazione ha eseguito i dovuti controlli e tutto è in regola: i dati anagrafici forniti per il finanziamento combaciano con i suoi.

Manda allora una raccomandata alla Finanziaria, disconoscendo la richiesta di finanziamento e chiedendo copia della presunta domanda. Preoccupato, stanco, nervoso - sono tre giorni che dorme poco e male - si reca al Commissariato della Polizia di Stato di zona e sporge la denuncia.

Si reca, poi, al Pubblico Registro Automobilistico e scopre che effettivamente è intestatario di una moto, la quale è regolarmente registrata ed immatricolata e gira tranquillamente per le strade d'Italia!

Passano altri giorni senza ricevere notizie finché, finalmente, gli perviene la copia della domanda di finanziamento.

Paolo esegue i dovuti controlli. Il suo nome e cognome combaciano con quelli della domanda di finanziamento, l'indirizzo dell'abitazione è giusto, la data ed il luogo di nascita sono esatti, il codice fiscale è esatto…ma il numero e la data di rilascio del documento no! Gli estremi della carta di identità sono errati! Meno male. Comincia a tirare un sospiro di sollievo.

Controlla la firma, ma è chiaramente falsa e non corrisponde alla sua. Si tranquillizza e pensa: «A questo punto sicuramente si sistemerà tutto»!

Un'attesa snervante

Passano i giorni, le settimane…

Paolo si reca spesso al Commissariato. Lì cercano di tranquillizzarlo, «anche se» - dicono - «le indagini sono lunghe…», «i tempi della Giustizia non sono brevi…». Ma lui è giustamente impaziente!

Tra l'altro ogni volta che si reca in Commissariato deve farsi dare delle ore di permesso, e di sicuro non gli fa piacere!

Tra gli amici c'è chi lo tranquillizza e chi, invece, lo ammonisce dicendo: «Non c'è da fidarsi»!

Un giorno suonano alla porta. È il postino che consegna una multa per aver guidato la "sua" moto in contromano!

Paolo fa ricorso ed allega copia della denuncia. In mano, tra l'altro, ha solamente questo, la denuncia che ha presentato, e null'altro.

Passano altri mesi e nessuno si fa vivo per tranquillizzarlo. Ma come si fa ad essere tranquilli pensando che c'è qualcuno che usa una moto intestata a te per fare chi sa che cosa? «Se questo criminale dovesse creare dei danni od investire un passante verrei coinvolto io oppure è oramai chiaro che non c'entro nulla?»– si domanda Paolo -. «E se un giorno la polizia suonasse alla porta con un mandato d'arresto per omicidio colposo?»

Sono già passati 8 mesi

L'altro giorno Paolo si è recato in Commissariato e gli hanno riferito che i furfanti sono stati individuati. La moto? Il giudice non ne ha autorizzato il sequestro e, pertanto, continua a girare per le strade italiane.

Paolo M. è ancora in attesa di un atto ufficiale che lo dichiari formalmente innocente. Ogni raccomandata che gli arriva o il suono del campanello della porta di casa lo agita.

Tutti gli dicono di stare tranquillo, ma, al suo posto, voi lo sareste?

Prime conclusioni sul caso citato

Il caso citato è reale ed è uno dei tanti che accadono ogni giorno in qualche parte del mondo. Vediamo ora di trarne degli insegnamenti. Paolo si è comportato bene, perché:

1. non ha mai perso la calma;
2. ha cercato di mettersi subito in contatto telefonico con la Finanziaria;
3. alla conferma verbale che il finanziamento era effettivamente destinato a lui:
   - ha immediatamente scritto una raccomandata con ricevuta di ritorno alla Finanziaria negando ogni addebito;
   - è andato al Commissariato di zona ed ha sporto denuncia;
4. ha conservato tutta la documentazione in originale.

Dove ha sbagliato:

- non ha costantemente seguito la pratica (anche la moglie lavora; non è facile assentarsi dal lavoro, ma andava fatto);
- poteva chiedere un parere non solo agli amici – che a volte parlano senza cognizione di causa – ma anche a qualcun altro. Poteva, ad esempio, rivolgersi ad una associazione dei consumatori: avrebbe evitato di trovarsi ora con qualcuno che ancora gira per le strade con una moto intestata a lui.

Che cosa è successo al povero Paolo?

Come abbiamo detto, quello di Paolo è uno dei tanti episodi di cui veniamo a conoscenza. I giornali non ne parlano molto – ci sono ogni giorno migliaia di notizie più gravi! – e dedicano all'argomento al massimo un "trafiletto" quando le Forze dell'Ordine scoprono gli autori del reato.

Negli Stati Uniti il reato di furto d'identità, di cui Paolo è stato vittima, è presente da tanti anni, tutti ne hanno conoscenza, ma nonostante ciò ha fatto molte vittime. Ci sono persone che vengono trattenute se tentano di partire con un aereo per un altro Stato. Sono ricercati per reati da loro mai commessi, ma imputabili a qualcuno che è in possesso di documenti falsi con il loro nome. Alcuni di loro portano con sé una dichiarazione dell'FBI, ma ciò non è sufficiente: chi lo controlla, vuole avere assicurazioni che la dichiarazione non sia falsa e, quindi, il cittadino viene trattenuto per ore presso un Distretto di polizia.

Conoscere il reato di furto d'identità, comunque, è l'unico modo per salvaguardarsi, adottando le cautele necessarie che vi suggeriremo di seguito, e per evitare che qualcuno s'impossessi dei nostri dati personali.

Cosa può accadere?

Se un criminale o una banda di criminali s'impossessa dei vostri dati personali - e vedremo come - può, ad esempio, eseguire acquisti, a vostro nome. Come?

- Ottenendo finanziamenti o apertura di linee di credito;
- utilizzando la vostra carta di credito o di debito;
- qualificandosi con le vostre credenziali su un sito Internet di vendita o aste on line come ad esempio eBay;
- trasferendo su un proprio conto corrente i soldi dal vostro conto bancario.

Come può essere messa in atto la frode?

Le informazioni utili ai criminali

Il criminale in genere ha bisogno di questi dati:

a. nome, cognome, indirizzo;

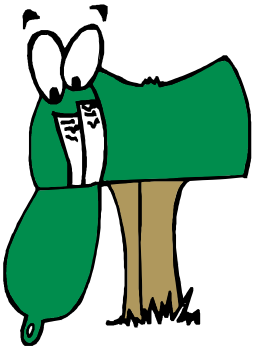
b. numero della carta di credito;

c. gli estremi del conto corrente, o, ancora, il numero del rapporto titoli della banca dove tenete i BOT, ad esempio:

- codice fiscale;
- numero di telefono di casa;
- luogo e data di nascita;
- altre informazioni su di voi, quali: nomi dei genitori, luogo di lavoro, nome del cane, ecc..

Dove trova le informazioni un criminale?

Molte informazioni le può trovare nella vostra **posta** cartacea, prelevandola dall'apposita cassetta oppure andandola a cercare anche nella spazzatura!



Un dato utile come il codice fiscale, per esempio, lo può trovare nell'estratto conto di qualche fornitore, come la fattura bimestrale del vostro gestore Telecom. Da questo dato è facile ricavare il luogo e la data di nascita.

Una recente fonte d'informazione riguardo ai vostri dati personali è il "**blog**" (famoso quello di Beppe Grillo), ossia quella abitudine dei giovani e, tra qualche tempo, anche dei meno giovani, di mettere a disposizione di Internet le proprie riflessioni, idee, suggerimenti, storia personale, curriculum vitae e professionale, foto, video, ecc..

Come si può facilmente comprendere, la mancanza di accortezza nella diffusione delle informazioni, che con troppa facilità vengono rese pubbliche, è un "invito a nozze" per i criminali!

Un'altra fonte è rappresentata dai **questionari** che vi vengono inviati, via posta o via Internet.

Se sono molto lunghi, il compilatore rischia di non accorgersi che sta fornendo le informazioni sufficienti a far conoscere ad estranei le sue

abitudini, i suoi gusti, i suoi consumi, eccetera. Generalmente queste informazioni vengono utilizzate dalle Aziende per suggerire degli acquisti, ma non possiamo sapere chi altro avrà la possibilità di accedervi.

Anche in questo caso, pertanto, si corre il rischio di fornire informazioni utili a perpetrare delle frodi nei nostri confronti.

Qualora il criminale necessiti della **copia di un vostro documento**, la può trovare, cercando con la dovuta pazienza, nello stesso luogo dove ha reperito le altre informazioni ossia, come già detto, nella cassetta della posta o nell'immondizia.

Eh già! Avete mai visto qualcuno rovistare nel secchio della spazzatura? C'è chi cerca un capo di vestiario vecchio e c'è chi, invece, osserva i consumi del quartiere (cosa viene consumato e in che quantità), per poi decidere se aprire o meno un esercizio commerciale. C'è poi chi vuole perpetrare un reato e cerca vecchie fatture, documenti scaduti che voi buttate via, vecchie ricevute della carta di credito, lettere, prescrizioni del veterinario, ecc...

Altre fonti possono essere il portinaio, la domestica del vicino, o voi stessi che, inconsciamente, raccontate in pubblico fatti che vi riguardano. Per esempio, in un ambulatorio in attesa di far visitare il cane, raccontate cosa vi è successo o fate considerazioni che, non sapendo, possono risultare utili a chi vi ascolta, per sapere più cose su di voi. Intanto, per esempio, raccoglie il nome del vostro cane e quanti anni ha! Cosa ci fa?

Può far credere a qualcuno della vostra famiglia che lui è un vostro caro amico o collega - sa tante di quelle cose! - ed ottenere così qualche ulteriore informazione utile per portare a termine la frode - ricordiamo sempre il trucco della pelle di pecora! -. Oppure può fare in modo che facciano qualcosa per voi.

Le ulteriori informazioni che in tal modo il criminale raccoglie possono tornargli utili – per citare altri esempi - quando telefona al call center di un'azienda per farsi dare la vostra password di accesso ad un servizio, facendo credere di non ricordarla più; per comunicare il vostro presunto cambio di residenza in modo da ricevere al suo indirizzo i documenti a voi destinati.

Più cose sa un criminale su di voi, più siete a rischio. Oltre a fare di tutto per non regalare informazioni ai criminali, dovete stare attenti ai "segnali" che vi indicano che siete oggetto di un attacco per furto d'identità.

Attenti ai "segnali"

Quali possono essere i "segnali" che vi suggeriscono di stare in guardia perché qualcuno potrebbe rubare i dati identificativi della vostra identità?

Ecco un elenco non esaustivo, ma che può essere utile:

- perdita/smarrimento di un documento di identità (patente; carta di identità; passaporto);
- furto del portafoglio contenente almeno un documento d'identità;
- furto in casa con o senza sottrazione di un documento d'identità (può essere stato fotografato);
- scippo o furto della carta di credito o debito come, ed esempio, il Bancomat;
- smarrimento della carta di credito;
- mancanza di un assegno nel blocchetto preso in banca;
- mancato arrivo di un assegno via posta, ovvero dell'estratto conto della banca, o della carta di credito;
- mancato arrivo della fattura di un'utenza (Telecom, Enel, ecc.);
- la cassetta della posta aperta o manomessa;
- qualcuno ha chiesto di voi al portiere e voi non avete idea di chi possa essere: ha solo detto che era un amico;
- la vostra banca, l'emittente la carta di credito o un Ente vi avvisano che è pervenuta una vostra richiesta di cambio di indirizzo - ma voi non l'avete mai inviata !-;
- qualcuno che si spaccia per un operatore della vostra banca e vi avverte che c'è un problema con il vostro conto;
- vi telefona una presunta società di assicurazioni che vi propone una polizza estremamente interessante e vi chiede di fornire i vostri dati personali per stipulare il contratto;
- ricevete una telefonata con cui qualcuno vi propone di acquistare un articolo ad un prezzo eccezionale: siete stato selezionato a caso e siete il vincitore!

L'elenco di possibili situazioni pericolose in cui potreste trovarvi rischiando di essere derubati dei vostri dati personali potrebbe essere molto lungo, ma è più utile conoscere gli strumenti di difesa da questo tipo di attacchi.

Ve ne suggeriamo alcuni, posto che nei casi che vi lasciano nel dubbio, è necessario agire con calma, ordinatamente, ma ponendo in essere azioni determinate e ben individuabili.

Come difendersi: misure preventive

Una premessa

Le Aziende (banche, società emittenti carte di credito, fornitori quali ENEL, ACEA, ecc.) non telefonano mai, non mandano email né propri rappresentanti a casa dei Clienti per chiedere dati personali o riservati come il numero del conto, il codice fiscale, il numero della carta di credito, le modalità di pagamento della carta di credito, i conti collegati.

Se l'Azienda dovesse aver bisogno di informazioni che vi riguardano, manderebbe un avviso cartaceo o vi pregherebbe di recarvi presso gli uffici dell'Azienda stessa.

Come difendersi dal furto di un documento o di un titolo di credito

È necessario:

- conservare a casa o, comunque, in un luogo sicuro una fotocopia dei documenti e, quindi, della patente di guida, del passaporto, della carta di identità, del porto d'armi, del tesserino professionale, dei dati relativi alla carta di credito o al Bancomat, ecc.;
- non conservare tutti i documenti di identità nello stesso posto, specialmente se si è in viaggio;

- non comunicate a nessuno i dati relativi ad un documento di identità. Qualora vi vengano richiesti, ad esempio, dalla società emittente la carta di credito o da un fornitore, verificate l'attendibilità della fonte contattando telefonicamente la società, prendendo il numero di telefono dall'elenco o da documenti in vostro possesso di cui siete certi. Dovete cercare di capire se la richiesta è accettabile e, quindi, inviare i dati ad un numero di fax della società stessa evitando di darli per telefono, anche se è più comodo;
- immediatamente dopo aver subito un furto o uno scippo, denunciate l'accaduto al Pronto Intervento (112 per i Carabinieri, 113 per la Polizia di Stato). Recatevi poi negli uffici dell'Autorità di Polizia Giudiziaria e presentate la denuncia, fornendo gli estremi dei documenti che vi sono stati sottratti;
- controllate frequentemente che nel portafoglio siano sempre presenti la carta di credito ed altri documenti. È accaduto, infatti, a diverse persone di essersi accorte troppo tardi di avere smarrito la carta di credito, non riuscendo così a limitare i danni;
- non lasciate mai incustoditi la giacca o la borsetta contenenti il portafoglio: il ladro è veloce! Iladro può essere la persona che lavora nella stanza accanto alla vostra: normalmente tutti ritengono che sia impossibile e, invece, ci sono tanti episodi che dimostrano il contrario.

Fate molta attenzione, quindi, ai segnali di "rischio", anche se deboli. Non trascurandoli, potreste accorgervi che qualcuno sta utilizzando il vostro documento d'identità o la vostra carta di credito. La Polizia vi può aiutare fornendovi molti consigli utili.

Suggerimenti su come gestire i documenti bancari

- Annotate le date di arrivo degli estratti conto (ad esempio: metà gennaio, aprile, luglio, ottobre) ed interrogate la banca se per una di quelle date non vi sono pervenuti (tenendo a mente che potrebbe essere in ritardo, ma è sempre meglio prevenire i pericoli!);

- quando ritirate un carnet di assegni, controllate ci siano tutti e fate questo controllo frequentemente, specialmente se lasciate il carnet a casa incustodito o lo tenete nel portafoglio;
- ricordate di non lasciare mai incustoditi il portafoglio o la borsetta!
- quando ricevete un estratto conto, controllatelo subito ed attentamente. Informatevi presso la banca o la Società emittente la carta di credito quando un prelevamento o una spesa non vi è nota;
- chiedete alla vostra banca ed alla Società di ricevere un SMS sul vostro cellulare quando viene eseguita una spesa. Costerà qualche centesimo di euro, ma vale la pena;
- quando decidete di buttare via gli estratti conto ed altri documenti bancari, incluse le ricevute della carta di credito, strappateli a pezzetti e buttateli insieme alla spazzatura alimentare. Se possibile, acquistate una trinciatrice della carta (fa tante piccole strisce di carta, rendendone più difficile la lettura): costa qualche decina di euro, ma è una misura di sicurezza in più.

Come utilizzare il Bancomat

- Cercate di prelevare sempre alla stessa apparecchiatura Bancomat;
- quando vi recate a prelevare, osservate il Bancomat e fate attenzione ad eventuali "segnali" anomali, alla presenza di qualcosa di diverso dal solito. Ad esempio, potreste trovare una tasca laterale che prima non c'era contenente avvisi pubblicitari;
- dove inserite la carta del bancomat un filo che esce o una sporgenza;
- visto che può essere stata apportata una "miglioria", oppure quello che appare un inconveniente è qualcosa di insignificante, chiedetene conferma alla banca; se questa è chiusa, lasciate stare e recatevi presso un altro Bancomat;

- mentre digitate il codice segreto con una mano, coprite la tastiera sulla quale state digitando il codice con l'altra mano o con fogli posti a pochi centimetri nella parte superiore;
- se avete digitato correttamente il codice segreto per il prelevamento al Bancomat, ma il computer vi dice che è errato, non insistete. Provate su un altro sportello Bancomat e ricordate che avete tre tentativi in tutto; quindi tentate al massimo due volte, una su uno sportello ed una su un altro. Controllerete meglio quando sarete a casa;
- fate attenzione a persone solerti che vogliono aiutarvi a prelevare: possono essere ladri!
- Il codice segreto: cercate di tenerlo a mente; se lo trascrivete, non lo riportate su un oggetto che tenete nel portafoglio o portate con voi nella borsetta. I criminali lo sanno e riescono a trovarlo perché potrebbero avervi visto mentre prelevate al Bancomat e quindi sanno dove lo conservate.

Il computer ed Internet: avvertenze generali

Attenti a quando viaggiate in strade deserte!

Il computer offre nuove possibilità per eseguire le operazioni bancarie e molti tipi di operazioni che fanno circolare denaro: il pagamento della nettezza urbana; il pagamento di bollettini postali; richiesta di documenti dal Comune di Residenza, ecc.. Poter usufruire di un vantaggio, però, ha sempre un costo in termini di impegno! Così è necessario, per non correre rischi, aggiornare frequentemente il sistema operativo, i software utilizzati, le apparecchiature usate in connessione al computer, etc.. Come abbiamo imparato ad usare la macchina da scrivere, il cellulare o a guidare l'auto, così dobbiamo imparare anche a gestire un computer, specialmente se ci si connette spesso ad internet.

Internet, una rete che mette in connessione tra loro computer situati in tutto il mondo, ha tantissimi vantaggi, ma richiede delle accortezze. Facendo un esempio di vita quotidiana, "uscire" su internet e dialogare con il mondo esterno è come decidere, quando siamo in vacanza in una città straniera, di andare a fare due passi in posto che non conosciamo e da cui non sappiamo cosa aspettarci. Se non conosciamo bene la città dove ci troviamo, è buona norma non avventurarsi in strade non frequentate o in quartieri malfamati così come non è assolutamente consigliabile uscire soli di notte!

Prima di partire, ci si deve informare, presso l'Agenzia o il Consolato, sui luoghi pericolosi e da evitare. Sono consigli banali? Eppure spesso leggiamo sui giornali di qualche turista rapinato, accoltellato o ucciso per rapina.

Anche su Internet bisogna avere le stesse cautele e non fidarsi! Anche se al momento non è possibile uccidere "via filo"…

Per reperire le informazioni che vi servono, informatevi prima sui siti da consultare, così da conoscere "le strade da evitare". E, con l'accortezza che usereste ogni volta che vi muovete in luoghi sconosciuti, "non fermatevi a parlare con estranei": non frequentate siti che promettono mirabilie e cercano, in realtà, solo una scusa per estorcere i vostri dati personali o quelli relativi alla vostra carta di credito!

Suoni e foto: possibili dolori!

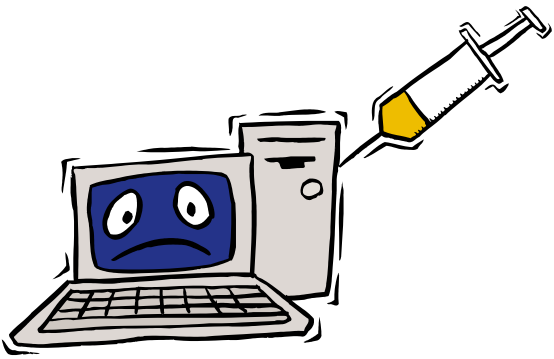
Potete correre un pericolo maggiore di subire un furto d'identità se scaricate video, brani musicali, foto da siti che non conoscete (specialmente se promettono cose…"hard"!). All'interno di presunti video o brani musicali, possono nascondersi dei programmi che, una volta arrivati sul vostro computer, si espandono e prendono il possesso di quanto in essi è contenuto. Il criminale non vorrà vedere le foto delle vostre vacanze o la vostra collezione di barzellette! Introducendosi nel vostro computer, invece, potrà visionare fatture, relazioni, indirizzi di posta: avrà libero accesso a qualsiasi dato che possa riguardarvi e potrà reperire ogni tipo di informazione sul vostro conto che sia utile allo scopo che intende raggiungere. E non solo.

Potrà essere aperta una "porta" di accesso che consentirà al criminale di entrare nel computer e usarlo. Ricordate la storia del cavallo di Troia? La tecnica è la stessa! Solo che nel vostro cavallo, che è il computer, non si nasconderanno guerrieri, ma software. Lo scopo? Carpire altre informazioni su di voi oppure rubare il contenuto del vostro pc e chiedervi denaro per "restituirvelo"! Oppure…chi lo sa? La fantasia dei criminali è senza fine…

A questo punto vi chiederete: «Ma l'antivirus non è in grado di rilevare queste operazioni?» La risposta è semplice: il programma di cui stiamo parlando non è un virus, non ne ha le caratteristiche. È come se aveste scaricato un qualsiasi programma utile per le vostre attività: l'antivirus non lo cancella - ci mancherebbe altro!- perché non lo riconosce come un virus, ma come un programma che voi avete scelto liberamente di installare.

E quando il programma apre la famosa "porta"? Se avete un "firewall" attivato, quasi sicuramente vi avverte. Ma forse è già tardi, perché il programma si è già sistemato all'interno!

L'antivirus



Crediamo che oramai tutti abbiano acquistato un computer. Ma molti non lo aggiornano ed allora tutto diventa inutile!

Insieme all'antivirus molte Società vendono il "personal firewall", che, opportunamente configurato, può consentire di proteggere il computer da un attacco esterno, che può colpirvi quando siete connessi in LAN o in Internet e può farvi inconsapevolmente inviare all'esterno informazioni riservate. Che cos'è un firewall? Letteralmente: un muro, una barriera anti-fiamma. Serve a bloccare un incendio. Nel nostro caso, il "fuoco" è rappresentato da tentativi di entrare nel computer, eseguiti da hackers o criminali tramite programmi, virus, ecc.. È, quindi, una barriera, una porta antincendio che è chiusa e che si può aprire solo se non c'è un incendio. Per citare un esempio, se un hacker sta provando ad entrare nel personal computer attraverso una delle cosiddette "porte", il firewall lo blocca e ne tiene evidenza. Un firewall può essere un software, memorizzato sul computer, o un apparato hardware, nel caso di protezione di computers in azienda.

Ecco i nostri suggerimenti:

- se sul vostro computer ci sono informazioni riservate o se lo usate per fare operazioni bancarie od acquisti su Internet, comperate un antivirus che risulti fra i migliori da uno studio approfondito dei prodotti e/o servizi presenti sul mercato: non risparmiate soldi inutilmente;

- aggiornate l'antivirus tutti i giorni e, possibilmente, attivate l' avviso automatico di disponibilità di un nuovo aggiornamento;
- chiedete all'antivirus una scannerizzazione totale del computer almeno una volta la settimana. Quando la fate, rimanete sconnessi dalla rete Internet o dalla LAN;
- attivate dal primo momento la protezione in tempo reale del file system;
- aggiornate il sistema operativo, specialmente quando ci sono degli aggiornamenti di protezione del computer;
- acquistate un personal firewall ed attivatelo secondo le istruzioni (molto spesso è venduto assieme al pacchetto antivirus).

Vediamo ora qualche altro suggerimento su alcune tematiche specifiche.

L'accesso al computer (userid e password)

Voi siete sicuramente l'amministratore del vostro computer e quindi potete caricare nuovi programmi, toglierne altri, ecc..

La prima cosa che un criminale cercherà di fare, non appena voi siete in Internet, sarà quella di accedere al computer con il vostro codice "utente" o "userid". Un esempio di codice utente o userid possono essere le parole "Amministratore" oppure "Paolo". Questi codici, però, sono troppo semplici e facilmente individuabili: sono termini comuni ed intuibili.

Per garantirvi un livello di sicurezza minimo, quindi, non usate parole comuni e facilmente intuibili, ma cercate di "costruire" un codice facendo in modo che sia composto alternativamente da lettere e numeri – almeno 8, se possibile –, che abbiano un significato per voi, in modo che possiate memorizzarle facilmente, ma che non abbiano un senso compiuto per altri.

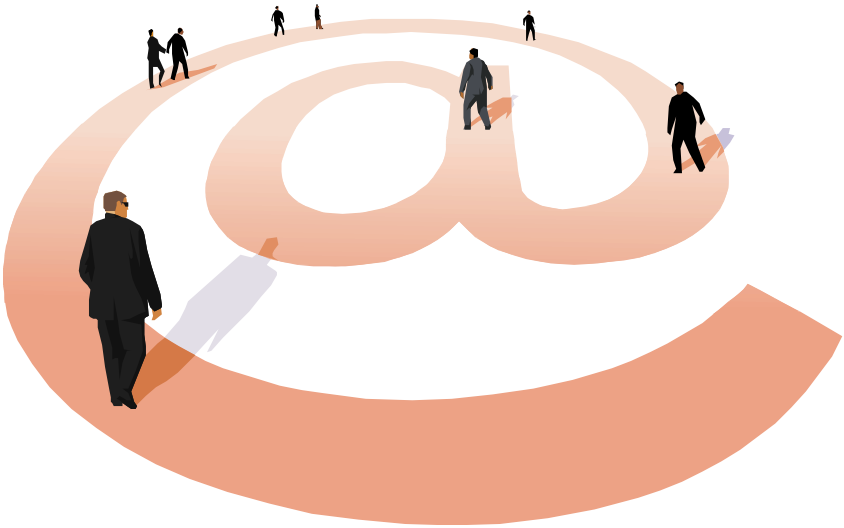
Per esempio, se vi chiamate Paolo Emilio e siete romano, potreste usare un codice utente del tipo PaEmErmejo e password temdrn10 (che sta per: totti er mejo de roma numero 10). In questo modo evitate che la parola chiave possa essere facilmente decifrata. Come privilegi, assegnate quelli di Amministratore.

Ogni due mesi circa, ricordatevi di cambiare la password. Potete cambiare il numero, oppure posizionarlo diversamente all'interno della password o, ancora, sostituirlo con le lettere.

È opportuno per voi cambiare la password ogni qualvolta qualcuno era presente nel momento in cui la digitavate. Non importa se questi è un collega e per di più amico: cambiatela. È importante ricordare, inoltre, che, quando ci si connette ad alcuni siti Internet, la "userid" è la prima parte del nome assegnato alla casella di posta. Facciamo un esempio: la userid è paolo.emilio se la casella si chiama: paolo.emilio@provider.it e non la si può cambiare. In questo caso, il codice identificativo può essere facilmente individuato: basta conoscere il vostro nome e cognome! Al criminale non resta che cercare di scoprire la vostra password.

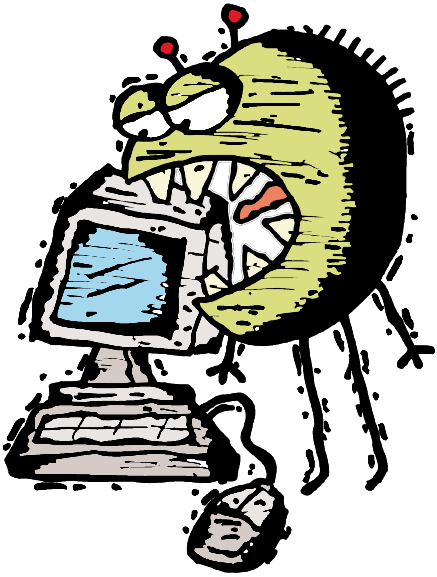
Ecco perché comunque è bene avere delle password difficili da scoprire. Se vi riconoscete nell'esempio appena citato, suggeriamo, se possibile, di cambiare la "userid", oppure di crearvi una casella di posta con un nome non facile.

In questo modo, potete utilizzare la casella stessa come "userid".



Il computer lavora da solo!

Questa affermazione viene usata sempre di più negli ultimi tempi. Se avete notato, ogni tanto il computer sembra affaccendato in altre cose. Se attivate "Task manager" (premendo contemporaneamente i tasti Ctrl-Alt-Canc) e guardate la cartella "Prestazioni", potrete notare che risulta un'attività del computer anche del 40%. Se non avete alcun programma in esecuzione, sicuramente vi spaventerete.



E giustamente, perché potrebbe trattarsi di un virus o un di programma che vi è stato iniettato.

Tuttavia, è più probabile che si tratti di programmi Microsoft (se il vostro sistema operativo è Windows) o dell'antivirus che stanno lavorando in "background".

Cosa fanno?

Potrebbe essere in corso un aggiornamento di Windows, se avete optato, correttamente, per un aggiornamento automatico del sistema operativo con le correzioni più recenti; oppure, analogamente, potrebbe trattarsi dell'antivirus che si sta aggiornando, anche lui dopo essersi collegato ad Internet, ovvero, sta esaminando il disco fisso alla ricerca di virus.

La domanda sorge spontanea: come faccio ad essere certo che non si tratti di un virus? Se siete abbastanza esperti del computer, seguite queste istruzioni:

- attivate "Task manager", come detto sopra;
- scegliete la cartella "Processi";
- cliccate sulla colonna "Tempo CPU" in modo da vedere in ordine decrescente di impegno di processore dei processi aperti;
- sotto "Nome immagine" leggete il nome del primo (escludete: "Ciclo di sistema", "services. exe", "svchost.exe", "ccSvchost.exe" e quelli di programmi noti, quale: "WINWORD.EXE");
- prendete il nome (ad esempio: ATKOSD.EXE) e cercate su Internet tramite Yahoo, o Google o altro motore di ricerca;
- potreste trovare su Internet indicazioni come la seguente: "atkosd.exe is a process installed alongside ASUS Motherboards and provides additional configuration options for these devices. This program is a non-essential process, but should not be terminated unless suspected to be causing problems. Se hai una scheda madre asus è un programma relativo a quella";

- da quanto leggete, comprendete che si tratta di un programma fornito assieme al computer che state usando. Così facendo potrete trovare commenti di altri utenti, ma attenti: qualcuno potrebbe divertirsi a fare del terrorismo e indurvi a cancellare un programma che invece serve! È bene, pertanto, che, prima di cancellare qualcosa, interroghiate Microsoft - sul cui sito potete trovare indicazioni assai utili - e il fornitore dell'antivirus; in quest'ultimo caso, andate sul sito del fornitore e digitate nel campo "Ricerca" (o "search") il nome del processo che vi preoccupa. Qualora si tratti di un virus, il sito vi avverte. In questo caso dovrete allora procedere secondo le istruzioni del fornitore (esempio: "aggiornare l'antivirus", "scollegare il pc da Internet", "eseguire una scansione", ecc.).

I computer con connessioni senza fili

Utilizzando computer che si connettono senza fili (la così detta tecnologia WiFi), dovete stare attenti perché siete ancora più esposti a possibili attacchi anche da parte del vostro vicino di casa!

È emblematico un caso. Un amico aveva comperato un telefono senza fili. Un giorno vide che una luce rossa dell'apparecchio era accesa, come se qualcuno stesse parlando. Spinse un tasto e sentì una conversazione fra due persone.

Gli venne in mente che qualche giorno prima aveva visto la sua dirimpettaia, una nota attrice televisiva, mentre parlava sul balcone con un telefono senza fili. Era lei che sentiva dal suo apparecchio: aveva sconnesso dalla presa di corrente la base sulla quale si innesta il ricevitore trasportabile, e parlava con un uomo, probabilmente residente in un' altra città, a spese sue! Tutto perché non aveva attivato il codice di protezione fra il telefono e la base.

La stessa cosa può accadere con il computer. Le raccomandazioni che vi suggeriamo di adottare sono di seguire le istruzioni del fornitore dell'apparato "wireless" e quelle del "provider" del collegamento Internet (Telecom, Fastweb, Tiscali, ecc.); in particolare, attenendovi alle istruzioni fornite, eseguire quanto segue:

- attivate la crittografia nella trasmissione;
- attivate i codici di protezione; in particolare:
  - cambiare userid e password per l'accesso al proprio "access point";
  - cambiare possibilmente lo SSID, identificativo utilizzato quando viene rilevato l'"access point" che spesso porta il nome della casa produttrice e quindi rende più facile la procedura di intrusione;
- se possedete un firewall, configuratelo e non disabilitatelo, anche se la procedura di accesso è più difficile.

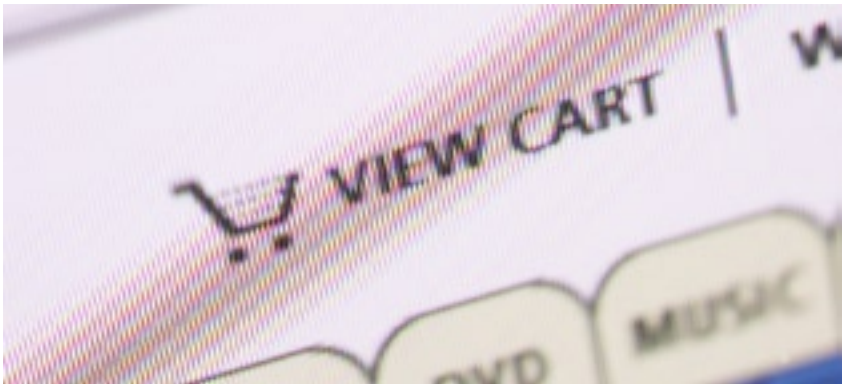
Una parola per chi è connesso ad una LAN: attenzione alle "cartelle" condivise. Esistono delle cartelle, in Windows, che risultano disponibili anche per altri che, come noi, fanno parte di una rete di computer connessi tra loro.

Se mettete in tali cartelle documenti contenenti dati personali o riservati, chiunque è connesso alla rete può accedervi. Prima di mettere qualche documento riservato in una cartella, quindi, accertatevi che non sia "condivisa" con altre persone.

Acquisti on line in tutta sicurezza

Data la sempre maggiore diffusione di questo mezzo, è bene conoscere le misure da adottare per poter effettuare gli acquisti online in tutta sicurezza. I suggerimenti:

- **evitate di usare la carta di credito per gli acquisti on line.** Esistono oggi delle carte prepagate che sono accettate in Internet. Le potete caricare in anticipo della quantità di contante che pensate di utilizzare. In tal modo quell'importo è la massima perdita economica possibile, nel caso siate vittima di una frode;
- **dubitate di prodotti venduti a prezzi estremamente vantaggiosi**: la polizia ha migliaia di denunce di compratori truffati;
- **agite con cautela** se il prodotto che volete acquistare viene proposto da un venditore che è situato in un Paese asiatico come la Cina o Corea, anche se ha una storia di vendite avvenute con successo e con giudizio di gradimento positivo da parte degli acquirenti: si può costruire facilmente una buona carriera con l'aiuto di un po' di amici!
- **dubitate dei venditori che non forniscono un numero telefonico "fisso"**;
- **dubitate dei venditori che danno solo un indirizzo presso una casella postale**;
- **evitate sempre di fornire dati personali riservati.** Quando siete costretti a farlo, tenete a mente che da quel momento in poi una persona quasi sconosciuta ne può disporre e li può utilizzare anche per scopi non leciti;
- **insospettitevi, dunque, se vi chiedono dati ed informazioni** ulteriori rispetto a quelle che avete fornito.



A pesca di dati riservati: il "phishing"

La tecnica

Con questo termine - che si pronuncia "fiscin" e che, tradotto, significa "pescando" -, si indica una recente tecnica volta a carpire i dati riservati di un consumatore. Il phishing può essere eseguito via telefono o via email.

Una persona, qualificandosi come impiegato della vostra banca o di una Società emittente la carta di credito, vi telefona e, con la scusa di controllare la bontà dei dati in vostro possesso ai fini di migliorare le misure di sicurezza per proteggere il vostro conto corrente, vi chiede di fornirgli una serie di informazioni che, successivamente, gli consentiranno di prelevare i soldi dal vostro conto, oppure di fare acquisti a vostro nome.

Il processo, con queste modalità, avviene generalmente via email. Può arrivarvi una email da un indirizzo Web che sembra in tutto e per tutto uguale a quello della vostra banca.

Nella email vi chiedono di accedere al sito indicato ed inserire i vostri codici di accesso nella griglia che apparirà, come fate abitualmente.

Eccone un esempio:

Posteitaliane

Gentile membro Poste Italiane,
Grazie ai recenti trasferimenti illegali di conti elettronici, il tuo conto BancoPosta c' stato bloccato per la tua sicurezza. Questo e' stato fatto per assicurare il tuo conto e le tue informazioni private. Come misura di sicurezza,vi consigliamo di collegarti al vostro Conto BancoPosta e cambiare il tuo codice di accesso

Il nostro sistema ti aiuterà rapidamente a cambiare il tuo codice di accesso. Il tuo conto non sarà sospeso in questo caso, però , se invece, 48 ore dopo aver ricevuto questo messaggio, il tuo conto non verrà confermato, ci riserviamo il diritto di sospendere la tua registrazione Poste Italiane. Poste Italiane è autorizzato a fare qualsiasi tipo di operazione affinche anticipi le fraude. Fare click qui per cambiare il tuo codice di accesso

Considerazioni migliori,
Il reparto sicurezza

Come si nota dall'esempio, nel testo ci sono vari errori grammaticali. Eppure sembra che qualche utente disattento abbia abboccato!

Se seguite alla lettera quanto scritto nella email che avete ricevuto, cliccando sul link vi collegate ad un sito in tutto e per tutto uguale a quello della vostra banca. Se fate attenzione, però, noterete delle differenze e, dopo aver inserito il codice di accesso e la password, sarete sconnessi dal sito e vi apparirà una scritta come "errore di connessione", oppure "transazione andata a buon fine". È certamente andata a buon fine per il criminale che ora accederà al vostro conto sottraendovi il denaro nel più breve tempo possibile!

Anche se un'indagine ANSSAIF – ICAA ha rilevato che in Italia solo lo 0,07% dei correntisti ha abboccato all'amo, la perdita economica per qualche ingenuo non è stata indifferente.

In sintesi: dubitate di chi vi chiede i vostri codici personali. Contattate voi stessi gli uffici della banca o dell'azienda che vi ha chiesto queste informazioni e chiedete spiegazioni.

Ricordate sempre che una banca non chiede di fornire dati personali via email.

CartaSi

Gentile Cliente,

Una nuova gamma completa di servizi online è adesso disponibile ! Per poter usufruire dei nuovi servizi online di CartaSi.it occorre prima diventare UTENTE VERIFICATO.

Accedi ai servizi online di Cartasi.it e diventa UTENTE VERIFICATO »

Cordiali Saluti

Anche in questo secondo esempio ci sono vari errori grammaticali. Gli intermediari finanziari non mandano messaggi di questo tipo!

I criminali sono psicologi!

Nel momento in cui riescono ad entrare in contatto con voi, è recente abitudine dei criminali ricorrere a toni drammatici nel corso di una telefonata, del tipo: «il vostro conto corrente è bloccato!», oppure: «La carta di credito è stata clonata!».

Questo perché un consumatore nel panico perde il controllo di se stesso, abbassa la guardia ed esegue alla lettera quanto gli viene chiesto dal criminale.

In questi casi ascoltate, fatevi dire chi ha telefonato e chiedetegli: nome, cognome, ufficio, numero di telefono.

Poi, dite che richiamerete.

Chiamate e chiedete spiegazioni, invece, all'Azienda o alla Banca, e parlate con una persona che conoscete o che si occupa della sicurezza. Non fornite mai a sconosciuti i vostri dati personali!

Informatevi, ma non cadete in trappola. Dovete mantenere il controllo della situazione.

E se vi dovessero minacciare - in genere non lo fanno, ma non si sa mai.. -, chiamate la Polizia o i Carabinieri e raccontate tutto.

Le email

È opinione diffusa che il mittente di una email è certo. Non è corretto. Anche una lettera che sembra provenire da un'Azienda, potrebbe non essere vera. Come si può falsificare una busta, una carta da lettere, una firma, così si può falsificare il mittente di una email.

Diffidate sempre dell'indirizzo del mittente e leggete il contenuto domandandovi: «è vera?».

Molti stanno iniziando ad usare email certificate e questo è già un passo avanti.

Amministratore delegato per i pagamenti on line
Posti disponibili: 17
Posizione geografica: Italy
Guadagno: 430-550 EUR a settimana
Occupazione: part-time (2-4 ore al giorno)

La descrizione del lavoro:
- **gestire i pagamenti on line**
- **rispondere alle e-mail/telefono collegati con il l progetto**

Assistente a distanza
Posti disponibili: 21
Posizione geografica: Italy
Guadagno: 350-480 EUR a settimana
Occupazione: part-time (2-4 ore al giorno)

La descrizione del lavoro:
- **ricevere la corrispondenza dalla nostra societD° o dai clienti**
- **rispondere alle e-mail/telefono collegati con il progetto**
- **effettuare un numero limitato di telefonate**
- **gestire i pagamenti collegati con il progetto**
- **supporto clienti**

Importante:
Nessuna di queste posizioni richiede un investimento.
Non deve pagare nessun libro, nessuna cassetta. NIENTE.
Deve solo investire un po di suo tempo e di lavorare per raggiungere gli OBIETTIVI

Per procedere con la domanda, la chiediamo di compilare il modulo come segue e rinviarcelo indietro alla nostra e-mail:

In questa email ingannevole, il mittente finge di cercare personale da impiegare a part time. Ma che tipo di lavoro viene offerto? Il truffatore, in questo caso, propone al destinatario dell'email di ricevere denaro in contanti - proveniente da dove? da quale business? - , di versarlo sul proprio conto corrente e di inviarlo successivamente all'estero con cadenza mensile tramite bonifico bancario, trattenendo per sé una percentuale. Al lettore, in realtà, viene proposto di **riciclare denaro sporco**!

Conclusioni

Un'indagine effettuata in Italia fra gennaio e febbraio 2007 mediante un sondaggio su un campione di 200 utenti domestici e 100 business, ha consentito di rilevare che il 60% degli utenti delle banche on line naviga senza adeguati sistemi di sicurezza.

Il 90% degli utenti domestici, inoltre, è a conoscenza dei rischi che si corrono navigando in rete, ma il 60% usa sistemi operativi non aggiornati o fuori produzione come Windows 95, ad esempio. L'88% ha installato un antivirus, ma non sa dire se e con quale frequenza venga aggiornato. Solo il 60% ha installato un firewall.

Una indagine eseguita nella seconda parte del 2007 da Dynamic markets su un campione di 750 fra utenti e responsabili delle Tecnologie dell'Informazione di piccole e medie aziende, ha rivelato che l'83% dei responsabili non crede che la sua azienda sia adeguatamente protetta!

La strada, quindi, per raggiungere un migliore equilibrio costi/rischi, è ancora lunga. Come mai? È nostra opinione che la continua rapida evoluzione nelle tecniche di attacco adottate dai criminali, rende vana una difesa basata esclusivamente sulla tecnologia.

Si dice nel campo della Sicurezza: «una catena è resistente agli attacchi nella misura in cui ogni suo anello è resistente».

La tecnologia (antivirus, firewall, antispamming, antiphishing, token, smart card, certificato digitale, ecc.) ha la sua importanza, ma uno degli anelli è rappresentato dall'uomo, con i suoi pregi ed i suoi difetti, con le sue paure e le sue ingenuità.

La tecnologia può aiutare, può far molto, ma serve la collaborazione attenta e consapevole del cittadino.

L'utente di sistemi informatici che usi un computer in azienda o a casa, deve avere un approccio ad esso che sia lo stesso che avrebbe con un estraneo per strada: deve dubitare.

A ciò si deve aggiungere una costante informativa proveniente dalle parti sociali ed istituzionali competenti. Come già detto, la Sicurezza è come una catena dove ogni anello deve essere robusto, deve fare la sua parte. È l'intento che questo opuscolo intende perseguire: che ognuno faccia la sua parte, la Banca, l'Azienda, ma anche il cliente, anche il consumatore, anche il cittadino.

Per concludere, riteniamo utile fornire qualche piccola regola riassuntiva:

- Non rispondete mai a richieste di informazioni personali ricevute tramite telefono, posta, posta elettronica, od SMS.
- Non visitate mai i siti Web cliccando direttamente nell'indirizzo (Url) ricevuto nella mail, ma, volendo accedere ad un sito, digitare i riferimenti - di cui siete certi - nella barra degli indirizzi.
- Verificate che il sito Web utilizzi la crittografia (https://).
- Esaminate regolarmente gli estratti conto bancari e della carta di credito e, ove l'Istituto fornisca il servizio di ricezione sms per ogni movimento, attivatelo.
- Usate sistemi operativi aggiornati.
- Non collegatevi mai da hotspot e da Internet café per consultare e fare transazioni on-line.
- E, non ultimo, NON SIATE INGENUI!

I consigli dell'Adiconsum

La tecnologia, nata per semplificarci la vita, spesso ci trasporta in mondi dove, all'aumentare delle opportunità corrisponde un necessario, se non obbligatorio, aggiornamento culturale per consentirci di essere padroni dei nuovi strumenti che la tecnologia ci mette a disposizione, e non servitori passivi.

Le possibilità che i nuovi sistemi ci danno di poter effettuare tutta una serie di operazioni, sia materiali che immateriali, senza dover essere "sul luogo", grazie ai telefoni, fax, posta e, più recentemente, la Rete, ha generato anche una nuova serie di reati che, se meno visibili del tradizionale furto, non per questo sono meno pericolosi, anzi…

Nelle pagine precedenti avete compreso come l'identità stessa sia un valore economico da difendere al pari dei vostri beni personali e come la posizione più responsabile sia quella di trovare la giusta via di mezzo tra i comportamenti ai limiti della paranoia e il pensare "siamo milioni, perché deve capitare proprio a me?".

Il livello di precauzioni da attivare varia inoltre da individuo a individuo, per cui non si può generalizzare, per cui le ulteriori indicazioni vanno recepite in funzione del proprio profilo.

Quali precauzioni?

Sul lato "vita reale" le avvertenze che avete potuto leggere nelle pagine precedenti sono facilmente comprensibili, per cui i nostri consigli pratici, in ordine di esigenza di sicurezza, sono:

1. dotarsi di una macchina distruggi-documenti, cui passare tutta la documentazione cartacea (ma ora anche carte di credito, CD, floppy, etc.) prima di gettarla nei rifiuti;
2. il conto corrente delle spese correnti, quello su cui sono attive le carte di credito, non deve avere cifre superiori alla spesa corrente. Gli altri soldi meglio tenerli in un secondo conto da usare solo per alimentare via via quello delle spese correnti;
3. usare solo carte di credito prepagate, in modo da ridurre la perdita a quanto da voi versato precedentemente;
4. non uscite di casa con il portafogli attrezzato come se doveste partire per un viaggio all'estero. Libretto degli assegni, bancomat e carte di credito, così come i documenti, vanno portati solo se si pensa di doverli usare, altrimenti meglio che stiano al sicuro in casa.

Nel cyberspazio le cose si complicano un pochino, perché le stesse società che vi spingono ad utilizzare sistemi telematici per le vostre transazioni economiche, sono le prime a scaricare sul consumatore finale tutte le responsabilità quando le cose prendono il verso sbagliato.

Dall'altro lato, come avrete potuto capire, il crimine telematico ha raggiunto livelli di sofisticazione tanto elevati da mettere a dura prova anche le persone competenti. Per cui, sempre ordinati per "desideri di sicurezza", i nostri consigli sono:

1. se non capite quello di cui stiamo parlando, non attivate nessun sistema "on-line". Non è un male non sapere, ma lo è l'usare senza sapere.
2. Verificate attentamente i livelli di sicurezza intrinseca proposti dagli operatori economici (banche, assicurazioni, finanziarie, etc.) scartando decisamente quelli che non utilizzano sistemi di sicurezza intrinseca (one time-password e simili) e si affidano alla semplice password per l'accesso ai servizi.

3. Leggere – e al limite farsi consegnare per far leggere a persone esperte di vostra fiducia – i contratti proposti, per verificare il livello di deresponsabilizzazione della società in caso di controversie per uso fraudolento del servizio.
4. In casa, data per scontata l'adozione di software di sicurezza, come firewall, anti-virus, anti-spy, etc., peraltro descritta nelle pagine precedenti:
   - non tenete per nessun motivo fotocopie dei documenti, codici fiscali, firme digitalizzate, dati dei conti correnti, etc., nell'hard disk del computer. Se proprio necessario, mettere tutto su un CD o chiavetta usb, da conservare in un luogo sicuro;
   - non tenete i documenti nella cartella "documenti", ma in un altro luogo, meglio se su un hard disk esterno. Questi dispositivi hanno la controindicazione di essere più lenti dell'hard disk, per cui il nostro ulteriore consiglio è quello di indirizzarvi su modelli con presa firewire, più veloce. La soluzione disco removibile, peraltro, ha l'indubbio vantaggio di poter usare i documenti con più PC;
   - fate sempre, ripetiamo: sempre, una copia di back-up del vostro hard disk, al di là del fatto che questa operazione debba essere eseguita per ovvi motivi di sicurezza contro i malfunzionamenti delle macchine. Alcuni software, oltre a rubarvi i dati, vi distruggono il contenuto dell'hard disk;

   - se proprio vi piace navigare per rotte perigliose (che non è necessariamente "quel" tipo di rotta), non è da escludere l'uso di una macchina "dedicata", completamente anonima e dove non è attivo alcun servizio all'infuori di quelli della navigazione o del P2P (peer to peer) che, ricordiamo, non deve essere usato per scambio di file protetti dal diritto d'autore.

- prima di inserire in una pagina internet qualsiasi dato che sia relativo alla vostra identità personale, verificare che in alto a sinistra, dove si mettono gli indirizzi internet, al posto del tradizionale http:// vi sia https://. Inoltre controllare che in alto e/o in basso a destra compaia un piccolo lucchetto; cliccare quindi sullo stesso e accertarsi che il certificato digitale sia valido.
- Usare PC Mac o, meglio, Linux, può aiutare. Per ovvie ragioni statistiche, la maggior parte dei software malevoli sono progettati per funzionare solo su macchine equipaggiate con Windows, sistema operativo attualmente installato sul 95% dei PC ad uso familiare. Nessun sistema vi mette comunque al riparo dalle mail o dai siti che vi invitano a fornire i propri dati;
- Attenti alle ore piccole: la stanchezza abbassa il livello di attenzione, e il click sbagliato ha maggiori possibilità di essere attivato.

Condannato dalla Cassazione per aver usurpato l'identità di una donna

In Internet si faceva passare per un'altra persona e ne utilizzava i dati per inviare e ricevere posta elettronica.

La sostituzione di persona in Internet appare sempre più rilevante. Tale norma non rientra a pieno titolo nelle previsioni tipiche dei computer crimes introdotti con la legge 547/1993, tuttavia una sua applicazione alle nuove tecnologie sembra opportuna ed efficace.

A supporto di quanto detto è arrivata una sentenza della Corte di Cassazione (V Sezione Penale n. 46674 del 14 dicembre 2007) che a fine 2007 ha riconosciuto colpevole un soggetto che aveva aperto un account di posta elettronica utilizzando i dati di altra persona esistente e mediante questo aveva allacciato rapporti in rete con altri utenti.

Una simile condotta, a parere della Corte, ben integra la fattispecie prevista dall'art. 494 del codice penale in quanto viene pregiudicato il bene tutelato dalla norma: la fede pubblica.

Il supremo collegio ha precisato in tal senso che "Oggetto della tutela penale, in relazione al delitto preveduto nell'art. 494 c.p., è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che possono superare la ristretta cerchia di un determinato destinatario, così il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome".

In particolare nell'analizzare la condotta posta in essere dall'imputato, la Corte ha valutato tutti i presupposti previsti dall'art. 494 codice penale. Infatti il fine primo e ultimo dell'imputato è stato quello di recare ad altri (il vero titolare delle generalità) un danno, inducendo taluno in errore (gli utenti della rete). Inoltre ha sostituito illegittimamente la sua persona a quella di altri, tant'è che gli altri utenti credevano di interloquire con la vera titolare di quei dati e non anche con un soggetto diverso, peraltro di sesso opposto, nascosto dietro la "falsa identità".

Infine la Corte si è soffermata sul danno arrecato previsto dalla norma che ha individuato "nella subdola inclusione della persona offesa in una corrispondenza idonea a ledere l'immagine o la dignità della XXXX". A seguito dell'iniziativa assunta dall'imputato, la stessa parte offesa ha ricevuto telefonate da uomini che le chiedevano incontri a scopo sessuale.

La presenta sentenza, dunque, mette in evidenza uno dei problemi intrinseci della Rete, ossia il nascondersi dietro nickname o nomi di altre persone per porre in essere condotte al limite del lecito. Il fatto di nascondersi dietro falsi nomi prevede la reclusione fino ad un anno.

Per qualsiasi chiarimento o maggiori informazioni su quanto contenuto nel presente opuscolo, non esitate a contattare l'**ADICONSUM** o l'**ANSSAIF**.

Ringraziamenti

Si desidera ringraziare l'ing. Anthony Cecil Wright per la stesura del testo e, per il loro contributo ai contenuti e per la successiva finalizzazione, i Sigg.: Antonio Caricato, Giancarlo Lopes, Paolo De Vito, Venera Diamante, Vito Umberto Vavalli, Philip Wright.

ADICONSUM

L'Adiconsum è l'Associazione Difesa Consumatori e Ambiente promossa dalla CISL nel 1987. Essa opera a tutela dei consumatori in piena autonomia dalle imprese, dai partiti, dal governo e dallo stesso sindacato.

Dopo oltre 20 anni di attività, l'Adiconsum è presente in tutte le regioni italiane, con oltre 280 sportelli nelle maggiori città. La capillare diffusione territoriale, che ne fa una rete sensibile e ben articolata, è occasione per un'attività di monitoraggio che si rivela insostituibile nella rilevazione di problemi emergenti, anche anticipando i canali di osservazione e di ascolto istituzionali.

La presenza sul territorio favorisce inoltre l'espletamento delle forme di assistenza diretta individuale, come la consulenza nei casi di contenzioso, la distribuzione di materiali informativi, la raccolta di segnalazioni e denunce. Ancora, lo stretto contatto con il grande pubblico e con i media è strumento prezioso nell'attuazione delle numerose campagne informative e formative il cui successo sta tutto nel rapporto di fiducia instauratosi con i consumatori.

La tendenza alla crescita dell'Adiconsum è visibile sia nel volume dell'attività (numero dei casi individuali trattati e delle azioni collettive intraprese) che nell'ampiezza dei settori di intervento e tutela: assistenza, consulenza e informazione sono il risvolto individuale di una protezione che parte comunque dall'azione collettiva e che riveste forte pregnanza politica.

www.adiconsum.it
Sede Nazionale: Via G.M.Lancisi, 25 – 00161 Roma
Tel.: 064417021 – email: adiconsum@adiconsum.it

ANSSAIF

L'Associazione Nazionale Specialisti di Sicurezza in Aziende di Intermediazione Finanziaria, associazione senza scopo di lucro, è stata fondata nel 2003 da dirigenti e funzionari di dieci gruppi bancari che si erano conosciuti nell'ambito di un lavoro sul rischio informatico presso la CIPA, ai quali si erano uniti anche il Presidente ed il Segretario Generale del CLUSIT. Successivamente nel Direttivo è entrato anche un alto dirigente di ABILab, nominato dall'ABI.

Le finalità dell'Associazione sono:

- la partecipazione alla maturazione, in tutte le sedi opportune, anche universitarie, della consapevolezza dei problemi connessi alla necessaria protezione dei beni informatici, dei dati e delle informazioni, per garantirne la riservatezza, l'integrità e la disponibilità;
- la promozione di studi e ricerche nel campo della sicurezza ICT (Information and Communication Technology), curando altresì di individuare processi e momenti di integrazione della sicurezza logica e di quella fisica;
- la conservazione del patrimonio di esperienze professionali degli specialisti di sicurezza del settore, anche al termine della loro attività lavorativa.

Oggi l'Associazione raccoglie nei suoi Seminari di studio e nei Convegni esperti e dirigenti delle maggiori banche e gruppi bancari, operatori di sistema ed aziende di servizi. Le sue Newsletter sono lette da quasi 600 professionisti.

www.anssaif.it
Sede legale: Via Monterosi 52 – 00191 Roma
Tel.: 0636001203 – email: info@anssaif.it

www.ecc-netitalia.it

Sede principale: Via G.M. Lancisi 31 - 00161 Roma
Tel.: (+39) 06 44290734/ (+39) 06 44238090 Fax: (+39) 06 44118348
E-mail: info@ecc-netitalia.it

Centro Europeo Consumatori Italia

Il Centro Europeo Consumatori ti aiuta a conoscere i tuoi diritti e a farli rispettare

Il Centro Europeo Consumatori dialoga con l'impresa per esporre le tue ragioni e vedere accolto il tuo reclamo

Il Centro Europeo Consumatori promuove la diffusione del ricorso alla soluzione extra-giudiziale delle controversie di consumo in ambito europeo

Il Centro Europeo Consumatori ti informa e ti assiste

Problemi di consumo transfrontaliero?

Il Centro Europeo Consumatori lavora in stretto contatto con la Commissione Europea, le istituzioni nazionali a tutela dei consumatori e gli altri Centri europei della rete ECC - Net per migliorare la tutela dei consumatori nel Mercato Unico europeo.

Se vuoi prodotti più sicuri e di qualità, servizi più efficienti, tariffe più trasparenti, alimenti più sani, un ambiente più pulito, la tutela dei tuoi diritti…

Se vuoi un'informazione più obiettiva, che sia un valido strumento di autodifesa…

Entra nella nostra associazione, iscriviti all'Adiconsum

ADICONSUM
associazione difesa consumatori e ambiente

Via G.M. Lancisi 25
00161 - Roma
Tel. 06 4417021 - Fax 06 44170230
E-mail: adiconsum@adiconsum.it
Web: www.adiconsum.it

Adiconsum,
dalla parte del consumatore.