

“Il furto della privacy”:

come smascherare chi si nasconde dietro una falsa identità per procurare danno ad altri o trarre profitto.

Il furto della privacy può comportare diverse categorie di crimini, ma tutti concorrono a generare uno stress emotivo e psicologico, rabbia, terrore continuo che l'esperienza si ripeta oltre ad un enorme spreco di tempo per risolvere i problemi che ne conseguono quali ripulire la propria reputazione, disfare quanto costruito dai malintenzionati:

Identity cloning

Consiste in una vera e propria sostituzione di persona con l'obiettivo di creare una nuova identità e un nuovo tipo di vita. **Molto diffuso negli Stati Uniti per sposarsi più volte.**

Financial Identity Theft

Reato che implica l'uso dei dati identificativi di un individuo per ottenere crediti, prestiti finanziari, aprire conti correnti in nome della vittima.

Criminal Identity Theft

Si verifica quando si forniscono i dati della vittima per compiere in sua vece atti pubblici illeciti di varia natura: at-tivare nuove carte di credito; attivare telefoni cellulari o altri account.

L'altro caso è la vendetta/ricatto verso colui che si vuole danneggiare (mandando in protesto assegni, non pagando bollette,...)

COME PUO' SUCCEDERE (Comportamenti)

SU INTERNET: basta un computer e un collegamento veloce ad internet, tanto tempo nel navigare e fare ricerche in giro nella rete

ACCESSO AI SERVIZI ON LINE: risultati di una recente indagine hanno dimostrato che gran parte della vulnerabilità è il risultato di una non attenta gestione di codici pin e password per l'accesso ai servizi online, ai sistemi desktop, bancomat e ad altri servizi elettronici e che solo una minima parte dei casi dei furti di identità si verificano su Internet

SOCIAL ENGINEERING: dando informazioni personali mentre si svolgono le normali attività di ogni giorno come, per esempio, compilare un modulo per ottenere la "carta fedeltà" del supermercato, scrivere il numero dei propri documenti su un modulo, firmare la ricevuta della carta -di credito su cui è riportato l'intero numero della carta

TRASHING ovvero l'atto di rovistare nei rifiuti solidi urbani di casa o di una azienda. In pratica il cyber crime scende sulla terra con la conseguenza che le attività fraudo- lente di pirateria virtuale - furto della privacy - inizia nei cassonetti della immondizia: utenze, estratti conto, documenti considerati erroneamente obsoleti, rimanenze di lettere, buste intestate, ricevute di pagamento e via discorrendo, lasciano delle tracce precise che, come in un puzzle, individuano indirizzi, numeri di telefono e recapiti dei loro proprietari.

TELEFONINI: mediante la ricezione di messaggi (SMS, Email) che comunica la vincita di un telefonino di ultima generazione seguendo un link che porta ad una azione di phishing finalizzata ad acquisire i dati degli utenti

QUALE PREVENZIONE

- ◆ Mai fornire informazioni personali sul Web a meno che non siate voi ad aver preso contatto con il soggetto al quale le fornite
- ◆ Fornire informazioni personali sul Web solo attraverso moduli ON-LINE solo se si è sicuri di essere in una connessione protetta controllare che http sia https e ci sia il lucchetto
- ◆ Mai rispondere ad e-mail dove vi si chiedi di inserire il vostro nome utente e password, le vostre coordina-te bancarie, il numero della carta di credito o altro, non cliccate su link dei quali non conosciate l'origine.
- ◆ Usare password sicure e complesse e non usare mai informazioni personali – come il codice fiscale o la data di nascita – come password
- ◆ Nell'utilizzo della carta di credito non associarla mai ad altri dati di identità
- ◆ Prima di firmare una ricevuta di una carta di credito, sarebbe meglio cancellare qualche cifra del numero della carta riportato sopra se la stessa è leggibile prima di firmare e se il negoziante non lo consente, meglio cambiare negozio
- ◆ Controllare sempre gli estratti conto delle carte di credito o del conto corrente bancario

Distruocere ogni carta dalla quale, con certissima pazienza, si possa risalire ai propri dati personali

Le Software House hanno iniziato ad investire nella sicurezza Tutti i Browser hanno implementato i loro sistemi per comunicare visivamente con chi ci si sta connettendo, alcuni altri regalano Suite gratuite con interessanti sistemi per navigare sicuri, un po' tutti intelligentemente hanno capito che creare disaffezione ad Internet è un danno

STRUMENTI LEGISLATIVI DI RIFERIMENTO

Il furto d'identità non è solo diretto al singolo individuo ma anche consiste alla frode all'identità delle organizzazioni private e si chiama **Company ID Theft**: è l'azienda che diventa la vittima diretta del furto di identità spesso a causa dell'insufficiente attenzione nella tutela delle informazioni .

Se i dati rubati riguardano i clienti dell'azienda, questa sarà considerata **responsabile del danno patrimoniale o morale davanti alla legge**, anche per violazione della legge sulla Privacy (tutti i soggetti che trattano dati debbano "adottare idonee e preventive misure di sicurezza che valgano a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi". (art. 31,1). In caso di smarrimento o diffusione o mancata distruzione dei dati trattati, e qualcuno ne entra in possesso, la responsabilità civile e penale cade sull'azienda titolare del trattamento (art.15 comma 1 e 2).

Il danno di immagine per l'azienda è incalcolabile. I clienti penseranno che sia inaffidabile. Questo danno è tanto maggiore quanto più delicate sono le informazioni rubate, come nel caso di dati medici, legali e finanziari.

Art. 494 Codice Penale (Sostituzione di persona)
Richiamato da una sentenza della Corte di Cassazione del dicembre 2007 che ha riconosciuto colpevole un soggetto che aveva aperto un account di posta elettronica utilizzando i dati di altra persona esistente. Condotta penalmente perseguibile in quanto viene pregiudicato il bene tutelato dalla norma: la fede pubblica.

ESPERIENZE E STATISTICHE

Il "furto della privacy" è reso possibile dalla definizione burocratica dell'identità e dai progressi tecnologici: se qualcuno corrisponde ai miei dati, punto per punto in tutte le variabili definite dagli apparati di controllo, se quel qualcuno ha un passaporto, una patente, un tesserino sanitario, tutti a mio nome, con la mia data di nascita e con i numeri giusti, allora quel qualcuno "è me". E tanto più un sistema tecnologico permette di intercettare questi dati, tanto più semplice è il "furto della privacy".

Una laureata in legge racconta che quando arrivò alla tribunale di San Diego (USA) per il suo primo giorno di assistente procuratore, fu ammanettata, arrestata, imprigionata, perquisita a fondo in base a un mandato di arresto a suo nome per traffico di droga e di armi.

La trasmissione indebita dei nostri dati è la ragione per cui siamo sottoposti a una valanga di pubblicità (postale ed @-postale): un giornalista aveva fatto l'abbonamento al *New Yorker* a nome del suo cane; subito dopo il suo cane ha ricevuto una carta di credito platino pre-intestata a suo nome.

Ha avuto notevole risalto sui mass-media, nel mese di novembre 2007, la notizia della clamorosa perdita di una copia su CD dei dati anagrafici di 25 milioni di famiglie britanniche (7,25 milioni di famiglie che avevano richiesto un sussidio): la faccenda ha suscitato apprensione e molte polemiche nel Regno Unito, dove si è temuta un'ondata di furti d'identità.

Fra i molti che non avevano chiara la dinamica dei furti d'identità e non credevano di essere realmente a rischio, sospettando l'ennesima campagna sensazionalista dei giornali (senza PIN e password, cosa volete che succeda, dicono, se qualcuno sa il mio indirizzo, nome, cognome e numero di conto in banca) c'era un popolarissimo conduttore di un programma dissacrante della BBC dedicato al mondo delle automobili.

Il conduttore ha quindi pubblicato le coordinate del suo conto corrente, insieme a qualche indizio per recuperare il suo indirizzo di casa, in un articolo del giornale "The Sun" per dimostrare che tutta la faccenda era una gran montatura e dicendo che la cosa peggiore che gli poteva capitare era che qualcuno versasse dei soldi sul suo conto.

Pochi giorni dopo, un burlone non identificato ha attivato un bonifico automatico di 500 sterline in uscita dal conto del presentatore, a favore di un ente di beneficenza. Ciliegina ironica sulla torta, la risposta alle rimostranze del conduttore la banca ha risposto che **"la banca non può scoprire l'autore del fatto (misfatto) a causa delle leggi sulla protezione della privacy"**.

<u>STATI UNITI</u>	<u>INGHILTERRA</u>	<u>ITALIA</u>
<p>Secondo il <i>Privacy Rights Clearinghouse</i>, negli Stati Uniti ormai ci sono ogni anno circa 750.000 furti della privacy (ma probabilmente sono anche di più, perché spesso i derubati restano a lungo ignari del furto).</p> <p>In un recente sondaggio condotto da <i>Experian e Gallup</i>, un americano su 5 dichiara di avere subito il furto di dati bancari (numero di conto corrente o di carta di credito), e uno su 7 di dati o documenti personali (certificati, patente, codice fiscale, dati previdenziali). Nel complesso il 26% degli americani afferma di aver subito almeno un furto di dati sensibili, 10 punti percentuali in più rispetto a quelli rilevati con un sondaggio analogo del 2006.</p> <p>Il sondaggio rivela anche che:</p> <ul style="list-style-type: none"> • il 21% dei furti di dati personali è purtroppo effettuato da conoscenti; • più della metà degli americani (51%), comincia a temere di subire non solo furti di dati personali, ma anche furti di identità; • il 70% degli americani non ha ancora adottato misure preventive contro i furti della privacy perché non sa che esistono e sono facilmente accessibili; • la scarsa informazione è purtroppo realtà, visto che il 75% della popolazione crede che le truffe con la carta di credito e il furto d'identità siano la stessa cosa. <p>Per ogni "sequestro d'identità", il conto si aggira in media intorno ai 17.000 dollari riferisce <i>The Economist</i>. Ma, soprattutto, il danno sta nel tempo, nella fatica spesi a discolparsi, a dimostrare che "io non ero io". Un gruppo di ricerca californiano ha calcolato che ogni vittima ci mette circa 175 ore (un mese di lavoro a tempo pieno) in due anni a discolparsi completamente e a recuperare i danni finanziari.</p>	<p>Secondo una ricerca divulgata da <i>Experian</i> (gruppo britannico leader mondiale dei servizi informativi sul credito e la prevenzione delle frodi) nell'anno 2007 in più dell'80% dei casi il furto della privacy non è denunciato alla Polizia in tempo utile, per vergogna o imbarazzo, e che fra i casi denunciati, solo il 7% ha portato a successi di polizia immediati, mentre ben il 29% non è stato nemmeno perseguito per carenza di elementi utili alle indagini.</p>	<p>Nel 2006 sono stati stimati oltre 17.000 tentativi di frode creditizia (+55% rispetto al 2005) per un ammontare complessivo pari a circa 80 milioni di euro (era 46,5 milioni di Euro la stima per il 2005)..</p> <p>Nel 93% dei casi le vittime non sono riuscite a denunciare l'autore della frode ma hanno sporto denuncia contro ignoti, e l'importo medio dei casi denunciati è stato di 5.301 Euro. Per quanto riguarda i tempi medi di scoperta delle frodi creditizie mediante furto della privacy, da parte della vittima, sono stimati in 206 giorni. Tale media sale a 580 giorni, nel caso in cui il reato consista nell'attivazione di una carta di credito e si attesta invece a circa 103 giorni nel caso di acquisto a rate con contestuale attivazione di una carta di credito.</p>

... MA SI PUO' REAGIRE.....

sulla base delle indicazioni fornite da Polizia e da operatori che, come la stessa *Experian*, forniscono alle famiglie servizi di prevenzione. In Inghilterra oggi l'**84%** (81% nel 2005) delle famiglie **straccia i documenti prima di gettarli in pattumiera**, il **46%** **protegge i computer di casa** da intrusioni Internet; il **25%** (19% nel 2005) si avvale di **servizi che segnalano** situazioni anomale; il **14%** ha **esteso le coperture assicurative** ai furti di identità.