Insidie nell'utilizzo del web ed aspetti legali e pratici dell'e-commerce

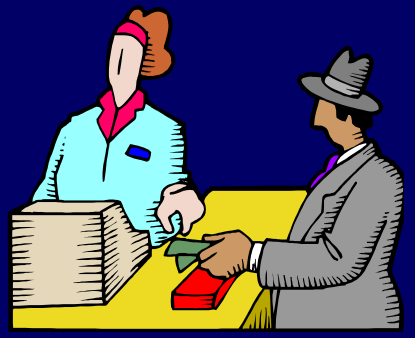
Brescia 28 giugno 2012

Dott. Antonio Fiorentino

L’impiego della Carta di Credito

Prelievo di denaro contante

Acquisti di beni e servizi presso esercenti convenzionati



Acquisti di beni e servizi attraverso Internet

INDEBITO USO DI CARTE DI CREDITO

Normativa
Attività di contrasto

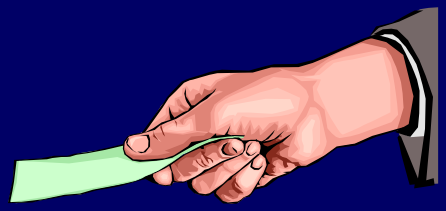
L'emissione delle Carte di Credito

CIRCUITO

EMITTENTE

ESERCENTE CONVENZIONATO

TITOLARE



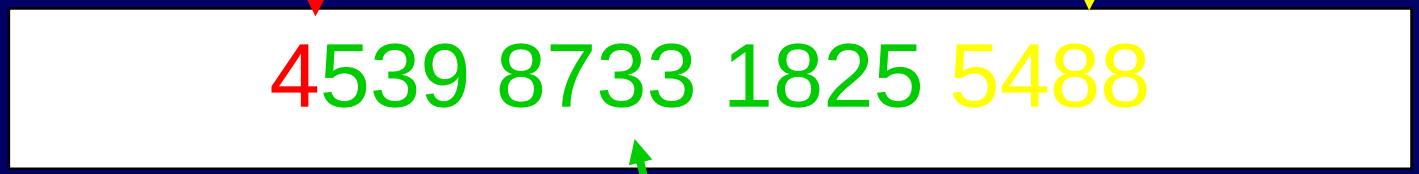
PAN: Personal Account Number

CIRCUITO:

4 = VISA

5 = MASTERCARD

TITOLARE



EMITTENTE:

Banca o Consorzio Bancario che ha emesso la Carta di Credito

Tipologie di frodi: *Plastic fraud*

- Uso indebito di carta smarrita o rubata

- Contraffazione delle carte

  -alterazione/falsificazione del supporto plastico

  -duplicazione della banda magnetica (skimming)

  -presenza dello skimmer accanto a quello usato per fini commerciali o presenza di uno skimmer portatile: la carta viene strisciata due volte

- Mancata ricezione della carta/intercettazione della carta durante la spedizione postale

Tipologie di frodi: *Card-not-present fraud*

- Utilizzo illegittimo del codice della carta

- Identità falsa o rubata

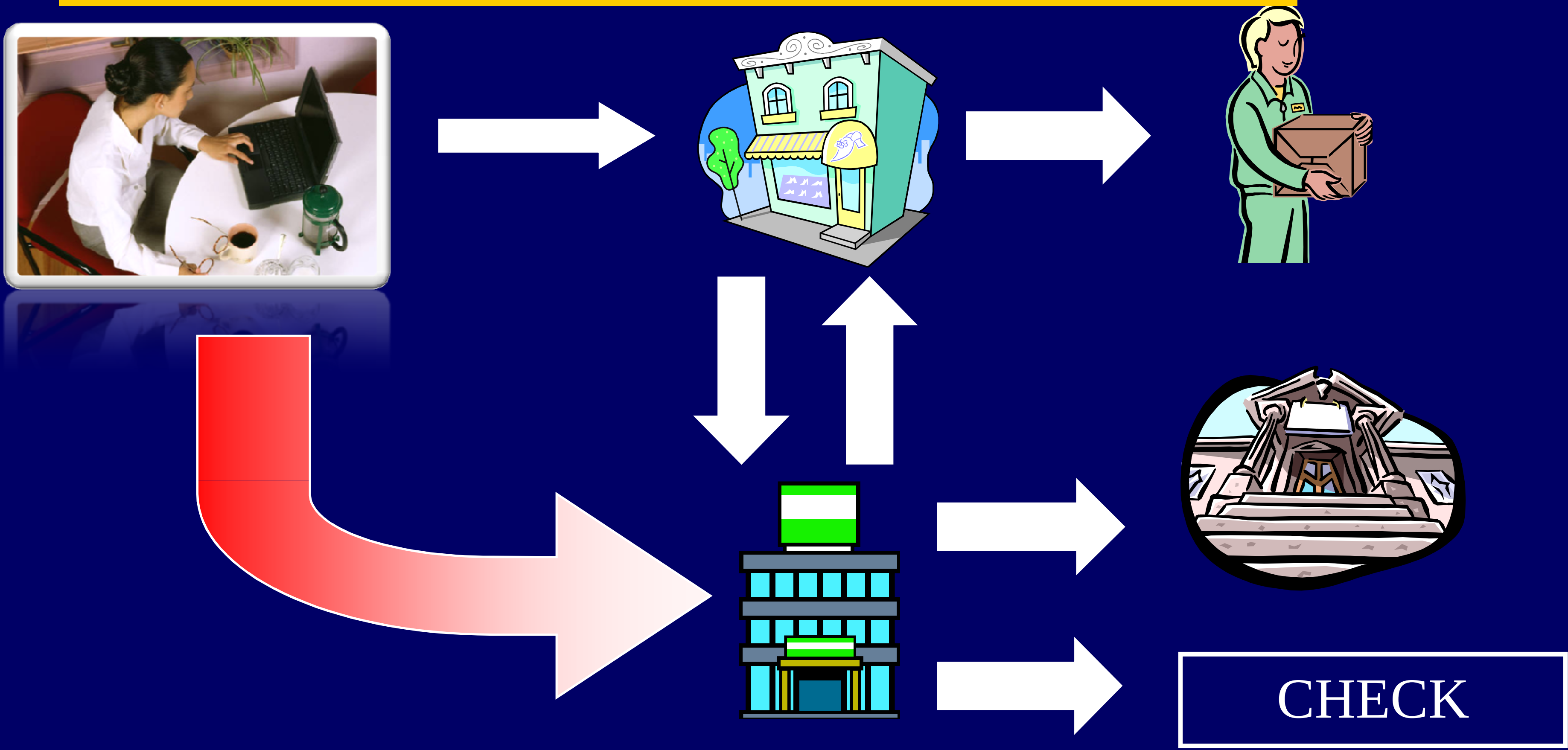
  -creazione di dati identificativi totalmente inventati

  -furto di dati identificativi veri

- Frode con numeri di carta inventati (carding matematico)

- "Ship to address" fraud: dopo che una valida transazione è stata posta in essere dall'effettivo titolare della carta, i truffatori carpiscono nel sito del fornitore le informazioni necessarie per assumere l'identità della vittima, modificando l'indirizzo a cui la merce sarà inviata

Il pagamento con Carta di Credito



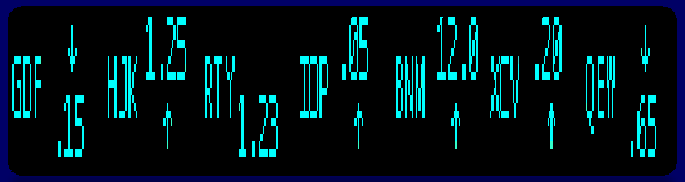
[illegible] la Banca effettua i controlli di autenticità.

3 – Il negozio virtuale pertanto provvede all'invio della merce acquistata.

[illegible] PROTOCOLLO CRIPTATO.

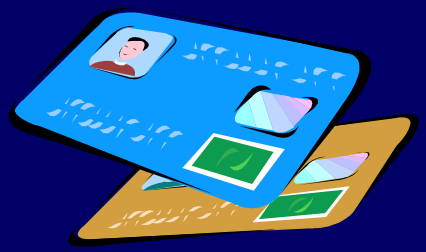
[illegible] che pertanto autorizza l'E-Shop ad accettare l'acquisto.

I controlli effettuati dalla Banca



Rispondenza del PAN (numero a 16 cifre) con l'algoritmo di creazione

Presenza nella STOP LIST

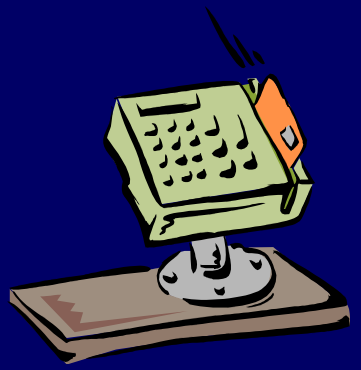


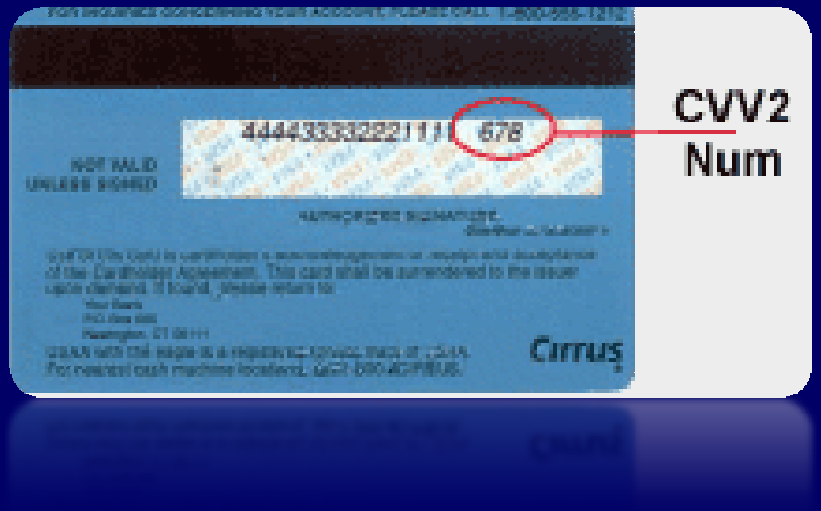
Verifica Assegnazione Carta e rispondenza della Data di Scadenza

Caratteristiche dei pagamenti elettronici

- Riservatezza della informazioni veicolate: adozione di sistemi di crittografia
- Autenticazione del venditore nei confronti dell'acquirente e dell'acquirente nei confronti del venditore: implementazione di sistemi che certifichino l'identità degli attori coinvolti (certificati digitali)
- Non ricusabilità dell'ordine trasmesso: presenza di enti "terzi" alla transazione che ne certifichino l'effettivo svolgimento (enti certificatori)
- Integrità dei dati trasportati: utilizzo di procedure di "digital enveloping" attraverso l'uso di certificati digitali

Le contromisure adottate





Richiesta, oltre che del PAN e della data di scadenza, anche del codice CVV2 (o CVC2) posto sul retro della Carta di Credito.

Acquisizione fraudolenta di Carte di Credito

Furto e/o Smarrimento
della Carta di Credito

Intrusione informatica

Punto di Compromissione

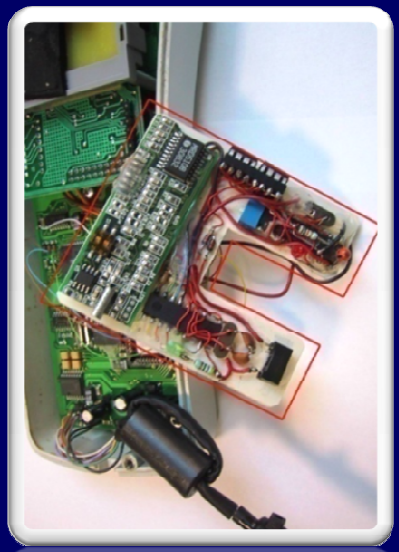
Generatore Software
(*carding*)

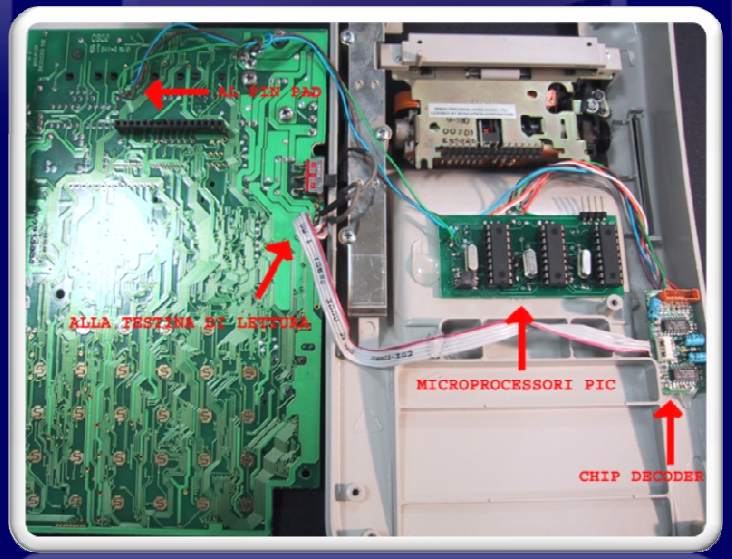
Vari tipi di “Skimmer” manuali

Vari tipi di “Skimmer” manuali


VIOLAZIONE DEL SIGILLO DI SICUREZZA
DASISTEMI
WARRANTY IS VOID IF
OR DAMAGED

Manomissione PIN Pad e POS



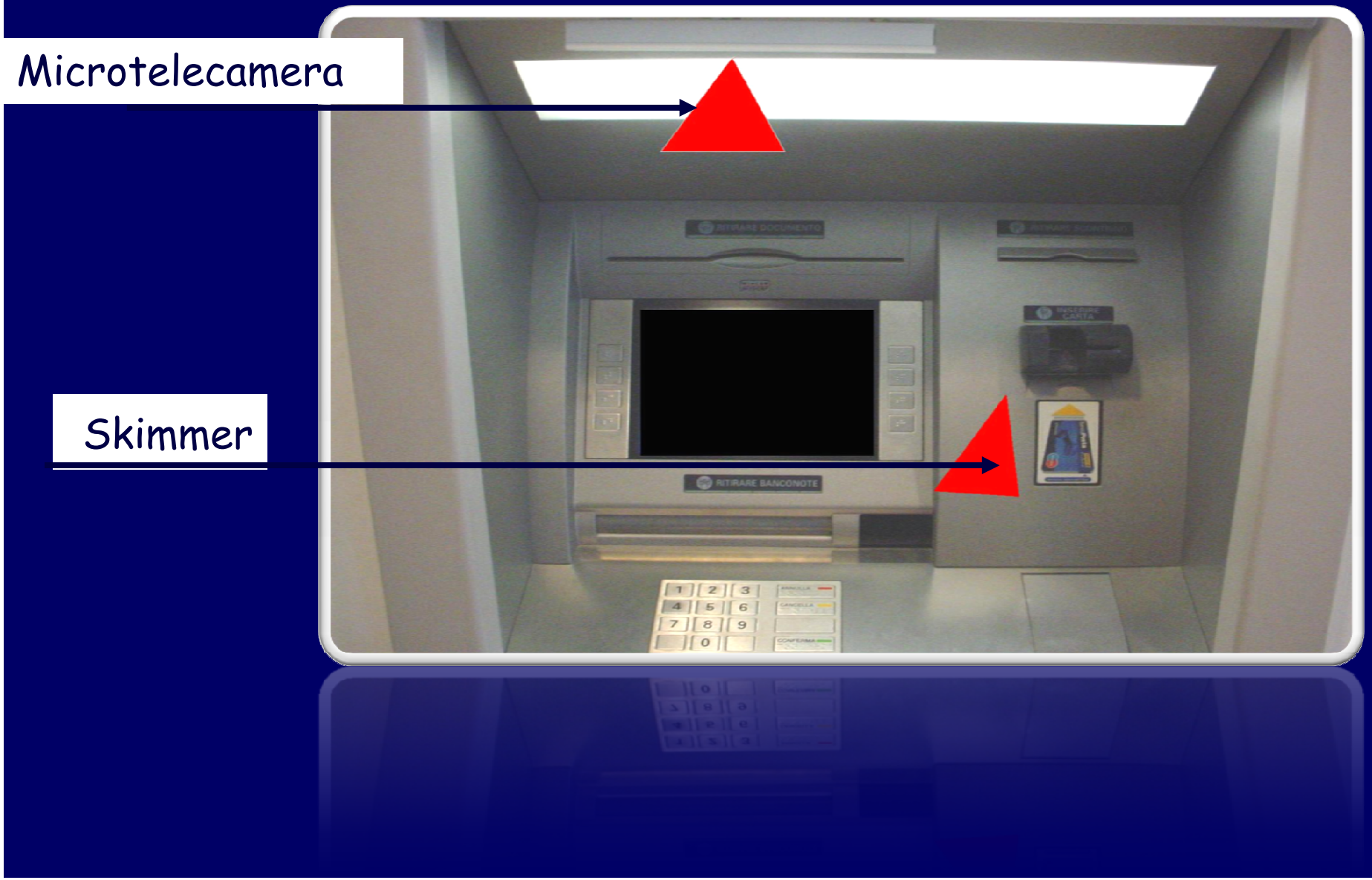


CLONAZIONE PRESSO BANCOMAT CON L'UTILIZZO DI UNO SKIMMER E DI UNA FALSA TASTIERA

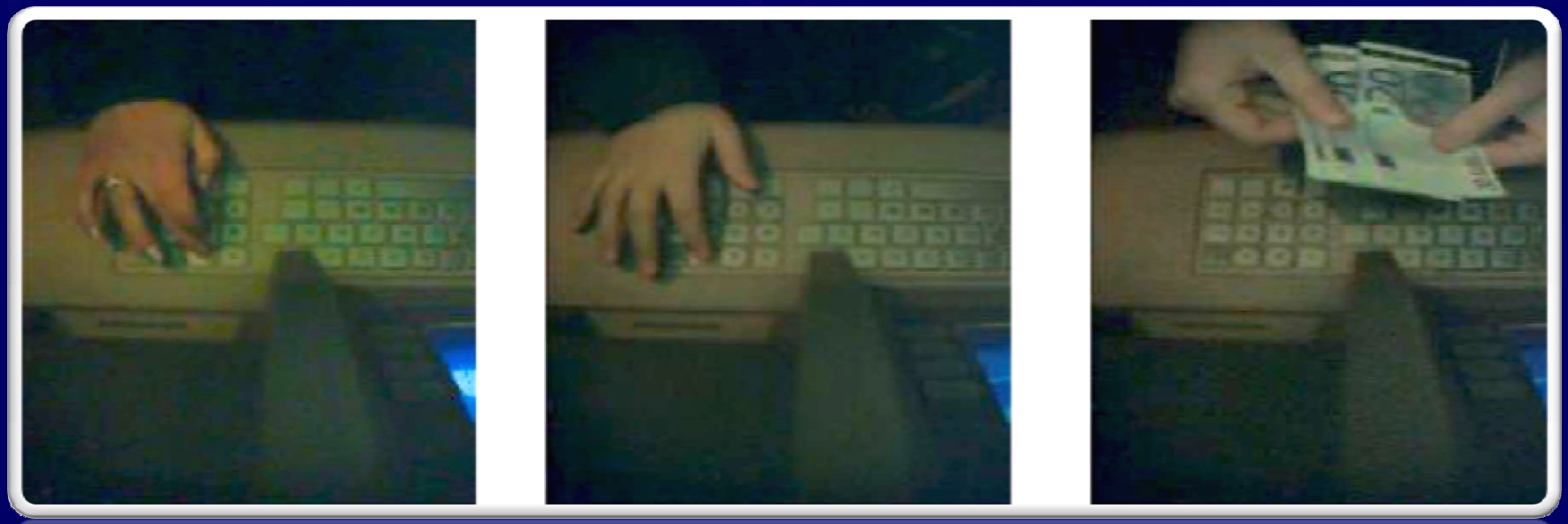
Fattura Straniera

CLONAZIONE PRESSO BANCOMAT CON L'UTILIZZO DI UNO SKIMMER E DI UNA MICROTELECAMERA CELATA ALL'INTERNO DI UN CONTENITORE PUBBLICITARIO

CLONAZIONE PRESSO BANCOMAT CON L'UTILIZZO DI UNO SKIMMER E DI UNA MICROTELECAMERA CELATA ALL'INTERNO DI UNA CANALINA



PARTICOLARE DI UNA MICROTELECAMERA E IL FILMATO DI UN CLIENTE RIPRESO MENTRE DIGITA IL CODICE PIN E PRELEVA IL DENARO

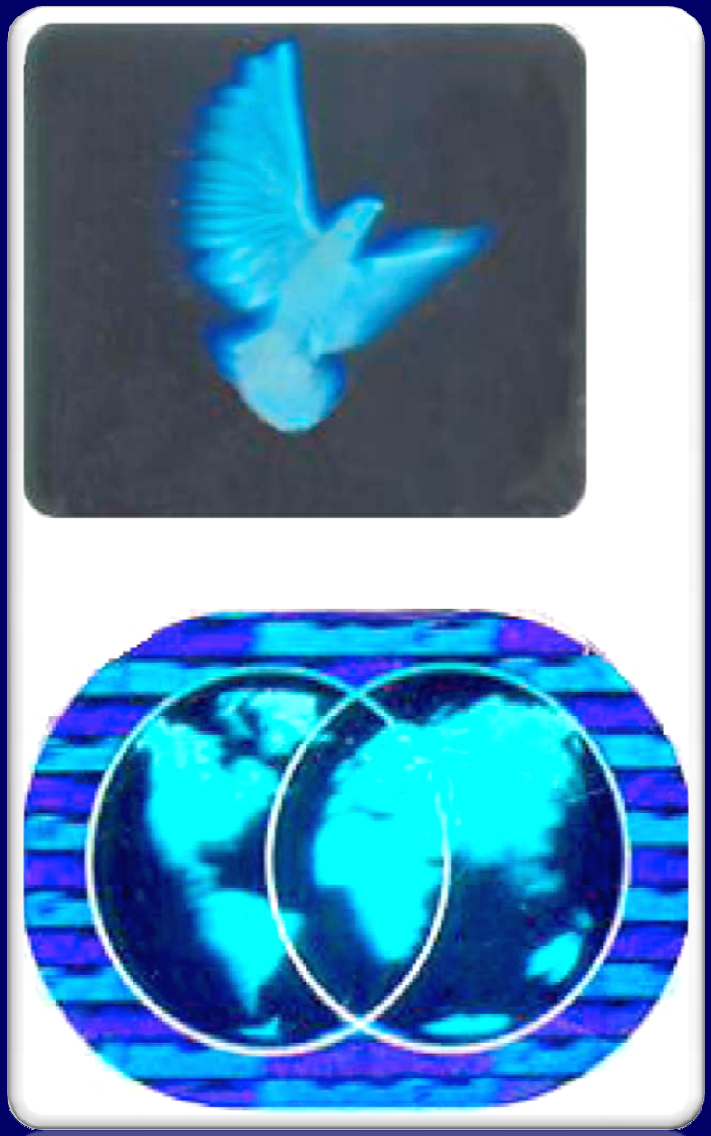


Skimmer manuale

Stampante termografica con scrittore Motorizzato di bande magnetiche

COME INDIVIDUARE UNA CARTA FALSA O CLONATA

Eurocard/MasterCard: A destra della data di scadenza è impresso a rilievo il carattere **MC**.
Visa: La lettera **V** è impressa a rilievo a destra della data di scadenza ed è leggermente inclinata a destra.



Ologramma

Visa: L'ologramma sul fronte della carta rappresenta una colomba che sembra volare quando si muove la carta.

Eurocard/MasterCard: l'ologramma sul fronte della carta rappresenta due mondi che s'intersecano dai quali, muovendo la carta, appare la mappa dei continenti.

In caso di contraffazione l'ologramma è assente o non aderisce perfettamente alla carta e non è iridescente

LA MICROSTAMPA

Le carte Visa ed Eurocard/MasterCard presentano un numero di quattro cifre, "detto stampa" stampigliato sotto le prime quattro cifre del numero di carta.

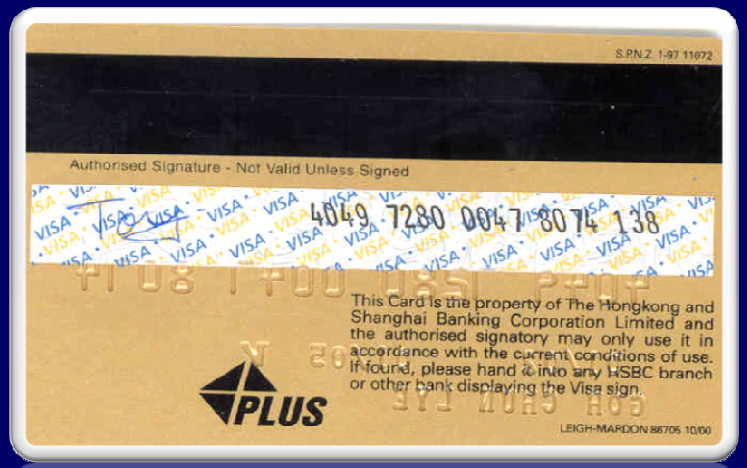
Le stesse devono essere impresse a rilievo e uguale alle prime quattro cifre che compongono la carta.

L'assenza o la non corrispondenza è indice di contraffazione della carta.

LA MICROSTAMPA

È importante verificare che nello spazio riservato alla firma sia presente una microscrittura diagonale in colori diversi, inclinata di 45° da sinistra a destra, che riproduce la dicitura del circuito d'appartenenza (Visa e Mastercard).

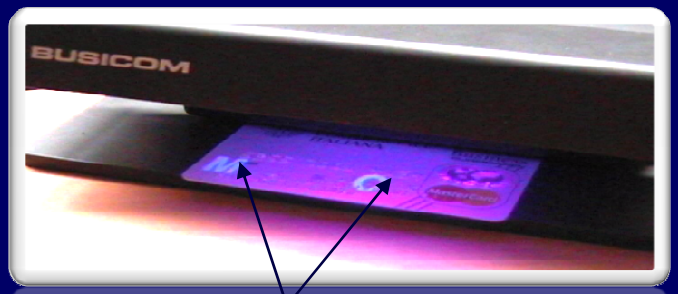
Devono essere riportati, inoltre, incisi, il codice completo della carta di credito o solo le ultime quattro cifre.



"LAMPADA WOOD" UNO STRUMENTO PREZIOSO

PONENDO LA CARTA DI CREDITO SOTTO LA LAMPADA DI WOOD COMPARIRANNO:

Per Visa una colomba uguale all'ologramma



Per Mastercard una "M" e una "C"

Per American Express la scritta AMEX

Per Diners Club l'immagine del logo posto sulla sinistra della carta stessa

Verificare che il numero di carta stampato sullo scontrino sia lo stesso numero impresso sulla carta, in questo modo, infatti, è possibile identificare un'eventuale differenza fra i dati inseriti nella banda e quelli presenti sul fronte della carta.

Le sanzioni penali

Articolo 55 del D.lvo 231/07

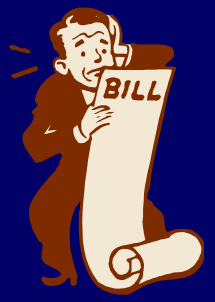
Chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da lire seicentomila a lire tre milioni.

Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi,

ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

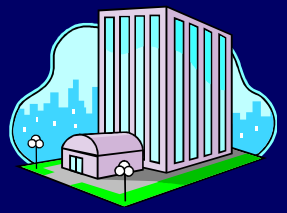
Frodi con carte di credito

I soggetti coinvolti:



Il titolare della Carta di Credito che controllando l'estratto conto ha notato acquisti addebitati, ma non effettuati da lui.

La società che gestisce il sito di commercio elettronico, alla quale vengono stornati gli importi disconosciuti.



La società emittente la carta di credito, che viene a conoscenza dell'illecito.

Procedura di blocco del titolo di credito e verifica per avviare richiesta di rimborso

Dal titolare frodato è importante acquisire:

L'estratto conto, evidenziando le spese genuine e le spese contestate.

Attività di indagine

Dal gestore del e-shop è importante acquisire:

Nome e Cognome indicati dall'acquirente (anche se falsi)

Indirizzo di consegna della merce

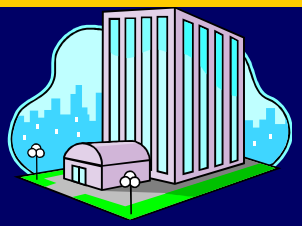
Recapiti indicati : telefoni, indirizzi email, cellulari, ecc

Indirizzo IP completo di data ed ora della connessione

I beni ed i servizi acquistati

Verificare se esistono altri acquisti effettuati dal medesimo acquirente o che riconducono al medesimo autore

Attività di indagine



Dalla società emittente occorre acquisire:

Elenco delle Carte di Credito utilizzate.

Elenco dei negozi virtuali presso i quali la stessa carta è stata utilizzata.

Indirizzo I.P. completo di data ed ora della connessione

Verificare se esistono altri acquisti effettuati dal medesimo acquirente o che riconducono al medesimo autore

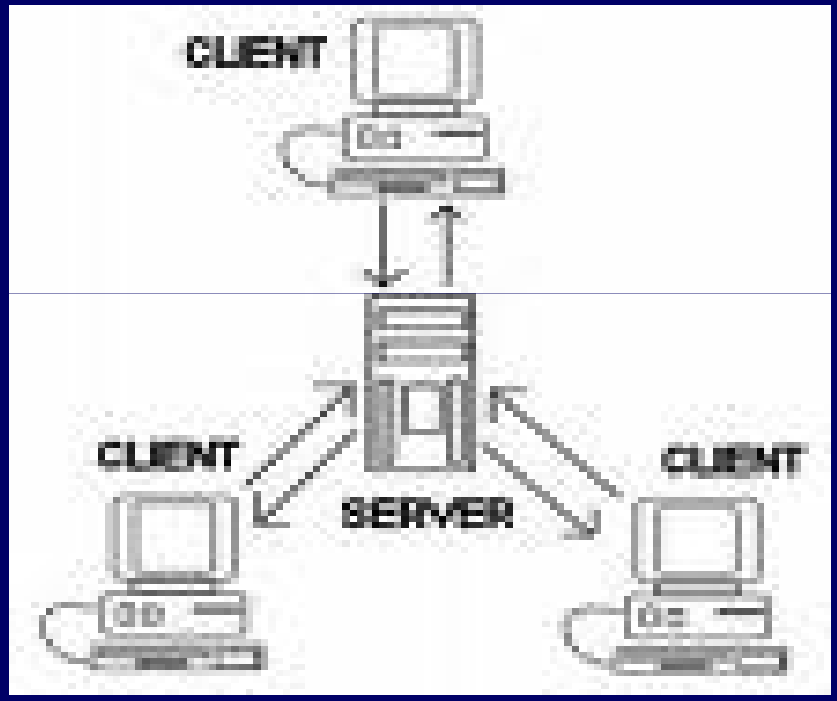
IL CONSUMATORE NELLA "RETE"

Quando si concludono delle transazioni commerciali sulla rete internet bisogna fare i conti con l'indeterminatezza della virtualità e perciò si suggerisce prudenza e zelo nelle diverse fasi contrattuali;

Prima di fare un acquisto telematico consultare i motori di ricerca per trovare informazioni utili a definire il livello di affidabilità del contraente

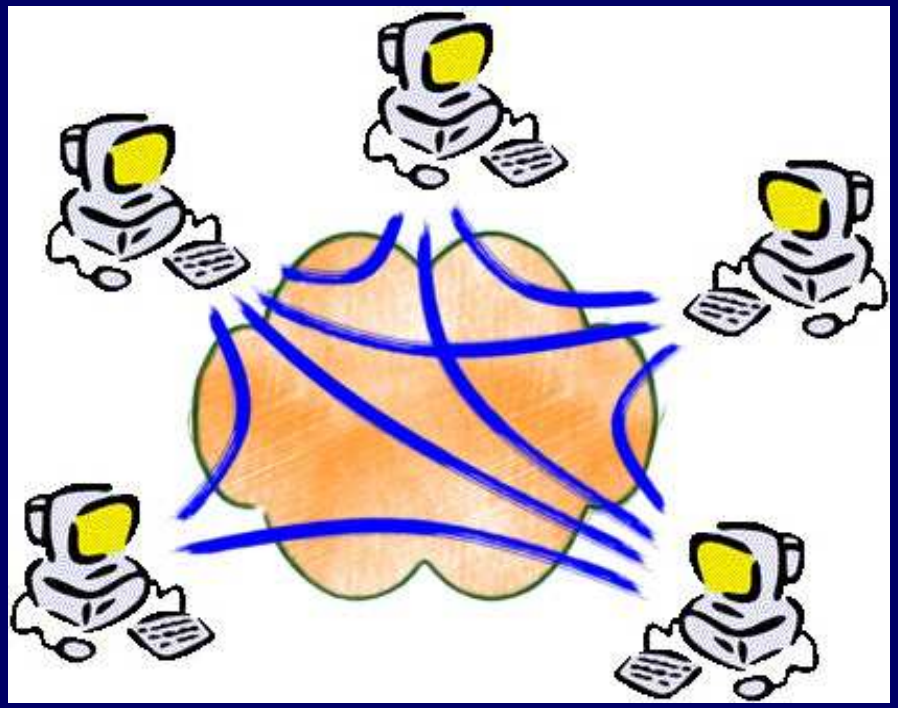
RETE INTERNET

SISTEMA CLIENT/SERVER



RETE INTERNET

SISTEMA P2P



IP ADDRESS

- Un **Indirizzo IP** (dall'inglese **Internet Protocol address**) è un numero che identifica univocamente un dispositivo collegato a una rete che utilizza Internet Protocol come protocollo di comunicazione. Un indirizzo IP assolve essenzialmente a due funzioni principali: identificare un dispositivo sulla rete e fornirne il percorso di raggiungibilità.
- ES. 79.87.132.121

CASO PEPPERMINT E CONSIDERAZIONI TECNICHE E LEGALI SULL'IP ADDRESS

- INIZIALMENTE IL TRIBUNALE AVEVA DECISO CHE L'IP ADDRESS NON E' UN DATO CHE RILEVA AI FINI DELL'APPLICAZIONE DELLA NORMATIVA SULLA PRIVACY

Caso PEPPERMINT

- raccolta e nell'elaborazione automatizzata, anche nell'ambito di banche dati, di innumerevoli informazioni di carattere personale (IP E RELATIVI FILE DI LOG) estratte tramite reti peer-to-peer per mezzo di un *software* denominato "*file sharing monitor*
- Contestazione della violazione dei diritti derivanti dalla produzione di fonogrammi e si è proposta una risoluzione bonaria, alternativa anche alla denuncia in sede penale, basata sul rispetto di alcune condizioni comprensive di un versamento di 330 euro.

Caso PEPPERMINT anomalia

- Un’azienda privata aveva ottenuto dei dati telematici con provvedimento del Tribunale civile
- I decreti erano stati notificati ai provider che in alcuni casi avevano contestato la validità di tale procedura;
- I privati che hanno ricevuto la contestazione hanno eccepito violazione della privacy

Caso PEPPERMINT data retention

- Successivamente il Tribunale ha statuito che i fornitori di servizi di comunicazione elettronica, allo stato della legislazione vigente, non possono comunicare in sede giurisdizionale civile a Peppermint e Techland i nominativi degli interessati ritenuti responsabili di violazioni del diritto d'autore in rete. Ciò, stante la specifica disciplina della conservazione dei dati di traffico, prevista solo per finalità di accertamento e repressione di reati (art. 132 del Codice della privacy e d.lvo 109/09)

CASO PEPPERMINT
data retention e orientamento giurisprudenziale

- La Corte di giustizia delle Comunità europee ha confermato che il diritto comunitario consente agli Stati membri di circoscrivere all'ambito delle indagini penali o della tutela della pubblica sicurezza e della difesa nazionale -a esclusione, quindi, dei processi civili- il dovere di conservare e mettere a disposizione i dati sulle connessioni e il traffico generati dalle comunicazioni effettuate durante la prestazione di un servizio della società dell'informazione. La Corte ha rilevato che anche i dati di traffico conservati per finalità di fatturazione non possono essere utilizzati in *"controversie diverse da quelle insorgenti tra i fornitori e gli utilizzatori, relative ai motivi della memorizzazione dei dati avvenuta per attività previste dalle disposizioni [dell'art. 6 della direttiva 2002/58/Ce*

CASO PEPPERMINT considerazioni del garante

- Il trattamento degli IP è risultato viziato sotto il profilo della trasparenza e della correttezza, posto che non è stata fornita alcuna informativa preliminare agli utenti. Dalla descrizione resa dalle società sul funzionamento del software *fsm* si è potuto rilevare che, mentre gli indirizzi Ip sono stati acquisiti da un terzo rispetto agli utenti (il *provider*), gli altri dati (ossia, i *file* offerti in condivisione, data e ora del *download*) sono stati raccolti direttamente presso gli interessati.
- Il Tribunale di Roma ha riconosciuto, per tali informazioni (quindi anche l'IP ADDRESS), la natura di *"dati personali"* relativi a utenti identificabili i quali dovevano essere informati di tale ulteriore e inatteso trattamento

CONCLUSIONI CHE DERIVANO DAL PUNTO DI VISTA DELLE PARTI CIVILI

- IMPOSSIBILITA' DI ACQUISIRE I DATI TELEMATICI (IP e FILE DI LOG) IN CASI INVESTIGATIVI DI CARATTERE CIVILISTICO (ES. controversie coniugali, infedeltà dei dipendenti di un'azienda, ecc) e INADEMPIMENTI CONTRATTUALI DERIVANTI DA CONTRATTI A DISTANZA

CONSEGUENZA ....

In caso di inadempimenti o adempimenti difformi e/ parziali molti utenti tendono a rivolgersi alla giustizia penale, presentando denunce per truffa;

Tale tendenza si rafforza in considerazione della nota lentezza e farraginosità della giustizia civile.

Art. 640 c.p. (truffa)

Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

Il delitto di truffa rientra nella categoria dei reati a forma vincolata, non ogni attività ingannevole configura questo reato odioso, ma solo quella che caratterizza la presenza di artifici o raggiri richiesti espressamente dalla norma incriminatrice.

COMMERCIO ELETTRONICO

- L'espressione commercio elettronico (e-commerce) si riferisce all'insieme delle operazioni per la commercializzazione di beni e servizi tra un professionista (offerta) e consumatore (domanda), realizzate tramite Internet;
- In questa accezione rientrano in generale tutti gli scambi di beni e servizi attraverso la rete globale.

TIPOLOGIE DI E-COMMERCE

- Il Commercio elettronico tra aziende (Business-to-Business)
- Il Commercio elettronico per i consumatori finali (Business-to-Consumer)
- Il Commercio elettronico tra consumatori finali (Consumer-Consumer)
- Il Commercio elettronico intra-aziendale (Intra-Business)

NORMATIVA DI RIFERIMENTO

- D.LVO 70/03 ATTUAZIONE DIRETTIVA COMUNITARIA 31/2000
- D.Lvo 114/98 – art. 18 (…vendita per corrispondenza, televisione o altri sistemi di comunicazione…)
- L'art. 15, comma 2, della legge 15 marzo 1997, n 59 attribuisce valore legale ad ogni effetto ai documenti, agli atti, ai dati, ai contratti formati dai privati e dalla pubblica amministrazione mediante strumenti informatici, trasmessi per via telematica …
- D.lvo 50/92
- D.lvo 185/99
- D.Lvo 206/05 (codice del consumo)

Aspetti legali dell'e-commerce

Affinché ai contratti telematici sia riconosciuta validità giuridica, occorre:

- Che al cliente venga consentito di utilizzare il sistema solo in modalità dimostrativa, così da non compiere inavvertitamente operazioni che lo potrebbero giuridicamente vincolare;

- Che sia prevista su ogni pagina visualizzata la possibilità di abbandonare la stipulazione e di cancellare i dati inseriti;

- Fare in modo che il cliente dia inequivocabilmente il proprio consenso;

- Accertarsi dell'identità del cliente.

-

Aspetti legali dell’e-commerce

- Il contratto on-line si considera concluso quando il destinatario del servizio ha ricevuto dal fornitore, per via elettronica, l’avviso di ricevimento (solitamente una mail) dell’accettazione dell’ordine.

Aspetti legali dell'e-commerce

- Il codice del consumo prevede particolari oneri informativi a carico del venditore e la possibilità per il compratore di esercitare il diritto di recesso senza alcuna penalità e senza dover fornire spiegazioni.

Aspetti legali dell’e-commerce

secondo il codice al consumo il venditore dovrà assolvere a precisi obblighi di informativa nei confronti del consumatore *" in tempo utile e comunque prima della conclusione di qualsiasi contratto a distanza* ", riguardanti:

- l'identità del fornitore (incluso il suo indirizzo geografico)
- le caratteristiche essenziali del prodotto o del servizio
- le modalità di consegna e impiego
- il tipo di pagamento e il prezzo comprensivo di tasse, le imposte e le spese di consegna
- modalita' e tempi di restituzione o di ritiro del bene in caso di esercizio del diritto di recesso;

ASPETTI LEGALI E-COMMERCE

- Per quanto riguarda l'esecuzione dell'ordine, salvo diverso accordo tra le parti, il fornitore deve eseguire l'ordinazione entro 30 giorni a decorrere dal giorno successivo a quello in cui il consumatore ha trasmesso la richiesta, mentre i termini utili per poter esercitare il diritto di recesso è di dieci giorni.

Lealtà contrattuale del professionista

Le notizie informative devono essere fornite in modo chiaro e comprensibile, con ogni mezzo adeguato alla tecnica di comunicazione a distanza impiegata, osservando in particolare i principi di buona fede e di lealta' in materia di transazioni commerciali, valutati alla stregua delle esigenze di protezione delle categorie di consumatori particolarmente vulnerabili.

CASO STUDIO – SITO DI ECOMMERCE SISTEMI DI LUCE

Vedere PDF PROVVEDIMENTO AGCM 23327/12 -

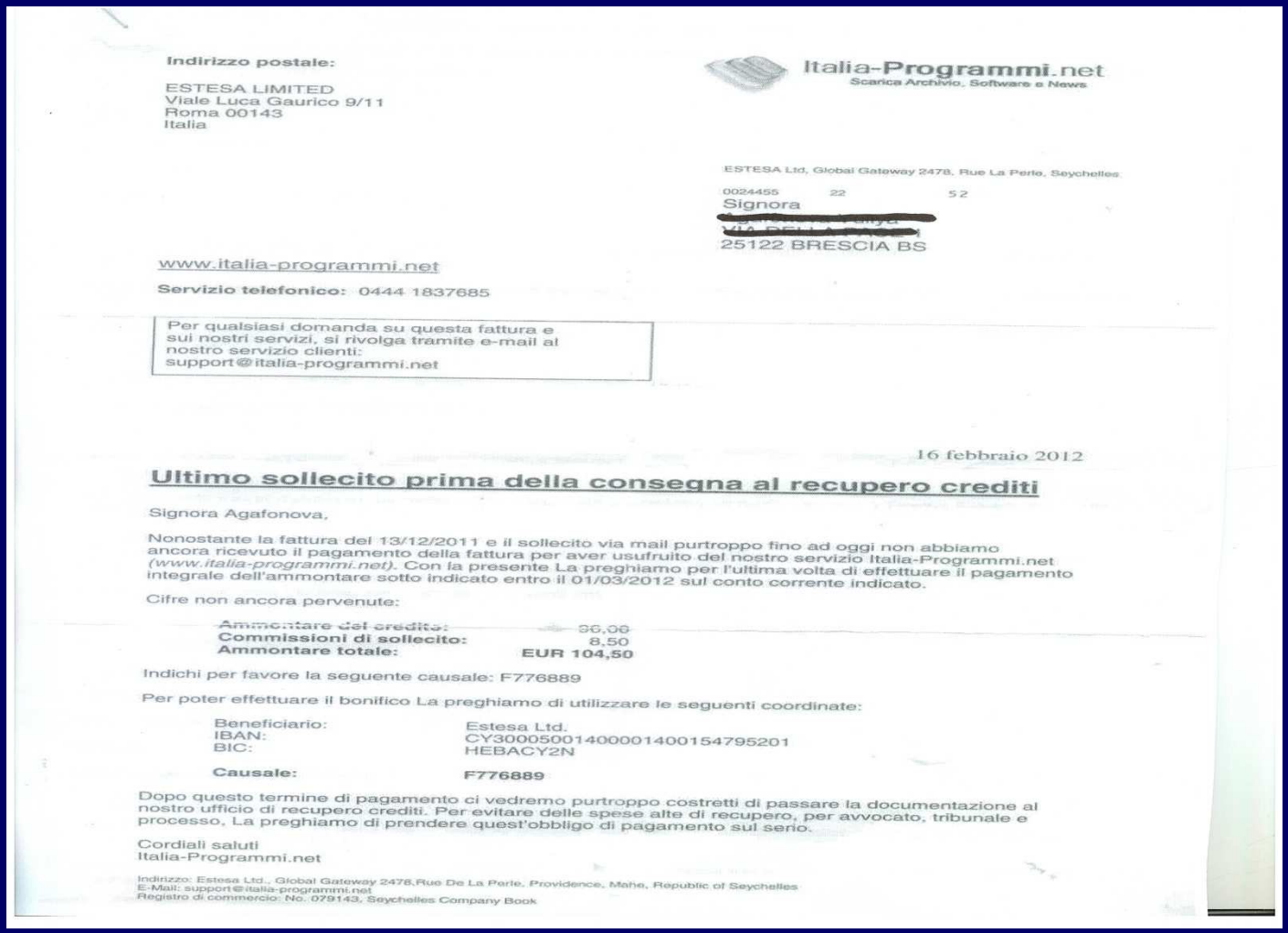
DIRITTO DI RECESSO
ART. 64 CODICE CONSUMO

….il consumatore ha diritto di recedere senza alcuna penalita' e senza specificarne il motivo, entro il termine di dieci giorni lavorativi…

RECESSO – MODALITA’

comunicazione scritta alla sede del professionista mediante lettera raccomandata con avviso di ricevimento. La comunicazione puo' essere inviata, entro lo stesso termine, anche mediante telegramma, telex, posta elettronica e fax, a condizione che sia confermata mediante lettera raccomandata con avviso di ricevimento entro le quarantotto ore successive

CASO FRODE ITALIA-PROGRAMMI.NET
RECESSO NON NECESSARIO PER INESITENZA DI ACCORDO CONTRATTUALE



Indirizzo postale:

ESTESA LIMITED
Viale Luca Gaurico 9/11
Roma 00143
Italia

Italia-Programmi.net
Scarica Archivio, Software e News

ESTESA Ltd, Global Gateway 2478, Rue La Perle, Seychelles

0024455 22 52
Signora
[redacted]
25122 BRESCIA BS

www.italia-programmi.net

Servizio telefonico: 0444 1837685

Per qualsiasi domanda su questa fattura e sui nostri servizi, si rivolga tramite e-mail al nostro servizio clienti:
support@italia-programmi.net

16 febbraio 2012

Ultimo sollecito prima della consegna al recupero crediti

Signora Agafonova,

Nonostante la fattura del 13/12/2011 e il sollecito via mail purtroppo fino ad oggi non abbiamo ancora ricevuto il pagamento della fattura per aver usufruito del nostro servizio Italia-Programmi.net *(www.italia-programmi.net)*. Con la presente La preghiamo per l'ultima volta di effettuare il pagamento integrale dell'ammontare sotto indicato entro il 01/03/2012 sul conto corrente indicato.

Cifre non ancora pervenute:

~~Ammontare del credito:~~	~~96,00~~
Commissioni di sollecito:	8,50
Ammontare totale:	**EUR 104,50**

Indichi per favore la seguente causale: F776889

Per poter effettuare il bonifico La preghiamo di utilizzare le seguenti coordinate:

Beneficiario:	Estesa Ltd.
IBAN:	CY30005001400001400154795201
BIC:	HEBACY2N
Causale:	**F776889**

Dopo questo termine di pagamento ci vedremo purtroppo costretti di passare la documentazione al nostro ufficio di recupero crediti. Per evitare delle spese alte di recupero, per avvocato, tribunale e processo, La preghiamo di prendere quest'obbligo di pagamento sul serio.

Cordiali saluti
Italia-Programmi.net

Indirizzo: Estesa Ltd., Global Gateway 2478,Rue De La Perle, Providence, Mahe, Republic of Seychelles
E-Mail: support@italia-programmi.net
Registro di commercio: No. 079143, Seychelles Company Book

Nuovi strumenti a tutela del consumatore nelle norme di disciplina dei servizi di pagamento

Il decreto legislativo nr. 11/10 ha attuato una direttiva europea che disciplina i servizi di pagamento.

Le disposizioni attuative emanate dalla Banca d'Italia sottolineano un'esigenza fondamentale nell'ambito dei sistemi di pagamento digitali:

" "

disciplina servizi pagamento

La fase genetica di un'operazione di pagamento è quella più delicata per la sua corretta esecuzione: per tale motivo il legislatore ripartisce nel dettaglio gli obblighi del prestatore di servizi di pagamento e dell'utilizzatore nel processo di autorizzazione all'esecuzione di un'operazione di pagamento. Proprio per evitare operazioni fraudolente vengono richiesti specifici accorgimenti, oltre che ai prestatori, anche agli utilizzatori di servizi di pagamento, in particolare per quel che riguarda la gestione dei codici di accesso all'utilizzo di strumenti o di conti di pagamento. Al fine di preservare la fiducia del pubblico negli strumenti di pagamento più efficienti (come ad esempio le carte di pagamento e gli addebiti diretti), al ricorrere di determinate condizioni agli utilizzatori di tali strumenti sono riconosciute forme di tutela rafforzate.

Disciplina sistemi di pagamento

Tutti i prestatori di servizi di pagamento si dotano di un adeguato e robusto processo di gestione dei rischi che permetta di identificare, valutare, misurare, monitorare e mitigare le minacce di natura tecnologica. Con l'obiettivo di mitigare i rischi individuati, tale processo deve individuare un insieme di misure di sicurezza e di controlli appropriati, in grado di assicurare gli obiettivi di confidenzialità, integrità, disponibilità dei sistemi informativi e dei dati ad essi associati.

Gestione dei servizi di pagamento obblighi a carico dei prestatori

Predisporre adeguati processi di gestione dei rischi associati alle tecnologie utilizzate, tra i quali:

- malfunzionamenti nei sistemi informatizzati interni;
- difetti delle procedure software e dei sistemi operativi;
- guasti dei componenti hardware;
- limitata capacita dei sistemi di elaborazione e trasmissione;
- vulnerabilità delle reti di telecomunicazione;
- debolezza del sistema dei controlli e delle misure di sicurezza;
- sabotaggi;
- attacchi da parte di soggetti esterni;
- tentativi di frode.

ORIENTAMENTO DI GARANZIA PER IL CONSUMATORE

Le operazioni di pagamento autorizzate eseguite su iniziativa del beneficiario del pagamento o per il suo tramite richiedono per il pagatore forme rafforzate di tutela nelle ipotesi in cui il trasferimento, pur se autorizzato, non corrisponda alle sue ragionevoli aspettative. Le operazioni in questione sono costituite dagli addebiti diretti e da quelle effettuate con carta di pagamento.

ORIENTAMENTO DI GARANZIA PER IL CONSUMATORE

Il diritto al rimborso è riconosciuto al ricorrere di entrambe le seguenti condizioni:

1. l'indeterminatezza dell'importo da trasferire al momento in cui il pagatore ha autorizzato il pagamento (es. contratti di fornitura servizi telef.);
2. l'importo trasferito sia superiore a quello che il pagatore, date le circostanze e il precedente modello di spesa, avrebbe potuto ragionevolmente attendersi: al riguardo, è necessario che vi sia una differenza considerevole…(es. addebiti telefonici per traffico dati non riconosciuto)

ORIENTAMENTO DI GARANZIA PER IL CONSUMATORE

Art. 9 D.lvo 11/10 c.1

“ l’utilizzatore (consumatore) venuto a conoscenza di un’operazione di pagamento non autorizzata o eseguita in modo inesatto, ne ottiene la rettifica se comunica al proprio prestatore questa circostanza entro 13 mesi dalla data di addebito…”

Importante conseguenza

Importanti istituti finanziari hanno interpretato in maniera estensiva tale disposto e su sollecitazione dei legali di consumatori che hanno definito una procedura di acquisto su siti di e-commerce, (che dispongono di sistemi di accredito diretto tramite prestatore di servizi di pagamento del beneficiario) non conclusa con la ricezione della merce, hanno bloccato l'accredito al beneficiario con contestuale rimborso al pagatore !!!

PHISHING

Il decreto legislativo 11 aprile 2011, n. 64, definisce il furto d'identità (Idtheft), ma in sintesi si può dire si realizza il phishing ogni qualvolta un'**informazione individuale**, relativa ad una persona fisica o giuridica è ottenuta in modo fraudolento da un criminale con l'intento di assumerne l'identità per compiere atti illeciti.

A: Banca RASBANK [support-ref25215 id@rasbank.it] Inviato: mercoledi 18/10/2006 7.45

A:

Cc:

Oggetto: Banca RASBANK: INFORMAZIONI [Tue, 17 Oct 2006 22:45:21 -0800]

Gentile Cliente di **Banca RASBANK,**

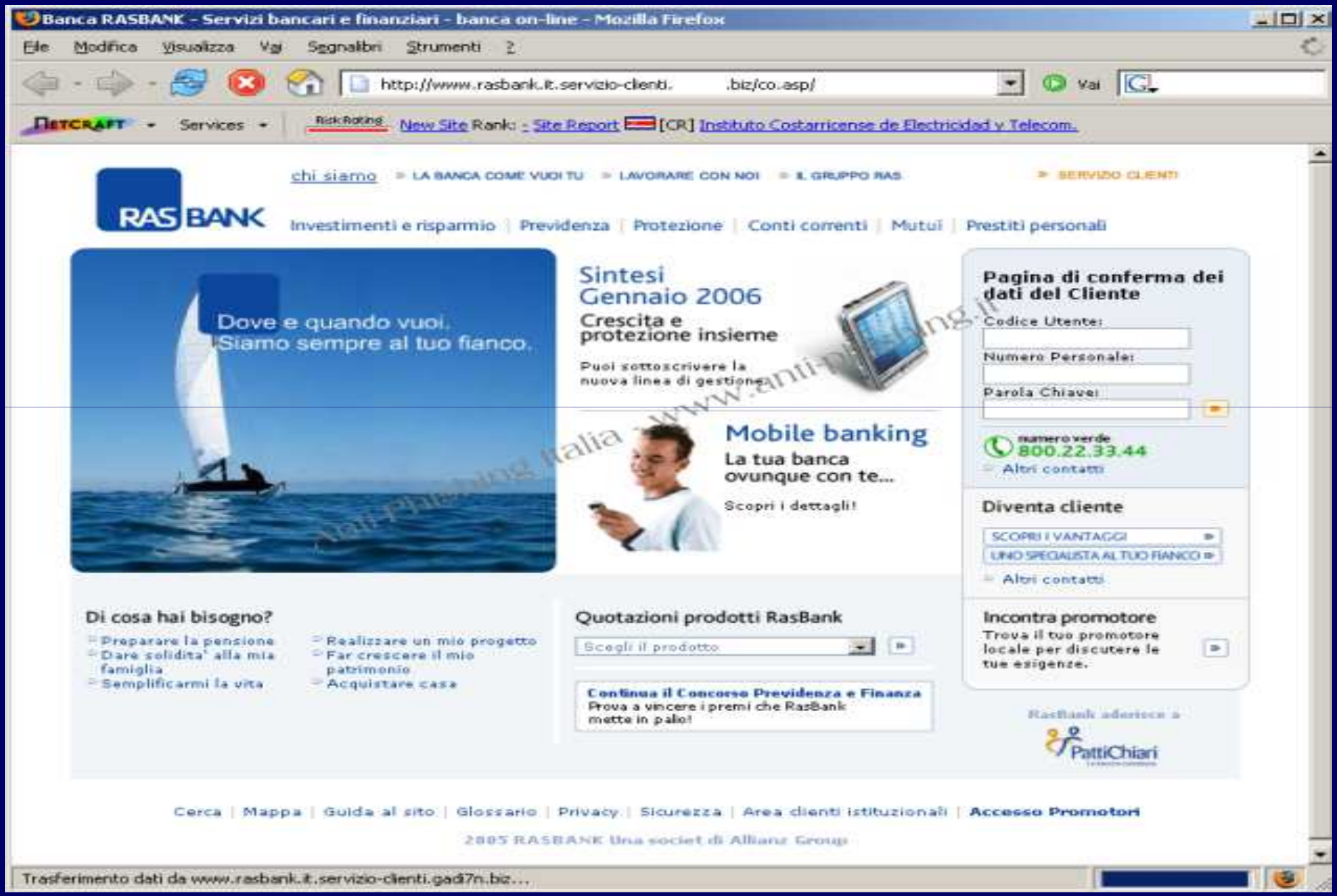
Il Servizio Tecnico di Banca RASBANK sta eseguendo un aggiornamento programmato del software al fine di migliorare la qualità dei servizi bancari.

Le chiediamo di avviare la procedura di conferma dei dati del Cliente.
A questo scopo, La preghiamo di cliccare sul link che Lei troverà alla fine di questo messaggio.

http://www.rasbank.it/servizio-clienti/conferma/co.asp

Ci scusiamo per ogni eventuale disturbo, e La ringraziamo per la collaborazione.

SITO CLONE


Banca RASBANK - Servizi bancari e finanziari - banca on-line - Mozilla Firefox
File Modifica Visualizza Vai Segnalibri Strumenti ?
http://www.rasbank.it.servizio-clienti. .biz/co.asp/
Vai
Netcraft Services
Risk Rating New Site Rank: - Site Report [CR] Instituto Costarricense de Electricidad y Telecom.
chi siamo LA BANCA COME VUOI TU LAVORARE CON NOI IL GRUPPO RAS SERVIZIO CLIENTI
RAS BANK
Investimenti e risparmio | Previdenza | Protezione | Conti correnti | Mutui | Prestiti personali
Dove e quando vuoi.
Siamo sempre al tuo fianco.
Sintesi
Gennaio 2006
Crescita e
protezione insieme
Puoi sottoscrivere la
nuova linea di gestione
Mobile banking
La tua banca
ovunque con te...
Scopri i dettagli!
Pagina di conferma dei dati del Cliente
Codice Utente:
Numero Personale:
Parola Chiave:
numero verde
800.22.33.44
Altri contatti
Diventa cliente
SCOPRI I VANTAGGI
UNO SPECIALISTA AL TUO FIANCO
Altri contatti
Incontra promotore
Trova il tuo promotore locale per discutere le tue esigenze.
Di cosa hai bisogno?
Preparare la pensione
Dare solidita' alla mia famiglia
Semplificarmi la vita
Realizzare un mio progetto
Far crescere il mio patrimonio
Acquistare casa
Quotazioni prodotti RasBank
Scegli il prodotto
Continua il Concorso Previdenza e Finanza
Prova a vincere i premi che RasBank mette in palio!
RasBank adersce a
PattiChiari
Cerca | Mappa | Guida al sito | Glossario | Privacy | Sicurezza | Area clienti istituzionali | Accesso Promotori
2005 RASBANK Una societ di Allianz Group
Trasferimento dati da www.rasbank.it.servizio-clienti.gad7n.biz...

Varie tipologie di ingegneria sociale

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

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

Criminal Identity Theft: utilizzare i dati della vittima per compiere in sua vece atti pubblici illeciti di varia natura, come attivare nuove carte di credito o telefoni cellulari o altri account;

Tecniche di appropriazione delle identità

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

Phishing (versione classica) si compone di tre fasi principali:

1. Spamming (invio massivo di mail) con mittente fake e con all'interno link che reindirizzano a siti cloni di istituti finanziari o enti noti;
2. Utilizzo dei dati carpiti per effettuare operazioni finanziarie;
3. Reclutamento consapevole o in buona fede di persone che possono riciclare il denaro sottratto illecitamente.

Tecniche di appropriazione delle identità

Altro metodo molto diffuso di appropriazione di dati personali consiste nell'attacco di hacking sul pc della vittima attraverso diffusione di vari tipi di malware:

- botvirus;
- Trojan;
- Keylogger.

Conseguenze pratiche e legali del phishing per il consumatore

Dopo essersi accorto del tentativo di trasferimento illecito di denaro dal suo conto corrente o dalla sua carta di credito o ricaricabile, l'utente deve comunicarlo al suo istituto bancario che blocca la posizione del cliente e suggerisce di sporgere una denuncia ;

Conseguenze pratiche e legali del phishing per il consumatore

In sede di denuncia la vittima riferisce della mail sospetta di phishing o del comportamento anomalo del suo p.c. nel caso di hacking;

Nel frattempo la banca verifica che il server su cui sono custoditi i dati riservati del cliente non abbia subito intrusioni;

Conseguenze pratiche e legali del phishing per il consumatore

Nella maggior parte dei casi il consumatore è convinto di essere tutelato e soprattutto garantito dal suo istituto bancario per questo tipo di operazioni fraudolente, ma quando si reca in banca per chiedere il rimborso arriva…la sorpresa!!!

Conseguenze legali del furto d'identità bancario

La banca afferma che la responsabilità della frode è attribuibile ad una negligente condotta di conservazione delle credenziali segrete di gestione del conto e rifiuta il rimborso delle operazioni illecite.

Rimedi legali – la conciliazione bancaria

La L. 262/05 ha introdotto l'istituto della conciliazione bancaria che si svolge attraverso:

- mediazione: si cerca di raggiungere l'accordo delle parti con l'intervento di un esperto indipendente (mediatore); l'accordo può essere omologato dal Tribunale e diventare titolo esecutivo.
- Arbitrato: procedura diretta a chiudere una controversia con l'intervento di un esperto, l'arbitro, cui viene affidato il compito di giudicare; costi limitati e tempi brevi.

Orientamento del conciliatore

In varie decisioni l'arbitro ha espresso il seguente principio:

"*La colpa del ricorrente non esclude la pari colpa concorrente dell'intermediario il quale avrebbe potuto adottare sistemi di protezione più efficaci ed affidabili di quelli messi a disposizione dei clienti, quali ad esempio tokens, digipass, ecc. ben conosciuti nel mercato informatico. Il fatto stesso che si sia potuta verificare una intromissione illecita nei sistemi di protezione adottati a tutela dei conti correnti dei clienti, costituisce la prova della inadeguatezza della tutela offerta e, quindi, della omissione da parte dell'intermediario della particolare diligenza che la legge richiede all'accorto banchiere*"

ITER

E’ POSSIBILE RIVOLGERSI ALL’ARBITRO BANCARIO DOPO AVER ESAURITO INVANO LA PROCEDURA DI RECLAMO ED E’ OBBLIGATORIO ATTIVARE L’ARBITRO PRIMA DI RIVOLGERSI AL GIUDICE ORDINARIO

GRAZIE A TUTTI

BUON LAVORO