ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

I Computer Crimes e il quadro normativo in tema di furto di identità

Fabio Di Resta
Esperto di diritto della privacy e delle nuove tecnologie
LLM – ISO 27001 ICT security auditor
Studio legale Di Resta

La riservatezza e l'identità digitale

Riservatezza, protezione dei dati personali

diritto all'oblio (right to oblivion – right to be forgotten)

Quale tutela si applica nell'ambio dell'identità digitale?

Prob. di replicabilità delle informazioni su Internet, diffamazione online, video online, ecc.; non c'è una soluzione universale, ma esiste la necessità di interventi efficaci e tempestivi : sfida del futuro in termini di cooperazione internazionale tra le autorità

Misure preventive del Garante privacy per mitigare il rischio di frodi bancarie e furto di identità

Provvedimenti a carattere generale del Garante

Provv. Garante 25 ottobre 2007, linee guida per i trattamenti relativi al rapporto cliente-banca: indicazioni generali relative al trattamento; principi generali, liceità, pertinenza e correttezza, qualità dei dati

Provv. generale Garante 27 novembre 2008 sulle attribuzioni degli amministratori di sistema: mappatura, separazione dei ruoli e tracciamento degli accessi tramite registrazioni (file di log)

Provv. generale Garante 13 ottobre 2008 sui rifiuti apparecchiature elettriche ed elettroniche (Raee) : misure per la memorizzazione e cancellazione sicura dei dati tramite sistemi di c.d. wiping e memorizzazione sicura al fine di evitare accessi non autorizzati

Recente Provvedimento a carattere generale del Garante privacy

Provv. Garante 12 maggio 2011 - Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - Gazzetta Ufficiale n. 127 del 3 giugno 2011

Scopo: ridurre gli indebiti accessi da parte di dipendenti svolti, in particolare, al fine di produzione in giudizio di documenti contenenti informazioni riservate (di norma, in separazioni giudiziali e procedure esecutive, in particolare, in pignoramenti presso terzi)

Misure prescritte entro 30 gg. dalla pubblicazione in GU: designazione outsourcer; tracciamento delle operazioni bancarie compiute dagli incaricati che operano sui data base contenenti dati bancari dei clienti; conservazione dei log file per almeno 24 mesi; implementazioni di sistemi di alert; audit interno di controllo-rapporti periodici;

Come avvengono i furti di identità? Dati Statistici

FURTO DI IDENTITÀ		
Truffe	***2007***	***2006***
Prestiti Finalizzati	76,26%	86,70%
Carte di Credito	11,72%	7,45%
Prestiti Personali	5,07%	3,06%
Aperture Revolving	3,92%	2,19%
Fidi di Conto	1,20%	-
Mutui	1,20%	0,07%
Leasing	0,62%	0,53%

Fonte: Indagine **Crif** - Espresso 4 Dicembre 2008

Quadro Normativo in tema di furti di identità

In Italia, non c'è una disciplina specifica con riferimento al furto di identità F1

I principali reati applicati: sostituzione di persona, accesso abusivo al sistema informatico, frode informatica, utilizzazione indebita di carte di credito, trattamento illecito dei dati, ecc.

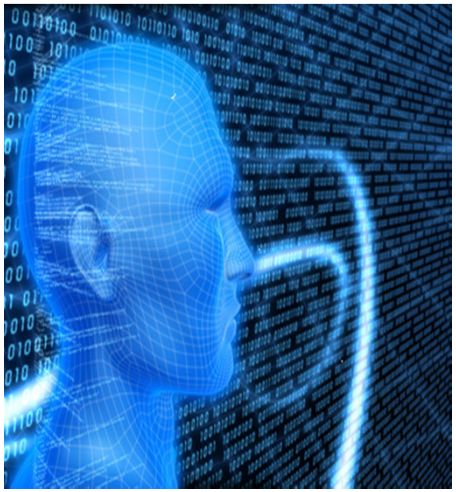
Diapositiva 6

F1 Riferimento Volume insidie Telematiche

Fabio; 19/06/2011

Definizioni

Il furto d'identità o frode da impersonificazione costituisce la fattispecie di frode più diffusa, a tal riguardo si distinguono le seguenti categorie:



impersonificazione totale: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto anche deceduto;

impersonificazione parziale: l'occultamento parziale della propria identità attraverso l'utilizzo, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto;

Sistema pubblico di prevenzione e monitoraggio delle frodi
Obiettivi attesi

Gli obiettivi del decreto sono tre:

- l'istituzione di un sistema di prevenzione e monitoraggio delle frodi ponendosi tra gli obiettivi la lotta al fenomeno delle frodi tramite un sistema di accertamento dell'identità;
- La costituzione di un valido deterrente per i potenziali frodatori;
- La riduzione del contenzioso civile e penale in materia.

Contenuto del Sistema pubblico di prevenzione

I dati oggetto di riscontro (Art. 30 quinquies) sono relativi al credito al consumo, alla dilazione o al differimento di pagamento, finanziamento o facilitazione finanziaria:

a) documenti di identità e di riconoscimento, comunque denominati o equipollenti, ancorché smarriti o rubati;
b) partite IVA, codici fiscali e documenti che attestano il reddito esclusivamente per le finalità perseguite dal presente decreto legislativo;
c) posizioni contributive previdenziali ed assistenziali.

Tali dati di riscontro proverranno da organismi pubblici o privati, tra i quali l'Istituto poligrafico della Zecca dello Stato, l'Agenzia delle entrate, INPS, INAIL, INPDAP.

Sistema pubblico di prevenzione e monitoraggio delle frodi

Il passaggio necessario per rendere efficace il sistema è di far colloquiare la banche dati dei soggetti pubblici.

I soggetti destinatari di tale intervento sono:

oltre le banche e gli intermediari finanziari, i fornitori di comunicazione elettronica, i gestori dei servizi interattivi e ad accesso condizionato, i gestori dei sistemi di informazioni creditizie, le forze dell'ordine e il Ministero dell'Interno.

Ambito di efficacia

Gli ambiti nei quali a regime, il decreto (una volta adottati i decreti ministeriali di attuazione) avrà sicuramente efficacia sono:

prestiti finalizzati;
prestiti personali;
aperture revolving;
mutui;
in genere le frodi di sottoscrizione.

Furto di identità ha un ambito molto più ampio

Tuttavia, come è noto Il **furto di identità** può essere perpetrato anche con **tecniche di ingegneria sociale** e riguarda molto spesso transazioni card not present.

In particolare, il **phishing, il pharming** sono fenomeni in larga ascesa sia in Italia che all'estero e rappresentano una sfida aperta.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Primi 20 reclami
Fonte: Federal Trade Commission (FTC) 2008

RANK	CATEGORY	COMPLAINS	%
1	Identity Theft	313,982	26
2	Third Party and Creditor Debt Collection	104,642	9
3	Shop-at-Home and Catalog Sales	52,615	4
4	Internet Services	52,102	4
5	Foreign Money Offers and Counterfeit Check Scams	38,505	3
6	Credit Bureaus, Information Furnishers and Report Users	34,940	3
7	Prizes, Sweepstakes and Lotteries	33,340	3
8	Television and Electronic Media	25,930	2
9	Banks and Lenders	22,890	2
10	Telecom Equipment and Mobile Services	22,387	2
11	Computer Equipment and Software	21,442	2
12	Business Opportunities, Employment Agencies and Work-at-Home	20,286	2
13	Internet Auction	17,294	1
14	Advance-Fee Loans and Credit Protection/Repair	17,263	1
15	Health Care	16,275	1
16	Auto Related Complaints	14,278	1
17	Travel, Vacations and Timeshare Plans	13,200	1
18	Credit Cards	13,196	1
19	Magazines and Buyers Clubs	10,188	1
20	Telephone Services	9,300	1

Furto di identità tramite sistemi di ingegneria sociale - Phishing

Modus comportamentale del phisher

Il cliente della banca immette le credenziali tramite il link della banca

I dati vengono carpiti dal phisher di solito residente all'estero

Il phisher recluta un financial manager (riciclaggio di denaro – art. 648 bis c.p.) al viene mandato il bonifico con proventi illeciti

Il financial manager preleva il denaro contante, detrae la quota di propria spettanza ed invia di solito tramite Western Union o Money Gram i proventi illeciti al phisher

Giurisprudenza sul phishing

Phisher – principali reati contestabili: sostituzione di persona, frode informatica, indebita utilizzazione di carte di credito, accesso abusivo al sistema informatico, detenzione abusiva di codici di accesso (reati più comunemente contestati anche nella forma di concorso di reati) e anche il reato di trattamento illecito ex art. 167 C.d.P.; normalmente essendo residenti all'estero ci sono difficoltà nell'esecuzione delle sentenze sia a favore delle banche (danno all'immagine, segni distintivi, marchi, ecc.) sia dei clienti vittime del phishing

Financial manager – reato di riciclaggio ex art. 648 bis; sì al riconoscimento del risarcimento del danno verso i clienti; più difficile l'accoglimento delle pretese risarcitorie degli istituti di credito

Cliente – aperta la possibilità di azioni civili nei confronti della banca: risarcimento per mancanza di misure idonee di sicurezza – migliori tecnologie di autenticazione del mercato e azioni di consapevolezza degli utenti ex art. 31 C.d.P., tenendo in conto le norme sull'antiriciclaggio.

Ricerca del financial manager
Money mule (c.d. mulo)

Inviato: venerdì 27 marzo 2009 14.11

Oggetto: Cerchiamo i nuovi lavoratori nella regione!

salve, egregi Signori e Signore!
ricerca i nuovi impegnati per i nuovi impieghi!
Se ancora cerca l'impegno La preghiamo di inviarci il Suo CV e l'informazione di contatto il numero telefonico e l'e-mail e le inveremo tutti i dettagli del posto disponibile.
L'impieghi sono limitati' La preghiamo di inviarci ilSuo CV per valutazione!

Il nostro manager vi chiamera subito!
Conclusione di un accordo, le garanzie sociali, un)salario|stipendio) meritato e l'orario di lavoro variato part-time
jobb.marco@gmail.com

Aspettiamo i Suoi CV!

Grazie per l'attenzione

Fabio Di Resta
Esperto di diritto della privacy e delle nuove tecnologie
LLM – ISO 27001 ICT security auditor
Studio legale Di Resta
Email: **info@studiolegalediresta.it**