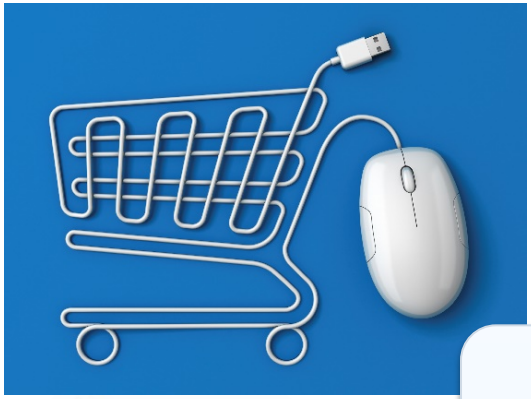
Evolving fraud landscape

Nuove strategie contro vecchie minacce

Veronica Borgogna
Consorzio BANCOMAT®

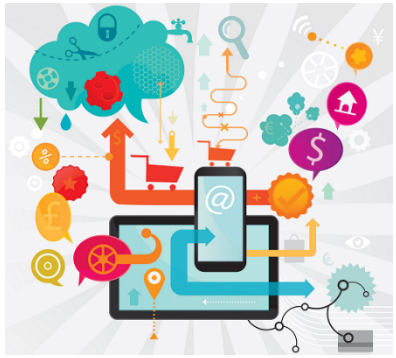
Oggi è già domani



Il mondo dei pagamenti elettronici sta attraversando un periodo di **forti cambiamenti**.

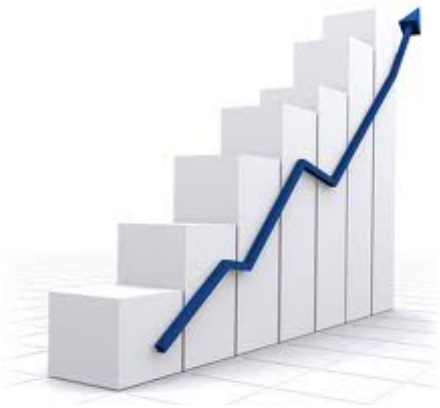
La diffusione delle nuove tecnologie favorisce l'adozione di molteplici forme di pagamento che sfruttano canali del tutto innovativi.

Tutto ciò crea vantaggi non solo per il **consumatore**, che incontra sempre meno limiti spaziali e temporali ai suoi acquisti, ma anche per il **business**, con particolare riferimento all'allargamento al segmento **small retailer**.



Diversificazione e contaminazione

Pagamenti di prossimità	Pagamenti remoti
▪ Pagamenti con carta fisica (sia a contatto che contactless) ▪ Mobile Secure Element ▪ Mobile Cloud Based/ HCE	▪ Pagamenti CNP ▪ Bonifici ▪ Wallet elettronici



TREND

Incremento dei pagamenti mobile

Incremento dei remote payment

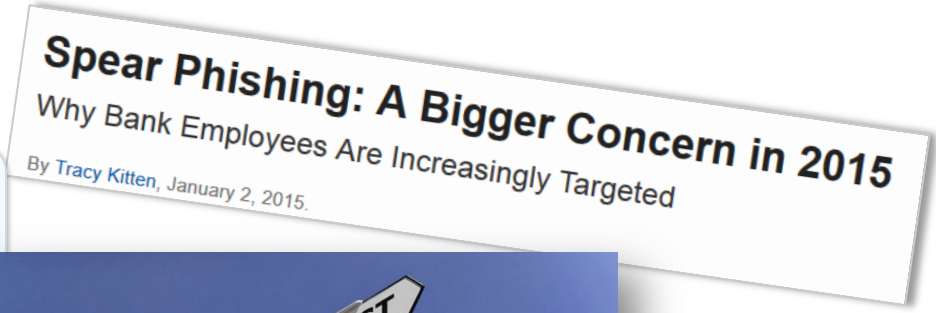
Continua crescita dei pagamenti con carta, sulla spinta anche degli strumenti contactless

Parallelamente alla crescita delle transazioni, si assiste a una **diversificazione** delle frodi e a una progressiva **contaminazione** dei fenomeni tra mondo fisico e mondo virtuale.

Vulnerabilità note per nuovi canali di pagamento

I fenomeni fraudolenti, seppur nuovi, sfruttano vulnerabilità «note»:

- **Comportamento dell'utente**: spesso non conosce le minacce legate alle tecnologie che utilizza e può adottare comportamenti non sicuri;
- **Investimenti in sicurezza**: i piccoli e-retailer (e non solo…!) talvolta dispongono di risorse insufficienti per dotarsi di difese adeguatamente robuste;
- **Inefficace segregazione dei dati**: i dati relativi alle transazioni custoditi dai soggetti coinvolti nei processi di erogazione dei servizi potrebbero non essere adeguatamente protetti.



DUPLICE TENDENZA

Informatizzazione/ sofisticazione delle tecniche e contemporanea persistenza di fenomeni «**collaudati**» che, tuttavia, continuano a garantire il successo della frode.

L'informatizzazione delle strategie di attacco

In questo complesso scenario, l'obiettivo dei frodatori non è più soltanto la frode finanziaria ma, più in generale, l'ottenimento di **dati che sono custoditi all'interno delle strutture e dei sistemi** da poter riutilizzare, poi, in modo più ampio (vendita, scambio, ricatto, spionaggio industriale…).

ATTACCHI AI **TERMINALI/ STRUMENTI** DI PAGAMENTO

- **Skimming**
- **Shimming**
- **Eavesdropping**
- **Malwaring (Trojan, Jackpotting)**
- **Remote attack (DoS)**

ATTACCHI AI **DATA BASE**

- **Furto d'identità**
- **Remote attack (DoS)**
- **Pharming/ Phishing**
- **Arp poisoning**
- **Key logging**

- **Firesheep**
- **Malwaring**
- **Data breach**
- **Spear phishing**
- **Remote attack (DoS)**

Attacchi ai terminali ATM/ POS

Skimming/ Malwaring

Skimming

Installazione su POS/ ATM di device in grado di leggere i dati delle carte operanti con tecnologia a banda e di memorizzarli/ inviarli a supporti esterni.

Nonostante sia una tecnica relativamente «vecchia» e conosciuta, è ancora la manomissione di terminali **maggiormente diffusa** in Italia

Alle tradizionali tipologie di *skimming*, si stanno affiancando alcune nuove **varianti** estremamente efficaci.

Jackpotting su ATM

- **Infezione** tramite attacco fisico all'ATM oppure attraverso un accesso alla rete grazie a una postazione esposta e non partizionata.
- Apparecchiatura posta sotto il **controllo** dei frodatori che sono in grado di attivare a comando la funzione di erogazione contante, di solito in orari non sospetti.
- Nessuna carta rubata/ clonata coinvolta.
- Spesso, il malware cancella le proprie tracce e modifica i log per **mascherare** la causa dell'attacco.

Trojan su POS

- **Infezione** con accesso alla rete tramite una postazione esposta e non partizionata.
- Installazione di un **loader** in grado di connettersi con il *command and control server* per «raschiare» la memoria del POS.
- **Ricerca** dei dati relativi alle carte all'interno della memoria usata dagli altri programmi e registrazione di quello che viene digitato sulla tastiera.
- Invio dei dati a un **server esterno** di raccolta.

Attacchi ai data base

Phishing/ Spear phishing

Molti fra i sistemi di pagamento innovativi prevedono l'interazione dell'utente con device collegati alla rete internet.
Spesso, però, nonostante i robusti sistemi di sicurezza implementati a difesa di tali servizi, è il **comportamento** stesso dell'utente che lo espone a rischio di frode.

Uno dei meccanismi più efficaci per catturare dati sensibili direttamente dagli utenti (es. password, codici di accesso, dati delle carte o dati personali) è rappresentato ancora dal **phishing**: secondo una recente ricerca di settore*, circa il 97% della popolazione mondiale non sarebbe in grado di riconoscere i tentativi di attacco.

L'ultima preoccupante tendenza riguarda lo **spear phishing** che non innesca attacchi su vasta scala ma si focalizza su un gruppo specifico di utenti – i dipendenti di una banca, ad esempio – al fine di avere accesso a proprietà intellettuali, sistemi aziendali, dati finanziari, segreti commerciali o altri dati riservati.
L'attacco si realizza tramite mail inviate a nome di strutture interne all'organizzazione o da partner con i quali i soggetti comunicano regolarmente o in generale da fonti apparente-mente affidabili.

** Fonte: Intel security*

Resilienza e sopravvivenza

La tecnologia evolve continuamente, i sistemi di pagamento si ampliano e si differenziano, i fenomeni fraudolenti si moltiplicano.

In che modo possiamo reagire al cambiamento? Implementando nuove strategie? Adattando a nuove minacce meccanismi di difesa che già utilizziamo?

E' possibile ricorrere a strumenti tecnologici a supporto di processi anche non propriamente tecnologici?

Se la nostra vulnerabilità è ancora troppo spesso il comportamento dell'utilizzatore, quanto ci aiuta la tecnologia? È sufficiente da sola?

...Diverse opinioni per orientarsi...