Guardia di Finanza
Nucleo Speciale Frodi Telematiche

IL FUTURO DEL MICROMARKETING

IL FURTO D'IDENTITA'

Parma
23 Ottobre '09

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department

Il futuro del Micromarketing

Customer Data Collection

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing

L'azienda, che fa uso di qualsiasi tipo di informazione relativa al customer details, deve intendere la privacy come:

trasparenza

Il futuro del Micromarketing

L'azienda, che fa uso di qualsiasi tipo di informazione relativa al customer details, deve intendere la privacy come:

~~trasparenza~~

corretto trattamento dei dati

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

dato personale

- **Qualunque informazione relativa ad un soggetto, identificato o identificabile, anche indirettamente, mediante il riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Raccolta dei Dati Personali

Per la GDO la raccolta dei dati personali e/o sensibili può avvenire attraverso :

- **La sede dell'esercizio pubblico;**

Il futuro del Micromarketing: La tutela del dato.

Raccolta dei Dati Personali

Per la GDO la raccolta dei dati personali e/o sensibili può avvenire attraverso :

- La sede dell'esercizio pubblico;
- **La rete Internet;**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Raccolta dei Dati Personali

Per la GDO la raccolta dei dati personali e/o sensibili può avvenire attraverso :

- La sede dell'esercizio pubblico;
- La rete Internet;
- **Sistemi di affiliazione della clientela (fidelity/loyalty cards)**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Particolare attenzione andrebbe prestata alla raccolta dati attraverso i canali telematici.

La compilazione di forms su pagine Web dovrà avvenire sempre in modalità protetta. Deve essere presente nella barra di navigazione del web explorer il protocollo "https://....." e nella barra inferiore, normalmente in basso a destra, la presenza del lucchetto

Il futuro del Micromarketing: La tutela del dato.

Adeguata informativa pertinente a:

- **Scopo del trattamento dei dati**

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Adeguata informativa pertinente a:

- Scopo del trattamento dei dati
- **Customer profiling**

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Adeguata informativa pertinente a:

- Scopo del trattamento dei dati
- Customer profiling
- **Marketing**

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Ridurre al minimo le informazioni richieste.
Non sono pertinenti, per la profilazione della clientela, i dati:

- **anagrafici del nucleo familiare, soprattutto se riguardanti minori;**

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Ridurre al minimo le informazioni richieste.
Non sono pertinenti, per la profilazione della clientela, i dati:

- **inerenti la salute;**

dato sensibile

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Ridurre al minimo le informazioni richieste.
Non sono pertinenti, per la profilazione della clientela, i dati:

- **relativi all'orientamento sessuale;**

dato sensibile

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Ridurre al minimo le informazioni richieste.
Non sono pertinenti, per la profilazione della clientela, i dati:

- **concernenti l'orientamento religioso**

dato sensibile

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Informare della presenza di VCC e del motivo del loro utilizzo

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Nel caso si dovessero utilizzare tecnologie e/o dispositivi in grado di "monitorare" i **prodotti**

Nessun problema

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Nel caso si dovessero utilizzare tecnologie e/o dispositivi in grado di "monitorare" la **clientela**

Informazione trasparente ed adeguata

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Nel caso si dovessero utilizzare tecnologie e/o dispositivi in grado di "monitorare" la **clientela**

Consenso dell'interessato

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Nel caso si dovessero utilizzare tecnologie e/o dispositivi in grado di "monitorare" la **clientela**

Possibilità di disattivazione/rimozione dei tag RFID

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

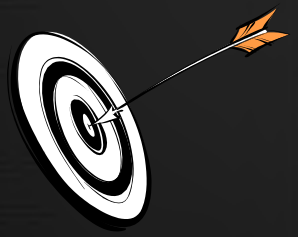
In presenza di e-commerce, comunicazioni via Web, ecc.

✓ **Evitare di utilizzare dati acquisiti all'insaputa dei clienti**
(cookies, parametri su motori di ricerca sia su web che sul sito di commercio elettronico; dati ottenuti da social network, ecc...)

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare



In presenza di e-commerce, comunicazioni via Web, ecc.

✓ **Inviare e-mail con target precisi**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

In presenza di e-commerce, comunicazioni via Web, ecc.

✓ **Cancellare immediatamente i dati dai propri archivi in caso di richiesta da parte dell'interessato**

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

In presenza di e-commerce, comunicazioni via Web, ecc.

✓ **Pubblicare in un'apposita sezione del proprio sito/portale web relativa alla tematica della privacy**

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Nell'utilizzare sistemi di archiviazione digitale dei dati acquisiti, bisognerà:

- ✓ **Adottare le giuste misure di sicurezza dei dati**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: La tutela del dato.

Cosa fare

Nell'utilizzare sistemi di archiviazione digitale dei dati acquisiti, bisognerà:

- ✓ **Detenere le informazioni minime indispensabili**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Fidelity Cards.

Opportunità

Le fidelity cards ed in particolare quelle del tipo contacless, permettono:

- **L'accredito dei punti in base agli acquisti effettuati;**

Il futuro del Micromarketing: Fidelity Cards.

Opportunità

Le fidelity cards ed in particolare quelle del tipo contacless, permettono:

- **L'uso di un borsellino elettronico previa ricarica di importi prepagati;**

Il futuro del Micromarketing: Fidelity Cards.

Opportunità

Le fidelity cards ed in particolare quelle del tipo contacless, permettono:

- **Di creare circuiti di fidelizzazione con negozi convenzionati**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Fidelity Cards.

Misure da adottare

Tecnologia di ultima generazione

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Fidelity Cards.

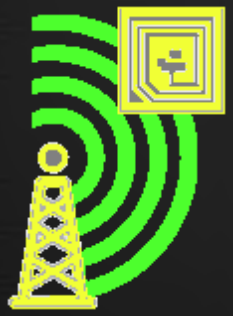
Misure da adottare

Sistemi di encrypting dei dati

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Fidelity Cards.

Misure da adottare

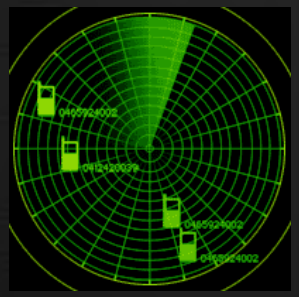


- **Autenticazione costante tra i tag Rfid attivi e/o passivi**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Fidelity Cards.

Misure da adottare

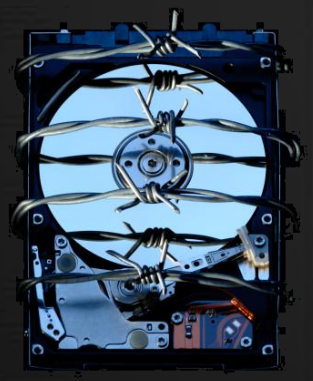


Nel rilasciare la fidelity/loyalty card contacless bisognerà mettere a conoscenza il cliente della possibilità di tracking degli acquisti effettuati

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Fidelity Cards.

Misure da adottare



Nell'utilizzare sistemi di archiviazione digitale dei dati acquisiti, bisognerà:

- **Qualora si detengano dati sensibili adottare misure d sicurezza ancor più accurate per evitare furti d'identità (*dati biometrici, dati di minori, dati sanitari, dati processuali, ecc..*)**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il Furto d'Identità
Conoscerlo per difendersi

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Social Engineering

ATTIVITÀ PRELIMINARE ADOTTATA DAI TRUFFATORI PER CONOSCERE IL SISTEMA PRESO DI MIRA, QUALI PROTEZIONI SONO ADOTTATE ECC…

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Social Engineering

Keylogging

I keylogger possono essere di tipo software e hardware.

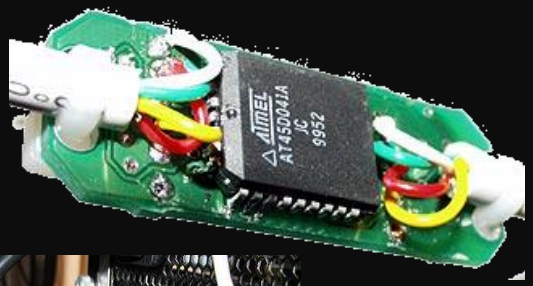
Non registrano solo le battute da tastiera, ma eseguono anche istantanee dello schermo, catturano informazioni riguardo l'uso di Internet ecc. La maggior parte di essi inviano per posta elettronica i loro rapporti.

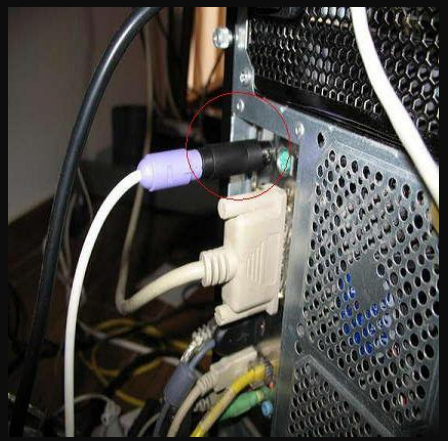
Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

Social Engineering

Keylogging





Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

Social Engineering

Keylogging

Spyware

Permettono di tracciare tutte le operazioni dell'utente effettuate, normalmente, durante la navigazione Internet. Questo tipo si malware dovrebbero avere come unica finalità quella di ottenere le informazioni necessarie per inviare messaggi e/o pop-up commerciali di potenziale interesse al cyber utente

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

Social Engineering

Keylogging

Spyware

Trojan

Permettono l'installazione di altri programmi, scoprire quali porte del computer non sono monitorate dal firewall/antivirus (backdoors), l'installazione di keylogger di tipo software, ecc...

Da questi il cracker ottiene via internet rapporti contenenti:

- siti web visitati
- print screen
- tasti digitati
- click del mouse

Normalmente i file autoinstallanti hanno un'estensione "**.pif**", "**.exe**", "**.bat**"

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Social Engineering

Keylogging

Spyware

Trojan

Screen Grabbing

Tecnica mediante la quale si è in grado di salvare intere pagine web, non solo semplici link.

Si riescono a conservare anche i "**DEAD LINK**", pagine che per qualche motivo non sono più online mantenendo tutto il loro contenuto.

In pratica si genera un clone, una sorta di fotografia esatta e corrispondente a quella vera.

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- **Phishing**

Attuato generalmente tramite posta elettronica. Il phisher invia e-mail che sembrano provenire da siti web autentici richiedendo, all'ingenuo utente, l'inserimento di informazioni personali come le credenziali di accesso all'istituto di credito on-line. (l'invio della posta elettronica si basa sullo Spamming)

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

Social Engineering

Keylogging

Spyware

Trojan

Screen Grabbing

Phishing

Port & Network Scanning

Fase 1: Identificazione dei bersagli

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- Phishing
- **Port & Network Scanning**

Fase 1: Identificazione dei bersagli

Fase 2: Network Scanning sapere quali Host di una determinata Rete sono attivi

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- Phishing
- **Port & Network Scanning**

Fase 1: Identificazione dei bersagli

Fase 2: Network Scanning sapere quali Host di una determinata Rete sono attivi

Fase 3: **Port Scanning** processo di connessione alle porte TCP e UDP del sistema da attaccare. Si riesce a sapere :

- Servizi in esecuzione e/o in stato di LISTENING;

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- Phishing
- **Port & Network Scanning**

Fase 1: Identificazione dei bersagli

Fase 2: Network Scanning sapere quali Host di una determinata Rete sono attivi

Fase 3: **Port Scanning** processo di connessione alle porte TCP e UDP del sistema da attaccare. Si riesce a sapere :

- Servizi in esecuzione e/o in stato di LISTENING;
- **Sistema Operativo;**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- Phishing
- **Port & Network Scanning**

Fase 1: Identificazione dei bersagli

Fase 2: Network Scanning sapere quali Host di una determinata Rete sono attivi

Fase 3: **Port Scanning** processo di connessione alle porte TCP e UDP del sistema da attaccare. Si riesce a sapere :

- Servizi in esecuzione e/o in stato di LISTENING;
- Sistema Operativo;
- **Quali programmi utilizzano determinate porte**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- Phishing
- **Port & Network Scanning**

Fase 1: Identificazione dei bersagli

Fase 2: Network Scanning sapere quali Host di una determinata Rete sono attivi

Fase 3: **Port Scanning** processo di connessione alle porte TCP e UDP del sistema da attaccare. Si riesce a sapere :

- Servizi in esecuzione e/o in stato di LISTENING;
- Sistema Operativo;
- Quali programmi utilizzano determinate porte
- **Quali porte sono monitorate dall'antivirus e/o Firewall**

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- Phishing
- Port & Network Scanning
- **Sniffing**

Attività di monitoraggio ed intercettazione dei pacchetti di dati che transitano in una Rete telematica (Internet/Intranet).

Viene utilizzata per il monitoraggio della rete da parte dei sistemisti (attività lecita), ma anche per acquisire account, password e qualsiasi altro dato sensibile (attività illecita).

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Le Tecniche Online

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- Phishing
- Port & Network Scanning
- Sniffing
- **Spoofing**

- EMAIL MIME SPOOFING
- SMS E PHONE SPOOFING
- WEB E IP SPOOFING.

CONSISTE NEL FAR CREDERE DI RICEVERE IL MESSAGGIO, LA TELEFONATA O IL PACCHETTO DATI DA UN'ALTRO UTENTE

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- Phishing
- Port & Network Scanning
- Sniffing
- Spoofing
- **Pharming**

Truffa che può essere portata a termine in due modalità:

- **DNS cache poisoning**
- **Modifica locale del registro DNS**

  modifica del file "hosts" nella directory del PC "C:\windows\system32\drivers\etc".

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

- Social Engineering
- Keylogging
- Spyware
- Trojan
- Screen Grabbing
- Phishing
- Port & Network Scanning
- Sniffing
- Spoofing
- Pharming
- **Vishing**

Evoluzione del phishing. I contatti preliminari possono avvenire a mezzo email, chat o sms. Non si chiede di "cliccare" su un link ma di chiamare un numero telefonico (quasi sempre del tipo a tariffazione aggiunta: es. 899xxxx). Un disco o un finto operatore del call center dell'istituto di credito, circuito della carta di credito, ecc., chiederà di fornire i dati di accesso al conto corrente bancario, dati della carta di pagamento o qualsiasi altro dato a noi riferibile.

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Social Engineering
Keylogging
Spyware
Trojan
Screen Grabbing
Phishing
Port & Network Scanning
Sniffing
Spoofing
Pharming
Vishing
Spamming

Inizialmente nato come nuova forma pubblicitaria, viene anche sfruttato per indurre a cliccare su link o scaricare file (es. foto, documenti ecc.) che, all'insaputa dell'utente, installano automaticamente nel PC collegato software fraudolenti.

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Mezzi di pagamento elettronico

CARD PRESENT

I DATI SI OTTENGONO SOLO CON LA PRESENZA FISICA DELLO STRUMENTO DI PAGAMENTO ELETTRONICO

CARD NOT PRESENT

IL TRUFFATORE RIESCE AD OTTENERE I DATI DELLA CARTA DI PAGAMENTO SENZA ESSERE VENUTO IN POSSESSO DELLA STESSA

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Card Present

Skimming

CON STRUMENTI DI PICCOLE DIMENSIONI, TANTO DA POTER ESSERE NASCOSTI NEL PALMO DI UNA MANO, DALLA "STRISCIATA" È POSSIBILE OTTENERE I DATI IMMAGAZZINATI NELLA BANDA MAGNETICA DELLA CARTA.

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Card Present

Skimming

ATM Skimming

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

- Skimming
- ATM Skimming
- **RFID Skimming**

Tecnica per acquisire ogni sorta di dati presenti su contactless cards

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

- Skimming
- ATM Skimming
- RFID Skimming
- **POS Fraud**

I terminali POS possono essere manomessi anche all'insaputa degli esercenti pubblici. Spesso vengono simulati furti con l'intento principale di apportare modifiche nei POS per riuscire a carpire i dati di carte di credito e debito

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

- Skimming
- ATM Skimming
- RFID Skimming
- POS Fraud
- **Embossing**

TUTTE LE INFORMAZIONI OTTENUTE A SEGUITO DEL COMPIMENTO DI QUESTE FRODI, SONO SUFFICIENTI PER CLONARE UNA CARTA DI CREDITO O UN BANCOMAT

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

- Skimming
- ATM Skimming
- RFID Skimming
- POS Fraud
- Embossing
- **Dumpster Diving**

QUESTA È UNA TECNICA POCO INFORMATICA, MA CHE PERMETTE DI OTTENERE INFORMAZIONI DI CARATTERE PERSONALE COME I PROPRI DATI ANAGRAFICI, IL NUMERO DI CONTO CORRENTE, IL NUMERO DI CARTA DI CREDITO ETC. FRUGANDO NELLA SPAZZATURA O RUBANDO LA POSTA

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Il futuro del Micromarketing: Identity Theft.

Social Network

POTENZIALI VITTIME POSSONO ESSERE INDIVIDUATE DAI SOCIAL NETWORK.

Ispettore Superiore dott. Antonio D'Onofrio
Responsabile Cybercrime Department – Nucleo Speciale Frodi Telematiche della Guardia di Finanza

Grazie per l'attenzione

GUARDIA DI FINANZA

GAT – NUCLEO SPECIALE FRODI TELEMATICHE

VIA MARCELLO BOGLIONE, 84 – 00155 – ROMA - TEL.+39.06.22938903

Cybercrime Department

Mar. Aiut. dott. Antonio D'Onofrio

+39.06.22938906/11 – antonio.donofrio@gat.gdf.it

sos@gat.gdf.it