



# 2011

## E-commerce & Security



Studente : Angelico Massimo

823903 - [mss.angelico@gmail.com](mailto:mss.angelico@gmail.com)

Professore : Marek Maurizio

Seminario di E-commerce

28/03/2011

## 1. Sommario

1	Introduzione .....	3
2	Sistemi di pagamento on-line.....	4
3	I protocolli per la sicurezza delle transazioni .....	6
3.2	SSL (Secure Sockets Layer).....	7
3.3	SET (Secure Electronic Transaction).....	8
3.4	SET Vs SSL .....	9
3.5	HTTPS .....	9
4	Principali tipologie di attacco .....	10
4.2	Phishing .....	10
4.3	Pharming .....	11
4.4	Firesheep.....	11
4.5	Negazione del servizio (DoS) .....	11
4.6	Keylogging.....	12
5	Truffe On-line .....	12
6	Come proteggersi .....	13
7	Alcuni casi reali .....	14
7.2	Hack EMV.....	14
7.3	Truffa su Facebook.....	15
8	Conclusioni .....	15
9	Sitografia .....	16

## 1 Introduzione

L'obiettivo principale che mi ha portato a realizzare questo seminario è stato fortemente quello di documentarmi maggiormente su un mondo che sempre più sta diventando un colosso del web. In particolare ho voluto capirci di più sui sistemi di pagamento on-line, visto che io in primis sono sempre stato scettico nei confronti di tale tecnologia. Grazie a questo seminario ed in particolare al corso di e-commerce ho "aperto gli occhi" e cambiato la mia idea, in positivo, sul commercio telematico. Oltre al fatto di aggiornare il mio pensiero a tal proposito, ritengo che parlare di sicurezza non sia mai argomento inutile, poiché la prudenza non è mai troppa. Nel prosequio del documento verranno presentati i principali sistemi di pagamento on-line e descritto il loro funzionamento, successivamente verranno presentati temi sulla sicurezza e delle accortezze per potersi difendere da attacchi informatici.

Fin dagli albori di internet, l'e-commerce (e successivamente l'e-banking) è stata una delle principali applicazioni in grado di cogliere le opportunità offerte dal web. Anche per il mobile internet, l'e-commerce rappresenta un servizio fondamentale. Si parla in questo contesto di m-commerce le cui potenzialità sono addirittura superiori a quelle dell'e-commerce tradizionale, soprattutto se si considerano i molteplici scenari di utilizzo oggi possibili (acquisti direttamente dal terminale mobile "on the road").

Garantire agli utenti la sicurezza delle transazioni effettuate significa proteggere sia le applicazioni sui terminali mobili sia i siti di mobile web. Negli ultimi anni abbiamo assistito all'enorme crescita dell'accesso ad internet in mobilità (mobile internet) e si presume che il trend continui su tale strada.

## 2 Sistemi di pagamento on-line

Lo sviluppo del commercio *on-line* ha come necessaria conseguenza l'implementazione di nuovi sistemi di pagamento che determinano il passaggio dalla banconota cartacea al "contante digitale".

Negli ultimi anni sono stati creati diversi strumenti per i pagamenti in internet e molti di questi richiedono l'intervento di una terza parte che funga da intermediario della transazione. A seconda del tipo di strumento utilizzato, l'intermediario può risultare legato da un rapporto contrattuale al compratore, al venditore o ad entrambi.

I fondamentali vantaggi connessi all'utilizzo dei metodi di pagamento *on-line* sono rappresentati dalla convenienza e dall'efficienza che li caratterizzano.

Alcuni di questi caricano una commissione comparabile a quella che viene addebitata con l'utilizzo delle carte di credito, ma altri sono meno costosi, quando non completamente gratuiti. Poiché i pagamenti *on-line* restano per molti aspetti non disciplinati, assistiamo ad una sorta di contrattualizzazione dei diritti di compratori e venditori.

Le modalità di pagamento utilizzabili nella rete sono sostanzialmente :

### **Carta di Credito**

Il principale metodo di pagamento per le transazioni on-line è sicuramente la carta di credito. Questo tipo di pagamento prevede che il cliente invii al venditore, compilando un'apposita pagina Web, gli estremi della propria carta di credito. In seguito lo stesso venditore trasmette i dati alla banca avviando una procedura di verifica e accredito. Le transazioni vengono addebitate sul conto corrente in via posticipata, solitamente a metà del mese successivo all'acquisto.

### **Bonifico Bancario**

Al termine della transazione il sito del venditore comunica gli estremi bancari ai quali effettuare un bonifico bancario per l'ammontare della merce. Al ricevimento del bonifico l'esercente invia la merce. Il problema, in questo caso, è costituito dai tempi tecnici di effettuazione del bonifico. Tali problematiche possono essere risolte con il web banking.

### **Contrassegno**

Questa forma di pagamento consente al cliente di correre il rischio minore, poiché il pagamento viene effettuato solo una volta che la merce è giunta a destinazione. Possono però sorgere delle difficoltà nel senso che al momento della consegna bisogna essere presenti e avere i soldi in casa. Il costo per inviare la merce in contrassegno sono di circa 5 euro che il venditore generalmente aggiunge al totale del valore della merce acquistata e delle spese di spedizione normale.

## **PayPal**

PayPal è la società del gruppo eBay che consente a chiunque possieda un indirizzo e-mail di inviare o ricevere pagamenti online in modo facile, veloce e sicuro. Il funzionamento di PayPal è molto simile a quello di un comune conto corrente bancario, dopo aver aperto il conto si può inviare o ricevere denaro ed effettuare pagamenti on-line. Tale sistema è utilizzato di frequente su eBay o presso numerosi negozi on-line, come metodo alternativo alla carta di credito.

## **Carte Prepagate**

Si tratta di carte che si possono acquistare con un importo disponibile prefissato, come accade similmente con le carte telefoniche. Con queste carte è possibile acquistare via Internet.

A tal fine, al momento dell'ordine, tra le possibilità previste per il pagamento si inserisce il nome della carta il codice PIN ed una Password in modo da poter effettuare il pagamento. L'importo viene così detratto dalla carta. Il vantaggio rispetto alla carta di credito tradizionale sta nel fatto che, in caso di abusi, si è sicuri che il danno subito non potrà superare il valore della carta prestabilito. Per questo motivo è consigliabile acquistare carte prepagate dal valore non molto elevato.

<b>Pagamento</b>	<b>Vantaggi</b>	<b>Svantaggi</b>
<i>Carta di Credito</i>	<ul style="list-style-type: none"> <li>- Facilità d'uso;</li> <li>- Confidenza nell'utilizzo della carta di credito;</li> <li>- Sistema di pagamento diffuso</li> </ul>	<ul style="list-style-type: none"> <li>- Il venditore deve pagare percentuale sulle transazioni</li> </ul>
<i>Bonifico bancario</i>	<ul style="list-style-type: none"> <li>- Semplicità d'uso;</li> <li>- Costi contenuti;</li> <li>- Sistema di pagamento molto diffuso</li> </ul>	
<i>Contrassegno</i>	<ul style="list-style-type: none"> <li>- Facilità d'uso;</li> <li>- Ampia diffusione;</li> <li>- Nessun canone periodico per l'esercente</li> </ul>	<ul style="list-style-type: none"> <li>- Costi elevati per l'acquirente</li> </ul>
<i>PayPal</i>	<ul style="list-style-type: none"> <li>- PayPal è facile e può essere eseguito in pochi minuti;</li> <li>- Discreta diffusione del servizio;</li> <li>- Nessuna tariffa mensile e nessuna tariffa di configurazione</li> </ul>	<ul style="list-style-type: none"> <li>- E' richiesta una doppia registrazione da parte dell'acquirente se non è già registrato a PayPal;</li> <li>- Tariffe per le transazioni</li> </ul>
<i>Carte prepagata</i>	<ul style="list-style-type: none"> <li>- Sono facili da usare e veloci da ottenere</li> </ul>	<ul style="list-style-type: none"> <li>- Scarsa diffusione,</li> <li>- Più adatte alle microtransazioni;</li> <li>- Costi elevati di attivazione e ricarica</li> </ul>

### 3 I protocolli per la sicurezza delle transazioni

L'usuale pagamento a mezzo carta di credito, nato negli anni '60, in un'epoca sicuramente antecedente alla diffusione di internet, è criticato a causa della sua intrinseca pericolosità relativamente al buon fine della transazione. Si teme, infatti, che, nel momento in cui l'acquirente trasmetta al fornitore i propri dati (numero di carta, identità del titolare, scadenza) attraverso internet, gli stessi possano essere intercettati da terzi ed utilizzati abusivamente.

In realtà, il problema sopra esposto si pone anche al di fuori di internet, mediante il normale utilizzo della carta di credito: nella ricevuta che

rimane in mano al negoziante sono infatti presenti gli estremi della nostra carta di credito.

A differenza di quanto potrebbe sembrare, la parte che, in astratto, corre i rischi maggiori dall'effettuazione di un pagamento a distanza mediante carta di credito è il venditore: questi, infatti, accettando il pagamento senza verificare l'identità tra il titolare della carta di credito e l'acquirente, si trova in una posizione giuridicamente molto debole. L'acquirente, per contro, potrà validamente fruire di una tutela abbastanza forte: potrà proporre azione di nullità del contratto nei confronti del venditore visto che potrà sostenere di non avere espresso la propria volontà formativa del contratto; potrà, altresì, ottenere dall'istituto di credito emittente il risarcimento della somma fraudolentemente pagata. La banca, per altro, non potrà validamente sollevare un'ipotetica responsabilità del titolare per ritardo nella comunicazione di smarrimento, visto e considerato che un uso illecito della propria carta può essere fatto da terzi, anche se il titolare rimane nell'effettiva disponibilità della stessa. Acquisti falliti, paure sulla sicurezza dei trasferimenti ed insoddisfazione nei confronti degli strumenti utilizzabili sono ostacoli con i quali confrontarsi per garantire lo sviluppo del commercio su internet. Da qui l'esigenza di implementare standard di sicurezza per le transazioni al fine di costruire la necessaria fiducia tra gli utenti della rete.

### 3.2 SSL (Secure Sockets Layer)

Un diffuso metodo per garantire la sicurezza ai venditori *on-line* è rappresentato dal protocollo SSL (*Secure Sockets Layer*), il quale stabilisce un canale di comunicazione sicuro tra un *browser* ed un *server* di internet. Questo protocollo fu implementato da *Netscape Communications* affinché fosse utilizzato con *Netscape Navigator*. La prima versione per il pubblico fu la 2.0 e fu diffusa con *Netscape Navigator* versioni 1 e 2. Sebbene fosse estremamente ben progettata, le seppur piccole imperfezioni ed i difetti di sicurezza di quest'ultima versione portarono alla rapida evoluzione del SSL versione 3.0 nel 1996. Circa nello stesso periodo, la *Microsoft Corporation* introdusse una tecnologia per la sicurezza del suo nuovo *browser Internet Explorer* chiamata *Private Communication Technology* (PCT). La fusione, poi, tra l'SSL e il PCT, al fine di prevedere un'unica proposta per uno standard comune per internet, portò alla creazione del *Transport Layer Security* (TLS) *protocol*. La componente fondamentale di una connessione protetta dal SSL è rappresentata dal *SSL Handshake Protocol*: esso comincia con un'obbligatoria autenticazione del *server*, mentre per il *client* è opzionale; dopo che il procedimento di autenticazione si è concluso, ha luogo la

contrattazione per la sequenza cifrata: il parametro così deciso sarà utilizzato durante l'intera sessione e garantirà la sicurezza di tutti gli scambi di dati.

In un pagamento *on-line*, quando un consumatore (*client*) desidera comprare qualcosa su internet da un commerciante (*server*) usando una connessione SSL, si assiste ad un procedimento che può essere suddiviso in due passaggi: in un primo momento si ha la costituzione della sessione, poi, avviene lo scambio di informazione tra *client* e *server* attraverso una connessione sicura. A questo punto, il *client* può riempire il suo carrello virtuale e quindi pagare il conto. Il *client* generalmente deve sottoscrivere alcune importanti informazioni personali quali il numero di carta di credito, la data di scadenza, il nome e l'indirizzo per la fattura. Tutte le informazioni che vengono così date in uscita sono cifrate ancora dal *server* con il protocollo SSL; viene spedita una richiesta per ottenere un punto di transito con conversione dei protocolli (*gateway*) per il pagamento in internet e si andrà, così, a chiedere l'autorizzazione alla banca. L'SSL *server* ottiene, allora, o l'autorizzazione o il rifiuto per la transazione attraverso il *gateway* per il pagamento, e spedisce il risultato al commerciante ed al consumatore. Tutto questo, però, non assicura la salvaguardia dei dati della carta di credito una volta che siano stati raccolti dal venditore: se questi non garantisce la protezione dei dati ricevuti, le informazioni inviate dall'utilizzatore non saranno più protette di quanto lo sarebbero state se non fosse stata utilizzata alcuna misura di sicurezza.

### 3.3 SET (Secure Electronic Transaction)

Al fine di migliorare la sicurezza dei pagamenti a mezzo carta di credito, nel febbraio 1996 è stato sviluppato uno specifico protocollo denominato SET (*Secure Electronic Transaction*). Questo sistema garantisce: la confidenzialità delle informazioni trattate; l'integrità dei messaggi; la certificazione di autenticità delle parti coinvolte nella transazione. Esso funziona nel modo seguente: il titolare della carta di credito SET riceve dalla banca emittente un certificato criptato in forza del quale egli è identificato univocamente dall'istituto di credito. Il titolare registra sul suo computer il certificato e, nel momento in cui effettua un pagamento via internet, dà la possibilità alla banca di certificare al venditore se chi sta utilizzando la carta sia l'effettivo titolare della stessa. Così facendo, la banca si sostituisce al venditore nell'onere di verificare la corrispondenza tra la firma di chi effettua il pagamento e la firma apposta sul retro della carta di credito, onere che, ovviamente, nelle transazioni via internet,

risulterebbe impossibile da assolvere. In questo modo chi riceve il pagamento risulta essere maggiormente garantito visto che, in caso di problemi, potrà tutelarsi sia nei confronti dell'acquirente, che ha negligenzemente permesso che altri utilizzassero per lui la carta SET, sia nei confronti dell'istituto emittente che, alla prova dei fatti, non ha saputo garantire un sistema sicuro ed inviolabile. I nuovi contratti delle carte di credito SET imporranno, inoltre, in capo al titolare un rigoroso onere di custodia del certificato. Nel caso in cui si verifichi che qualcuno sia venuto a conoscenza del certificato e del numero della carta di credito, il titolare non può contestare l'eventuale esborso addebitatogli fintantoché non abbia provveduto a denunciare all'istituto di credito emittente la violazione di sicurezza. Il SET, per garantire la confidenzialità delle informazioni, assicurare l'integrità dei messaggi e autenticare l'identità degli utenti, utilizza la crittografia a chiave simmetrica ed asimmetrica.

### 3.4 SET Vs SSL

Mettiamo ora a confronto i due protocolli maggiormente diffusi sulla rete per la sicurezza dei pagamenti *on-line*, ovvero SET ed SSL.

Innanzitutto il SET protegge l'identità di tutte le parti coinvolte nella transazione attraverso la firma digitale; il SSL non è, invece, predisposto per porre in essere un tale tipo di operazione.

Il SET, infine, diversamente dal SSL, non solo definisce tutti i necessari protocolli per lo scambio dei dati al fine del trasferimento tra il consumatore ed il commerciante, ma anche garantisce che questi dati siano trasferiti alla banca del commerciante. Resta, però, un'importante difficoltà per lo sviluppo del SET: esso rappresenta una tecnologia nuova, non ancora sufficientemente testata e molto più difficile da implementare rispetto al SSL: i suoi alti costi, unitamente alla mancanza di incentivi economici per i commercianti, rappresentano un freno alla sua diffusione. Inoltre, l'utilizzo di SET richiede l'acquisto di software da utilizzare per un sito di e-commerce e l'installazione di un borsellino elettronico sul client.

### 3.5 HTTPS

I protocolli di sicurezza utilizzati in rete, richiedono protocolli applicativi altrettanto sicuri quali HTTPS ed SMTP per poi concludere con TCP a livello trasporto.

In particolare il protocollo HTTPS viene utilizzato per aggiungere sicurezza alle pagine del WWW in modo tale da rendere possibili applicazioni quali il commercio elettronico. L'abbinamento di SSL al normale standard HTTP permette di ottenere un nuovo protocollo: l'HTTPS. Questo garantisce l'invio delle informazioni personali sottoforma di pacchetti criptati. In questo modo, la trasmissione delle informazioni avviene in maniera sicura, prevenendo intrusioni, manomissioni e falsificazioni dei messaggi da parte di terzi.

Il protocollo HTTPS garantisce quindi tanto la trasmissione confidenziale dei dati, quanto la loro integrità. L'HTTPS è un URI (Uniform Resource Identifier) sintatticamente identico allo schema `http://` ma con la differenza che gli accessi vengono effettuati sulla porta 443 e che tra il protocollo TCP e HTTP si interpone un livello di crittografia/autenticazione. In pratica viene creato un canale di comunicazione criptato tra il client e il server attraverso lo scambio di certificati; una volta stabilito questo canale al suo interno viene utilizzato il protocollo HTTP per la comunicazione.

Questo protocollo assicura una buona protezione contro attacchi del tipo *man in the middle*. Per impostare un web server in modo che accetti connessioni di tipo `https`, l'amministratore deve creare un certificato digitale ovvero un documento elettronico che associa l'identità di una persona ad una chiave pubblica. Questi certificati devono essere rilasciati da un certificate authority o comunque da un sistema che accerta la validità dello stesso in modo da definire la vera identità del possessore.

In particolari situazioni, come per esempio nel caso di aziende con una rete intranet privata, è possibile avere un proprio certificato digitale che si può rilasciare ai propri utenti.

Questa tecnologia quindi può essere usata anche per permettere un accesso limitato ad un web server. L'amministratore spesso crea dei certificati per ogni utente che vengono caricati nei loro browser contenenti informazioni come il relativo nome e indirizzo e-mail in modo tale da permettere al server di riconoscere l'utente nel momento in cui quest'ultimo tenta di riconnettersi senza immettere le credenziali.

## 4 Principali tipologie di attacco

### 4.2 Phishing

Una delle tecniche più conosciute ed utilizzate per finalizzare un furto di identità è senz'altro il phishing. Questa attività illegale si basa sull'utilizzo delle comunicazioni elettroniche, specie messaggi di posta elettronica falsi, per reperire informazioni relativi all'utente vittima.

Il contenuto di queste e-mail contiene spesso link a siti fasulli, costituiti da pagine molto simili a quelle del sito reale in modo da ingannare l'utente facendogli inserire su appositi form dati sensibili. Questo tipo di attività, pur risultando ancora molto usata ed efficace, sta cedendo il passo ad una nuova tecnica che negli ultimi anni sta prendendo sempre più valore: il vishing. Il vishing è una particolare tipologia di phishing che si basa sulla comunicazione vocale, ovvero attraverso telefonate alla vittima. Al contrario delle e-mail, una telefonata può risultare molto più efficace, aprendo nuovi scenari anche a coloro che non hanno grande dimestichezza con il mondo dell'informatica.

Inoltre, il vishing trova sempre più forza, grazie alla diffusione capillare delle piattaforme di Voice over IP, grazie alle quali risulta più facile per i truffatori camuffare il proprio identificativo.

### 4.3 Pharming

Pharming è una tecnica di cracking, utilizzata per ottenere l'accesso ad informazioni personali e riservate, con svariate finalità. Grazie a questa tecnica, l'utente è ingannato e portato a rivelare inconsapevolmente a sconosciuti i propri dati sensibili, come numero di conto corrente, nome utente, password, numero di carta di credito e molti altri dati. L'obiettivo finale del pharming è il medesimo del phishing, ovvero indirizzare una vittima verso un server web "clone" appositamente attrezzato per carpire i dati personali della vittima. Per difendersi dal pharming non esistono ancora dei programmi specifici se non i firewall che tentano di impedire l'accesso al proprio PC da parte di utenti esterni e programmi antivirus che bloccano l'esecuzione di codice malevolo. Se il sito a cui ci si collega è un sito sicuro prima dell'accesso verrà mostrato un certificato digitale emesso da una autorità di certificazione conosciuta, che riporterà i dati esatti del sito.

### 4.4 Firesheep

Un'altra tecnica, ancor più pericolosa, poiché utilizzabile da chiunque, non richiede infatti, nessuna conoscenza specifica di informatica.

Firesheep è un add-on per Firefox in grado di rendere estremamente facile il furto di identità. Questa estensione "cattura" le credenziali di accesso degli utenti presenti su una stessa rete, e con un semplice login il cookie corrispondente viene catturato e lo mette a disposizione per l'accesso in una comoda barra laterale del browser. Firesheep sfrutta alcuni bug presenti nei siti web, quali Facebook, Amazon, Twitter e molti altri. Per recuperare le sessioni attive, che viaggiano in chiaro, utilizza un apposito script. Alcuni siti, oggetto di tali attacchi, si sono messi al riparo utilizzando connessioni sicure sfruttando protocollo HTTPS durante il trasferimento dei cookies.

### 4.5 Negazione del servizio (DoS)

Un'altra tipologia di attacco, frequente sul web ed in particolare nei confronti di siti dedicati all'e-commerce, è il DoS (Denial of service). Questo attacco viene condotto attraverso reti (botnet) formate da alcuni computer cosiddetti zombie, che connettendosi contemporaneamente ad un sito Internet lo sovraccaricano rendendolo inutilizzabile. Ancor più distruttivo è l'attacco distribuito su larga scala DDoS dove i computer attaccanti sono migliaia. I proprietari dei computer coinvolti spesso non

sono nemmeno consapevoli di far parte della botnet (l'insieme di computer infetti) e questo rende la difesa molto più difficile, poiché individuare l'attaccante non è compito facile.

Questa tipologia di attacco viene normalmente utilizzata per scoprire falle nel sito di e-commerce, in modo da recuperare informazioni sugli utenti che si collegano, in particolare le credenziali d'accesso e numero di carte di credito.

Inoltre, in quest'ultimo periodo si sta assistendo al fenomeno del racket su Internet. Bande organizzate di cracker lanciano attacchi DoS a siti web chiedendo il pagamento di una somma di denaro per farli cessare.

#### 4.6 Keylogging

Un'altra tecnica consiste nell'inserimento di applicativi di keylogging. Un keylogger è uno strumento in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio computer.

Esistono due tipi di keylogger:

- *hardware*: vengono collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera;
- *software*: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.

I keylogger hardware sono molto efficaci in quanto la loro installazione è molto semplice e il sistema non è in grado di accorgersi della loro presenza.

### 5 Truffe On-line

Gli acquisti su internet sono una comodità e una vera e propria manna dal cielo per la concorrenza. E' anche vero che il rischio di incappare in una truffa online è sempre elevato in particolar modo nei siti di commercio elettronico e di aste tra privati. Una truffa online avviene principalmente attraverso l'invio di e-mail e collegamenti a siti fasulli.

Per quanto riguarda le e-mail, il loro obiettivo principale è quello di rubare la coppia user-password all'utente, in particolare le credenziali di servizi bancari presenti sul web, in modo da potervi accedere ed effettuare una transazione dei soldi su altri conti correnti. Per sottrarre i dati sensibili, il truffatore, invia e-mail false, dette e-mail di phishing dove si cerca di invitare l'utente ad accedere a siti altrettanto fasulli che richiedono una login. Spesso per convincerci che il messaggio è autentico, le e-mail di phishing hanno la stessa impostazione grafica di quelle originali dove però viene falsificato il mittente dell'e-mail inserendo, per esempio, il nome della nostra banca.

Alcune volte, invece di inoltrare l'utente in un sito fasullo, chiedono espressamente di rispondere all'e-mail fornendo le proprie credenziali fingendo un finto guasto al sistema informatico del servizio web a cui l'utente fa riferimento.

Questi messaggi di posta elettronica, normalmente, sono facili da scoprire poiché sono impersonali e non hanno nessun riferimento individuale, inoltre vengono inviate a decine di indirizzi sparsi per la rete.

Altre tipologie di truffe hanno a che fare con i siti di e-commerce, dove il truffatore basta che crei un sito web con dati false e inizi a vendere prodotti a prezzi molto vantaggiosi. Questo tipo di sito nasconde un cosiddetto negozio fantasma, in quanto, dopo aver acquistato il prodotto questo non viene mai spedito e il negozio sparisce.

## **6 Come proteggersi**

Per quanto riguarda i siti phishing bisogna porre molta attenzione all'url presente nel web browser in modo da verificare subito se si è connessi al sito giusto, inoltre esistono appositi plug-in per Firefox, esempio Netcraft toolbar, che blocca l'accesso a siti truffaldini mostrando un pop-up che notifica all'utente l'evento. Prima di effettuare un pagamento online, in particolar modo su un venditore non conosciuto, bisogna prima di tutto verificare se nel sito sono presenti la partita IVA e riferimenti quali il numero di telefono e l'indirizzo fisico che permettono di contattare l'azienda. In secondo luogo, verificate che il negozio on-line permetta altre forme di pagamento oltre alla carta di credito, per esempio la vendita in contrassegno. E' anche possibile ricercare informazioni sul venditore utilizzando i motori di ricerca, in modo da reperire recensioni e modalità di acquisto su quel sito web.

## 7 Alcuni casi reali

### 7.2 Hack EMV

Un giovane studente dell'Università di Cambridge (Omar S. Choudary), presentando una tesi con tanto di video dimostrativo, ha mostrato come sia possibile utilizzare una carta di credito rubata sfruttando le falle presenti nella tecnologia "chip & pin" (basata sul protocollo EMV). Ha quindi realizzato un dispositivo portatile per aggirare la tecnologia in questione e usare, senza conoscerne il codice PIN, una carta di credito rubata per fare acquisti.



Di fronte alle potenziali critiche sugli impieghi illeciti di un tale apparecchio, l'inventore ha precisato che l'obiettivo primario del dispositivo è quello di evitare frodi ai danni dei titolari delle carte di credito (auspicati destinatari dello *Smart Card Detective*). Infatti, lo studente informa che l'SCD

avrebbe varie funzionalità, e il display presente sul circuito visualizzerebbe in tempo reale alcune informazioni sulla transazione, permettendo al titolare della carta di controllare che la somma visualizzata sul POS di un dato esercizio commerciale sia effettivamente quella addebitatagli e che il terminale non sia stato di fatto alterato.

Maggiori info :

- <http://www.intertraders.eu/notizie/96/Come-usare-una-carta-di-credito-rubata-per-fare-acquisti.html>
- [http://www.youtube.com/watch?v=3MD6WEGMmag&feature=player\\_embedded](http://www.youtube.com/watch?v=3MD6WEGMmag&feature=player_embedded)

### 7.3 Truffa su Facebook

La nuova applicazione che permette di giocare online a Twilight Breaking Dawn presente sul più famoso social network è una vera e propria truffa. Infatti, una volta cliccato sull'immagine che permette l'accesso all'applicazione si viene reindirizzati su una pagina Facebook con la stessa immagine ed il tasto "Play Now" e se non si utilizzano applicazioni di protezione come "No Script" e malauguratamente si inizia a giocare, automaticamente viene deciso che il gioco "vi piace", esponendo così al pericolo anche tutti gli amici. In più viene chiesto di permettere a "terze parti" di accedere al vostro account e sarà fornito anche un sondaggio "malevolo" da compilare.



## 8 Conclusioni

Con la diffusione dell'e-commerce si sono diffuse truffe sempre più insidiose che colpiscono principalmente gli acquirenti.

Si passa dalla vendita di prodotti da siti civetta dove al ricevimento del pagamento non viene inviata la merce, o viene solamente simulata la spedizione alla realizzazione di siti clonati con la finalità di rubare informazioni quali il codice della carta di credito.

La normativa italiana prevede che tutti i siti di commercio elettronico riportino nella *home page* la partita IVA e la denominazione dell'azienda. I siti più importanti di e-commerce hanno un certificato digitale che consente di verificare l'autenticità del sito visitato.

Il principale problema dal punto di vista delle aziende è la gestione degli ordini simulati, dove vengono indicate generalità false o non corrette per l'invio dei prodotti. Per ridurre il problema molte aziende accettano solamente pagamenti anticipati. Oggi giorno possiamo definire questo periodo storico come "era delle truffe on-line", dove invece del famosissimo pacco napoletano si viene frodati nel mondo telematico, è recente infatti, la notizia che il numero delle denunce alla polizia postale per reati telematici è salito a circa 3mila, il 30% in più rispetto agli anni scorsi.

## 9 Sitografia

<http://it.wikipedia.org/>

<http://www.truffeonline.net/>

<http://www.ilcorrieredellasicurezza.it/>

<http://www.sonosicuro.it/Cms/sono-sicuro/L%27e-commerce-intelligente/7/15>