

Perché il furto d'identità è un problema grave?

Il furto d'identità è il crimine contro i consumatori che sta crescendo più rapidamente nel Nord America. Questo crimine colpisce ogni giorno sempre più vittime, ma molti credono che non toccherà proprio a loro. Il recente incremento di questo reato è dovuto in gran parte alla grande diffusione di lettori di schede elettroniche e nel crescente coinvolgimento criminale nel fenomeno dell'hacking dei computer.

Cos'è il furto d'identità?

Il furto d'identità avviene quando un individuo utilizza l'identità di un'altra persona per commettere una frode o conseguire un guadagno illecito. Utilizzando semplici dati personali, come il nome, l'indirizzo o il numero della previdenza sociale, il ladro d'identità può chiedere prestiti, mutui, carte di credito, noleggiare auto, affittare appartamenti e compiere altri crimini, sempre usando l'identità rubata. Questo lascia spesso la vittima innocente a fronteggiare le responsabilità legali e finanziarie degli atti commessi dal ladro, con l'onere, oltretutto, di dover ricostruire la propria reputazione creditizia.

Come ottengono i criminali i vostri dati personali?

Telecamere nascoste: i ladri di identità usano telecamere nascoste situate sopra le casse dei punti vendita o sui Bancomat, per vedere il numero PIN, il numero della carta di credito o la password delle vittime.

Cassonetti dell'immondizia: i ladri d'identità sono noti per cercare nell'immondizia domande di credito buttate vie, resoconti delle carte di credito o altri estratti conti finanziari per ottenere informazioni personali.

Furto di oggetti personali: i criminali prendono di mira i portafogli, le borsette delle signore e il cassetto portaoggetti delle automobili, per ottenere informazioni personali. Anche i computer sono eccellenti fonti di dati riservati, perché contengono l'elenco dei siti Internet visitati, i messaggi e-mail personali e le informazioni sulle operazioni bancarie effettuate online.

Skimming o manomissione: accade di frequente nei Bancomat o nelle casse dei punti vendita. Nello skimming, il criminale ottiene i numeri della carta di debito o di credito, grazie a un apposito dispositivo elettronico che li memorizza. Questi dispositivi possono memorizzare varie informazioni personali, che il ladro usa successivamente per riprodurre le carte e usarle nelle sue frodi.

Informazioni di acquisto: impiegati disonesti, che hanno accesso ai dati personali e ai numeri delle carte di credito possono far circolare o vendere queste informazioni nelle chat room di Internet.

Cassette postali: i ladri d'identità possono rubare la corrispondenza della vittima o farla inoltrare a un altro indirizzo o casella postale. I ladri cercano nella corrispondenza nuove carte di credito, offerte di credito pre-approvate, resoconti di assicurazioni, informazioni relative alle imposte sui redditi, documenti su investimenti e moduli per i benefici ai dipendenti.

Altri mezzi per ottenere informazioni personali

Phishing (pronuncia: "fishing") – Si tratta di una vecchia frode, aggiornata per adeguarla alle moderne tecnologie. Il phishing si svolge tramite comunicazioni per posta, telefono o e-mail, nelle quali i ladri si fingono rappresentanti di imprese legittime. Forniscono notizie allarmanti o entusiasmanti che richiedono una risposta immediata, con la speranza di convincere la vittima a fornire dati riservati. Questo approccio è usato quasi esclusivamente con intenti fraudolenti; le vittime non ricevono ciò che è stato loro promesso.

Pharmers – I ladri d'identità si limitano, in questo caso, a dirottare gli utenti di Internet da siti legittimi verso siti fraudolenti che sono stati realizzati in modo da sembrare quelli originali che la vittima intendeva raggiungere. Ciò si ottiene sfruttando un link inserito nel sito, che afferma di inoltrare il navigatore verso un sito sicuro. Quando la vittima fornisce la propria identità e la password, i ladri sono in grado di memorizzarle per usarle successivamente.

Suggerimenti per un uso sicuro del computer

- Non utilizzare mai computer pubblici per effettuare transazioni finanziarie;
- Installare programmi antivirus e aggiornarli frequentemente;
- Visitare siti il cui indirizzo inizi con il prefisso http:// ;
- Verificare che nel sito vi sia il simbolo di un lucchetto o di una chiave non rotta, in basso nello schermo, che indicano un sito sicuro.

Guard your personal information and documents.

Phising – essentially this is an old con game updated to take advantage of new technology.

Phising means using mail, phone or internet promotions in which thieves falsely claim to be representatives of legitimate enterprises. They provide you with upsetting or exciting information which demands an urgent response in an attempt to scam the user into disclosing private information.

Example – receiving a bogus e-mail from a company that appears to look legitimate asking for account or PIN numbers.

Pharmers – simply redirect as many internet users as possible from legitimate commercial web sites and lead them to malicious sites that are made to look legitimate.

This is done by a “imbedded link” which claims to bring you to a secure site. When users enter their login name and password, criminals are able to capture this information.

Tips for Computer Use

- Never use a public computer for financial transactions.
- Install virus protection software and update it regularly.
- Be careful what e-mails you open
- Look for web sites that begin with <http://>
- Look for an icon of a lock or an unbroken key.

CRIME PREVENTION

TORONTO POLICE SERVICE



EMERGENCY

9-1-1

POLICE NON – EMERGENCY

(416) 808-2222

For more information regarding [IDENTITY THEFT](#) contact the Crime Prevention Officer at your local Police Division

Working Together to Prevent Crime...

SP - E, 2005/08



IDENTITY THEFT

