Ecco come salvarsi dalle truffe con Bancomat e carte di credito anche sul web

Bancomat, carte di credito o contanti. Nessuno strumento di pagamento né nel mondo web né in quello reale è al sicuro da truffe e furti . Avvalendosi però di piccole accortezze ed ai sistemi di sicurezza, il numero delle truffe nell'uso della moneta elettronica sono diminuite. Infatti in Italia nel 2014 sono stati accertati e denunciati 21mila casi di utilizzi fraudolenti di Bancomat (Atm), Pos elettronici e moneta elettronica utilizzata per fare acquisti e pagamenti in Internet, per un totale di 1,8 milioni di euro (dati Abi). Nel 2013 erano 23mila per un ammontare di oltre 2,6 milioni.

Secondo **Stefano Torri**, European Sales Director di ***March Networks***, società specializzata in sistemi di videosorveglianza Ip, strumento molto utile per aumentare il livello di sicurezza e recupero dati *"la diminuzione è dovuta, oltre che a una maggiore informazione dei consumatori, soprattutto a un incremento dei sistemi di protezione attuata sui vari fronti, sia in Rete, che presso Atm ed esercizi commerciali, come la videosorveglianza, gli Atm collocati all'interno delle filiali, i Pos di nuova generazione che possono essere manomessi molto difficilmente. Per esempio osservando con le videocamere il tempo di permanenza nell'area self delle banche o il numero di operazioni svolte dal cliente si può intervenire bloccando il sospettato se si osservano delle anomalie nel comportamento*".

Gli sportelli Atm-Bancomat delle banche infatti non vengono più utilizzati solo per prelevare soldi con il bancomat, ma anche per depositare assegni e contanti, per effettuare i pagamenti di bollette, assicurazioni. Così come gli Atm di pagamento sempre più diffusi sono quelli presso i distributori e i parcheggi. Alla fine del 2014 si contavanoIn Italia oltre 40.500 mila Atm, utilizzati sempre meno per i prelievi (-28%) e sempre più per altre operazioni di pagamento (+26%).

Ecco **le trappole** maggiormente utilizzate dai malviventi:

- Lo **skimmer** in pratica una **finta fessura** apposta su quella reale, utilizzata per leggere la banda magnetica del vostro bancomat e copiarne i dati.
- Il **card trapping**: i truffatori fanno in modo che la tessera rimanga incastrata nella fessura e aspettano che il cliente chieda aiuto o entri in filiale per agire e prelevare i soldi.
- Il **cash trapping**: una volta terminata l'operazione i soldi non

escono e restano intrappolati nel meccanismo (trapper), che una volta smontato ridà al truffatore tutti i soldi prelevati nel tempo d'installazione del trapper.

- Il **Lebanese loop**: sullo sportello viene applicato un dispositivo che trattiene la carta. Il truffatore interviene prestando soccorso al cliente davanti allo sportello, lo invita a digitare nuovamente il Pin, che viene memorizzato dal ladro. Dopo l'allontanamento della vittima, il criminale può recuperare la carta e utilizzarla con il pin.
- Il **Trashing**: i truffatori utilizzano gli scontrini delle carte di credito che talvolta gli utenti gettano via dopo un acquisto in modo poco attento.

"*Le banche oggi hanno adottato dei sistemi di sicurezza per prevenire le truffe*" spiega **Paolo Romanò**, responsabile commerciale Italia ***March Networks*** "*come l'installazione di Atm nelle aree self delle banche che non consentono la sovrapposizione di false tastiere o fessure. Oppure utilizzano carte di credito con i chip, più difficili da clonare rispetto a quelle con la banda magnetica. Il problema è che queste carte non sono ancora così diffuse negli Stati Uniti e in America Latina. Purtroppo ora che le banche sono più sicure, i truffatori si stanno concentrando sui punti più deboli come i* ***distributori di benzina*** *e i* ***totem per il pagamento dei parcheggi,*** *meno protetti*".

Ecco alcuni consigli utili per **prevenire le truffe** all'Atm-Bancomat e cosa bisogna fare se si è caduti nella trappola:

1. **controllare che la tastiera sia ben fissata**.
2. che la **fessura dove si inserisce la carta sia anch'essa ben fissa**.
3. se la carta rimane incastrata **denunciare l'accaduto alla banca senza abbandonare lo sportello Atm** ma telefonando in filiale o al numero verde per bloccarla se l'agenzia è chiusa.
4. se possibile **utilizzare Atm nell'area Self all'interno della banca**.
5. se lo sportello è su strada **diffidare della gente che tende ad avvicinarsi troppo** e nel caso sospendere l'operazione.
6. **rifiutare l'aiuto di terzi**.
7. **digitare il pin sempre coprendo la digitazione con l'altra mano**.
8. **attivare il servizio sms** per ricevere messaggi informativi per ogni operazione svolta con la carta.
9. **denunciare la truffa alle forze dell'ordine**.
10. **non gettare mai la ricevuta**. Da quel foglietto i malviventi **possono recuperare i dati** della vostra carta elettronica.

AMO MAI SMESSO DI DARE RISPOSTE AI TUO

Anche i **Pos** utilizzati negli esercizi commerciali possono essere compromessi, mediante apertura e inserimento da parte dei malviventi di un microprocessore che registra i codici della carta di credito o il pin. Il microprocessore viene poi rimosso e usato dal criminale per realizzare delle carte di credito "clonate" proprio grazie ai dati acquisiti ed immagazzinati. In questo caso, mancando i controlli ad hoc implementati dalle banche, è necessario adottare alcuni accorgimenti.

1. Tenersi sempre aggiornati sui limiti di prelevamento e pagamento della carta, e **controllare frequentemente l'estratto conto** e la **lista dei movimenti**.
2. Quando si utilizza la carta di credito in un esercizio commerciale **è consigliabile consegnarla direttamente alla cassa** e **tenerla sempre sott'occhio**.
3. **Non cedere mai la carta di credito e il pin ad altre persone**.
4. Diffidare di chi **non ha il Pos a vista** o effettua più "*strisciate*".
5. **Prima di firmare una ricevuta d'acquisto controllare che l'importo indicato sia corretto**.
6. **Non gettate mai le ricevute**.

E' su Internet che avvengono ancora la maggior parte delle truffe (circa 15mila nel 2014). In questo caso i criminali riescono a circuire le vittime con **mail fasulle in cui si chiedono le coordinate bancarie** oppure riescono a carpirle infilandosi nel sistema o **intercettando le transazioni**. "*Oggi molte banche o società che emettono le carte di credito adottano doppi livelli di sicurezza, come il securcode o il token fisico, ossia un codice da utilizzare per una sola transazione che viene inviato sul numero di cellulare*" spiega **Torri**. "*Il consiglio è sempre di fare acquisti su siti e che usano dati criptati: nella url appare '**https**' e non '**http**'. Negli http infatti i dati sensibili sono "in chiaro", quindi accessibili anche ai malintenzionati*".

Sniffing e phishing sono alcune delle tecniche più comuni utilizzate per carpire i dati delle carte di credito in Rete:

Sniffing: i criminali informatici intercettano le coordinate di pagamenti fatti con carte di credito, utilizzando poi le stesse tracce per fare nuovi acquisti all'insaputa del vero proprietario.
Phishing: all'indirizzo di posta elettronica di un qualsiasi utente potrebbe arrivare una mail che, attraverso qualche stratagemma (per esempio simulando nella formula e nel layout grafico una comunicazione ufficiale della banca), porti ad inserire i dati personali e quelli relativi alla carta di credito.
Trojan banking: diffusione di virus informatici, non sempre rilevati

dai software antivirus, che carpiscono le credenziali di accesso ai servizi bancari online. Sfruttano i "buchi" del sistema di protezione, si autoinstallano, si autoriproducono e diffondono fino a minare il corretto funzionamento del sistema, inclusa la fuoriuscita incontrollata dei dati personali.

Negli attacchi di phishing, un utente potrebbe ricevere un'email che sembra inviata da ***Facebook***, con tutte le immagini e la grafica tipica di **Facebook**; l'unica differenza è che in questa email si chiede all'utente di resettare la propria password attraverso un link. L'utente ignaro clicca sul comando e viene redirezionato **ad una pagina web falsa che assomiglia a quella di Facebook**. A questo punto inserisce le prorie credenziali (username e password) e il gioco è fatto: è così che funzionano gli attacchi di Phishing.

Il phishing funziona perché conta sulla fiducia delle persone. **Facebook** ne è un gran esempio. Questo diffisussimo social network è diventato, in questi ultimi anni, uno strumento molto popolare per i phisher. I truffatori sfruttano, da un lato, la grande popolarità di ***Facebook*** e, dall'altro, la paura delle persone di perdere i propri dati personali. **Ironicamente per rubare i dati degli utenti vengono inviate loro richieste fasulle di resettaggio della password che imitano in tutto e per tutto quelle autentiche di Facebook, ma non lo sono**.

Non rispondete mai a una richiesta di informazioni personali che proviene da un'email

Naturalmente, gli attacchi di phishing che si presentano sotto forma di email di ***Facebook*** non rappresentano l'unica forma di phishing. Gli hacker inviano messaggi simili che imitano il formato delle email delle principali banche e carte di credito. L'obiettivo in questo caso è ottenere l'accesso al conto in banca della vittima. Indipendentemente dal servizio web di cui si parla, l'obiettivo degli attacchi di phishing è sempre lo stesso: sfruttare la fiducia che gli utenti ripongono in determinati servizi ed istituzioni per ottenere username, email, password o codici PIN.

I consigli per proteggere i propri acquisti online:

Se si riceve un'email simile a una comunicazione ufficiale della banca personale che suggerisce di inserire i dati personali e quelli relativi alla carta, non rispondere e **avvertire subito la banca** e **le forze dell'ordine,** stando attenti a **non eliminare la mail** ricevuta.
Verificare sempre che sul sito sia riportato un indirizzo fisico e telefonico attraverso cui sia possibile contattare l'azienda.

Assicurarsi sempre che i siti utilizzino protocolli di sicurezza per la protezione dei dati e che la pagina in cui vengano inseriti i dati sia criptata con la dicitura "***https***" in corrispondenza dell'indirizzo web della pagina.
Utilizzare sempre, se possibile, **carte prepagate non direttamente collegabili al conto corrente**.
Stampare e conservare con cura le ricevute di pagamento.

Ma cosa fare se nonostante tutte le attenzioni si rimane comunque vittime di criminali informatici ? Risponde l'emettitore della carta spiega **Romanò**. Quindi appena ci si accorge che sono stati effettuati acquisti di cui si è ignari, **va chiamato l'istituto o la società che ha emesso la carta**, **bloccare la carta** e spiegare l'accaduto. Contattare anche l'azienda che ha ricevuto il pagamento e cercare di farsi restituire il denaro. Altrimenti si apre la pratica di rimborso con la banca. In ogni caso **è bene denunciare l'accaduto alle forze dell'ordine**. "*Occorre dimostrare, con ricevute alla mano, che non c'è stato l'uso fraudolento della carta e si verrà rimborsati in toto*" spiega **Romanò**. "*Se invece l'utente ha usato impropriamente la carta, ma senza dolo o colpa grave, potrebbe pagare una franchigia di 150 euro, come previsto dal decreto legislativo 11/2010*".