Vademecum della Sicurezza

Il pagamento con carta è sempre più diffuso ed utilizzato in quanto flessibile, comodo e sicuro. Tale tipologia di pagamento sta diventando una valida alternativa al contante anche per i pagamenti di basso importo.
La sicurezza dei pagamenti con carte è costantemente migliorata attraverso lo sviluppo di nuove tecnologie e nuovi standard tecnici che sempre più frequentemente confluiscono nelle nuove normative emesse a livello europeo e nazionale.
Ma l'evoluzione tecnologica consente anche lo sviluppo di nuove frodi sempre più sofisticate e i truffatori trovano sempre nuove strade per impossessarsi delle carte o dei dati della stessa.
Per tale ragione, la tecnologia non è sufficiente per evitare le frodi associate alle carte se non è accompagnata da "comportamenti" adeguati che il titolare della carta deve assumere in base al contesto in cui si trova ad utilizzare la carta.
L'obiettivo del presente vademecum della Sicurezza è di indicare una serie di regole semplici da applicare sia quando si usa la carta "fisicamente" che quando si effettuano pagamenti "on line" in internet.

La Custodia della Carta di Credito

Arrivo della nuova carta

La carta di credito viene inviata per posta al cliente in stato non attiva. Quando si riceve il plico, verificare sempre che sia integro e che non sia stato manomesso. In caso contrario, informare l'Ufficio Clienti di Sella Personal Credit.
La carta di credito va immediatamente firmata sul retro con una penna a sfera.

Arrivo del PIN

Il PIN rappresenta il codice segreto necessario per il prelievo presso gli sportelli Bancomat in Italia e all'estero. Il codice viene recapitato a casa entro 15 giorni dalla data di attivazione. Anche in questo caso, verificare che il plico sia integro e che non sia stato manomesso. In caso contrario, informare l'Ufficio Clienti di Sella Personal Credit.

Custodia della carta

La carta di credito va custodita alla stessa stregua di un'importante somma di denaro. Va quindi conservata in un posto sicuro sotto il proprio controllo e non va lasciata in borse, valige, bagagli non custoditi.
Non cedere mai la carta a terzi.

Custodia del PIN

Il PIN è un codice segreto e quindi non deve essere mai rivelato ad altre persone. Si deve cercare di memorizzare il PIN e non bisogna mai conservarlo insieme alla carta. Ad esempio, se si memorizza il PIN sul proprio Cellulare, evitare di tenere il Cellulare nella borsa insieme alla carta, memorizzare il PIN in rubrica sotto un nome fittizio facile da ricordare, aggiungere delle cifre davanti per simulare un numero di telefono e tenere sempre il cellulare bloccato con il codice di blocco. Conservare il plico con il quale è stato ricevuto il PIN in un posto sicuro dentro casa in modo da poterlo utilizzare in caso di emergenza.

Utilizzo della Carta di Credito

Pagamenti presso un POS

Il pagamento presso il POS di un esercente deve essere sempre effettuato con la presenza del titolare per evitare che la carta sia clonata o siano effettuati più addebiti di quelli richiesti. Prima di confermare la transazione (ad esempio apponendo la firma sullo scontrino), verificare che l'importo sia corretto. Analogamente, verificare sempre che l'importo indicato come totale sulla ricevuta d'acquisto sia quello corretto. Se il totale non è compilato (in alcune ricevute il titolare può indicare una mancia), compilare sempre il totale, con o senza mancia, prima di firmare. Ritirare sempre le ricevute della carta e conservarle fino all'arrivo dell'estratto conto.

Operazioni presso gli ATM

Quando si effettuano delle operazioni agli sportelli Bancomat oppure, in generale, presso tutti i terminali per i pagamenti automatici (es. distributori di benzina, distributori automatici di biglietti, etc), bisogna tutelare riservatezza dell'operazione che si vuole eseguire seguendo dei semplici consigli:

- evitare di farsi distrarre o aiutare da altre persone. Se il bancomat è troppo affollato, evitare e sceglierne un altro.
- Se mentre si esegue l'operazione si avvicina qualcuno, invitarlo ad allontanarsi.
- Coprire con la mano libera la tastiera quando si digita il PIN, il truffatore potrebbe aver messo una telecamera per carpire il PIN.
- Non dimenticarsi mai di ritirare la ricevuta e la carta.

Se per un qualsiasi motivo, durante un operazione presso un terminale di pagamento la carta viene trattenuta dal terminale, bloccarla immediatamente e procedere alla sua sostituzione.

Evitare i terminali di pagamento alterati perché c'è un forte rischio che siano stati manomessi per clonare le carte.
Per riconoscere se un bancomat è stato manomesso, seguire questi semplici consigli:

- verificare che la fessura dove si inserisce la carta sia stabile e non si muova. Analogamente verificare se la carta entra con difficoltà oppure si fa fatica ad estrarla. In entrambi i casi la fessura potrebbe esser stata ricoperta con un lettore che legge i dati della carta.
- verificare che la tastiera del bancomat sia stabile e non si muova perché in tal caso potrebbe essere stata ricoperta con un'altra tastiera per catturare il PIN.

In tutti questi casi, e in genere quando si notano delle modifiche al bancomat, evitare di utilizzare il terminale e sceglierne un altro. Se si ha il forte sospetto che il bancomat sia stato manipolato, avvisare le forze dell'ordine.

Altre tipologie di pagamento con carta

È buona norma non comunicare mai i dati della propria carta di credito (numero, scadenza, CVV) a degli sconosciuti, a meno che non si stia effettuando un ordine telefonico o una prenotazione. Tali tipologie di pagamenti presentano alti rischi e quindi bisogna essere sempre certi dell'identità e dell'affidabilità delle persone a cui si stanno dando i dati della carta di credito.

Utilizzo "On Line" della carta di credito

La diffusione esponenziale di internet avvenuta negli ultimi anni ha consentito uno sviluppo sempre più di massa del commercio elettronico e con esso un uso sempre più spinto della carta di credito, che in tale contesto rappresenta la principale modalità di pagamento utilizzata. Ma se tale sviluppo ha creato buone opportunità sia per gli utilizzatori che per gli operatori commerciali on line, dall'altra ha consentito l'insorgere di frodi ogni giorno sempre più sofisticate.
La tecnologia offre soluzioni di sicurezza sempre più efficienti ed efficaci, ma nulla possono queste se accanto ad esse l'utente non adotta le opportune cautele quando utilizza i propri terminali (PC, SmartPhone e Tablet), quando naviga in Internet e quando effettua i pagamenti con la sua carta di credito.

Il Personal Computer

In ogni casa ormai è presente un PC che rappresenta, al momento, il mezzo principale con il quale si effettuano gli acquisti on line.
La protezione del PC diventa quindi uno snodo essenziale per garantire la sicurezza dei propri acquisti on line ed è per questo che deve essere protetto in maniera adeguata.
Un semplice insieme di regole da adottare per il proprio PC sono le seguenti:

- costruire delle password per l'accesso al PC e ai propri servizi (es. e-mail, area riservata della carta, siti degli e-merchant, etc) che siano robuste e nel contempo anche semplici da ricordare;

- non memorizzare le password di accesso ai propri servizi sul browser o su un documento memorizzato sul PC e cambiarle di frequente (almeno ogni tre mesi);
- aggiornare costantemente i software presenti sul Pc secondo le modalità di ogni singolo software adotta;
- installare antivirus inclusivo di un antispyware, o/o un antitrojan. Diffidare di prodotti poco conosciuti distribuiti non a pagamento perché potrebbero essere dei trojan distribuiti da hacker. Andare sui forum specializzati e analizzare le opinioni degli altri utilizzatori.
- installare un firewall personale sul proprio PC.

Alcuni approfondimenti

Come costruire una Password robusta……

La robustezza di una password si basa prevalentemente sulla sua lunghezza e sulla "non predicibilità" del suo contenuto. Evitare quindi accuratamente di utilizzare il proprio nome/cognome, la data di nascita, la combinazione dei due, il nome dei figli, della moglie, del proprio cane e così via. Bisogna evitare in pratica qualunque informazione che gli hacker possano reperire dai social tipo facebook e attuare quello che si chiama un dictionary attack con il quale cercano di "indovinare" la password.

Viceversa, bisogna evitare di produrre password molto complesse che poi si scrivono sul classico post it attaccano sul monitor del computer. Si possono utilizzare delle "passphrase" che contengono una frase intera tipo "Vivaglignocchidimiamadre!" mettendo sempre la prima maiuscola e un carattere speciale alla fine.

Altro metodo molto utilizzato è costruire la password mettendo le iniziali di un ritornello/poesia/ canzone che si conosce a memoria. Ad esempio "nel mezzo del cammin di nostra vita mi ritrovai per una serva oscura che la dritta via avea smarrita" diventa "Nmdcdnvmrpusocldvas!". La password può essere ulteriormente complicata inserendo numeri, altri caratteri speciali, alternando le lettere maiuscole/minuscole e così via.

Lo sapevi che……

Hacking *deriva dal verbo "to hack" che significa letteralmente "spaccare", "tagliare a pezzi". Trasposto all'informatica, significa cambiare un programma in modo che operi o compia operazioni che il programmatore originale non avrebbe voluto fare o considerato. Hacking può significare anche usare un computer senza averne diritto.* ***Hacker*** *è colui che effettua hacking.*

Si definisce ***Malware*** *(contrazione dei termini inglesi malicious e software) un qualsiasi software creato con il solo scopo di causare danni più o meno estesi al computer su cui viene eseguito*

Per ***Social Engineering*** *(in italiano Ingegneria Sociale) si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni o perpetrare truffe.*

Gli SmartPhone e i Tablet

Gli SmartPhone e i Tablet sono strumenti molto pratici e semplici da usare e si stanno diffondendo sempre più anche per effettuare acquisti on line (i cosiddetti mobile payment). Tale diffusione attira però anche truffatori che stanno sviluppando nuove tecniche di attacco mirate per questi terminali.

In linea di principio valgono le stesse cautele descritte per il PC, anche se la loro portabilità li rende più vulnerabili a minacce quali furto e smarrimento.

Le principali cautele da adottare per questi terminali sono:

- assicurarsi che tutti i software presenti su tali dispositivi (sistema operativo e le varie APP installate) siano regolarmente aggiornati installando tutti gli aggiornamenti non appena disponibili;
- non memorizzare sul cellulare dati sensibili di pagamento (es. password, numero di carta di credito, etc) che possono essere utilizzati da un hacker per perpetrare una frode;
- non lasciare incostuditi i propri terminali mobili;
- non installare Jailbreaks e rooting su smartphone e tablet perché rimuovono i principali meccanismi di sicurezza, consentendo l'accesso a terzi;
- acquistare le APP, i software e gli aggiornamenti da stili affidabili e preferibilmente da store ufficiali;
- utilizzare solo hotspot sicuri e disattivare il Bluetoot quando non utilizzato;
- custodisci con cura l'utenza telefonica su cui ricevi i servizi SMS e in caso di funzionamento anomalo contattaci ai recapiti indicati alla sezione "contatti" del sito www.sellapersonalcredit.it, potrebbe infatti trattarsi di un furto di identità telefonica finalizzato a un tentativo di frode.
- se si regala, si vende o si rottama uno smartphone o un tablet assicurarsi che tuttui i dati sensibili, ed in particolare quelli di pagamento, siano stati completamente cancellati;

Lo sapevi che……

*Il **Remote Lock** e il **Remote Wipe** sono delle funzionalità disponibile su quasi tutte le principali tipologie di SmartPhone e Tablet che consentono di bloccare il terminale (remote lock) o di cancellare tutti i dati in esso contenuti (remote wipe) in caso di smarrimento o furto del terminale mobile.*
*Il **rooting** è una tecnica utilizzata sugli smartphone con sistema operativo Android per aggirare le limitazioni e le misure di sicurezza realizzate dal fornitore dello smartphone e acquisire il controllo del sistema operativo.*
*Il **Jailbrea**k è una procedura che permette di sbloccare l'accesso a tutti i file che compongono il sistema operativo di Apple che troviamo su iPhone, iPad ed iPod Touch.*

Navigare in Internet

La navigazione in Internet è irta di pericoli e pertanto, anche in questo caso, l'utente deve adottare delle semplici cautele di buon senso:

- non andare su siti potenzialmente pericolosi (es. i siti di giochi on line);
- scaricare software solo da siti affidabili ed effettuare una scansione dell'antivirus prima di installarli;
- se appaiono pop up inattesi, come quelli che avvertono della presenza di virus sul computer e che offrono una soluzione, non selezionare il link e non autorizzare nessun download. Potreste scaricare e installare software potenzialmente dannosi;
- non inserire i dati personali (indirizzo di e-mail, numero di telefono, etc) se non sono finalizzati ad uno scopo ben preciso e in siti che non sono considerati affidabili;
- controllare la impostazioni sui social (facebook, twitter, etc) ed evitare di inserire informazioni personali che possono essere viste da molte persone. Queste informazioni potrebbero essere utilizzate da un hacker per effettuare un attacco finalizzato a carpire le credenziali utilizzate dall'utente.

Il Phishing

*Il **Phishing** è una frode informatica finalizzata all'acquisizione di dati personali riservati e sensibili come, ad esempio, numeri di carta di credito, password, dati relativi al proprio conto e così via. Questi sono generalmente richiesti tramite e-mail in cui il mittente si presenta come una fonte legittima per richiedere l'immissione di tali dati. Una volta inseriti, l'autore della frode potrà operare al posto dell'utente legittimo, movimentando somme di denaro dal suo conto/carta di credito.*

*Il **Phishing** è una tecnica di Ingegneria Sociale che si basa sulla reazione emotiva delle persone di fronte a eventi critici. Non ha caso, la richiesta di inserire i propri dati nelle mail di Phishing sono precedute da frasi tipo "il conto o la carta sono stati bloccati", "la carta è stata disattivata", "verificare la transazione", "aggiorni i suoi dati", etc.*

*Il termine **Phishing** è una variante della parola fishing che in inglese significa pescare. Infatti, il phisher (l'autore del phishing) invia migliaia di mail a indirizzi carpiti su internet (ad esempio sui social o con altra mail di phishing) e confida sull'impatto emotivo che la mail avrà sui suoi potenziali "pesci".*

Come riconoscere le mail di Phishing

Le mail di phishing sono facilmente riconoscibili perché generalmente contengono la richiesta di inserire le proprie credenziali nel sito della banca o dell'emittente della carta di credito che è raggiungibile cliccando su un link riportato nella mail.

Sella Personal Credit, così come tutte le banche e gli istituti di pagamento, non inviano mai ai propri clienti della mail con un link dentro, ma eventualmente invitano i clienti ad accedere alla sua area riservata disponibile sul sito della banca/istituto di pagamento.
Inoltre, osservare con attenzione nella mail i seguenti aspetti:

- gli indirizzi da cui provengono queste mail sono generalmente lunghi, con errori e caratteri non usuali;
- non sono personalizzate (es. "Gentile Cliente" invece di "Gentile Sig, Rossi") e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici, etc) facendo uso di toni intimidatori, ad esempio minacciando la disattivazione della carta in caso di mancata risposta;
- non contengono quasi mai una scadenza per l'invio delle informazioni richieste;
- i testi delle mail di phishing contengono errori nella formattazione e nel testo poiché molti dei phisher agiscono dall'estero;
- le mail contengono dei link che dirottano l'utente sul sito falso creato dal phisher;
- la url del sito del phisher è simile a quello della società, ma contiene delle piccole differenze soprattutto sull'indicazione del Paese che molto spesso non è .it, indicando così che il sito è localizzato all'estero;
- la ragione sociale è simile alla società, ma non identica.

Come difendersi dal Phishing

I programmi per la navigazione (browser) maggiormente utilizzati hanno sviluppato delle funzionalità che incrementano la sicurezza della navigazione ed è quindi buona prassi tenere il browser che si utilizza costantemente aggiornato all'ultima versione (le patch sono disponibili sui siti delle aziende produttrici). Accanto al browser, si consiglia di utilizzare software antivirus aggiornati e toolbar con filtro anti-phishing gratuito.
Ad ogni buon conto, una volta riconosciute le mail di phishing, non aprirle mai, neanche in anteprima.
Se si ha il dubbio di essere caduto in un phishing, informare tempestivamente l'Ufficio clienti di Sella Personal Credit che adotterà le necessarie azioni di contrasto.

Gli acquisti on line

Quando si effettuano gli acquisti on line, adottare opportune cautele prima, durante e dopo l'acquisto. La prima verifica da fare è sull'affidabilità del e-merchant valutando i seguenti indizi:

- verificare se il sito fornisce informazioni sulle misure di sicurezza realizzate (es. cifratura dei dati) e se il merchant utilizza soluzioni di sicurezza riconosciute quali, ad esempio, 3-D Secure, Verified by Visa, etc.;

- verificare che il sito riporta i dati dell'azienda, i recapiti (mail, telefono, fax,..), le condizioni generali di fornitura, etc;
- verificare che la connessione avviene in maniera sicura (l'indirizzo inizia con https e nella barra di stato è presente un lucchetto);
- leggere le recensioni di precedenti clienti che hanno acquistato sul sito per capire la qualità dei prodotti e del servizio offerto;
- fornire i dati personali e confidenziali solo nella misura in cui questi sono assolutamente necessari per il servizio desiderato;
- non fornire, se richiesto, la carta di credito a puri scopi informativi o per controllare l'età. Le aziende che richiedono tali informazioni raramente sono serie.

Verificata l'affidabilità dell'e-merchant, si procede con l'acquisto verificando sempre quello che si sta acquistando, il prezzo e le condizioni generali del commerciante prima di inserire i dati della carta di credito ed inoltrare l'ordine.

Dopo l'acquisto, controllare il proprio estratto conto per verificare che l'addebito sia stato effettuato in maniera corretta.
È comunque una buona prassi controllare costantemente l'estratto conto della propria carta di credito per essere certi che non ci siano addebiti non riconosciuti. In quest'ultimo caso, chiamare tempestivamente l'Ufficio Clienti di Sella Personal Credit.