Accesso sicuro ai siti web: alcune regole per evitare le frodi

*dott. ing. Alberto Rosotti**

Introduzione

Tramite i siti web si compiono un gran numero di operazioni, come prenotare voli aerei, consultare il conto corrente, acquistare e vendere oggetti o svolgere pratiche burocratiche. Questo articolo è una sintetica guida per il riconoscimento dei siti web sicuri, ed un prontuario di regole utile per difendersi dalle truffe online.

Riconoscere un sito sicuro

Con l'avvento delle reti dati a banda larga, è oggi possibile accedere ad informazioni personali e sensibili via Internet. Se da un lato questa pratica agevola la vita di tanti individui, dall'altro li espone a notevoli rischi. Solamente alcuni siti web possono infatti dirsi sicuri, offrendo la garanzia che i dati inseriti vengano trattati solo per le finalità dichiarate e visualizzati unicamente da personale autorizzato. La legge 196/2003 offre tutele e garanzie a chi compie le operazioni online ma è comunque consigliabile conoscere alcuni elementi di base per proteggersi dalle trappole che copiosamente si incontrano navigando in Internet.

Possiamo affermare che un sito web è sicuro quando:

- 1. fornisce certezze sulla sua identità;
- 2. possiede un certificato digitale che:
- a. garantisca la riservatezza della comunicazione;
- b. accerti l'identità dell'utente.

Fornire la certezza sull'identità di un sito significa indicare il proprietario del sito stesso ed il suo

amministratore. Quindi, la prima cosa da fare per verificare se un sito è sicuro è accertarsi che l'indirizzo, detto in gergo URL (Uniforme Resource Locator), sia immediatamente riconducibile all'azienda che ne è proprietaria. Attenzione quindi alle somiglianze dei nomi: in alcuni casi gli hacker sfruttano gli errori di digitazione o le assonanze nei nomi per creare siti web simili a quelli ufficiali, e truffare gli utenti. Il miglior strumento per verificare l'identità del proprietario di un sito web nel dominio .it è disponibile su Internet all'indirizzo http://www.nic.it (Network Information Center per l'Italia).

I certificati digitali

Dopo aver verificato l'identità del proprietario del sito, il secondo passo è quello di verificare se dispone di un certificato digitale. Un certificato digitale è l'equivalente elettronico di un documento, quale per esempio la carta d'identità. Viene fornito da un ente terzo, imparziale e fidato, al proprietario di un sito e consente l'identificazione univoca dell'amministratore o del sito stesso. I certificati digitali sono quindi strumenti di identificazione elettronica ed assolvono a tre fondamentali funzioni: garantire l'identità del sito con cui si sta dialogando, garantire la privacy tramite criptazione dei dati e delle comunicazioni e garantire l'integrità dei dati. Chiamati anche Digital ID, i certificati possono essere emessi solo da autorità di certificazione ufficiali, come il CNIPA (Comitato Nazionale per l'Informatica nella Pubblica Amministrazione), enti che prima di fornire il certificato espletano rigorose procedure di autenticazione, controllo e sicurezza. Il certificato permette di creare un tunnel all'interno del quale viaggiano i dati tra i computer che navigano in Internet: ciò costituisce una garanzia per l'utente, la cui operazione web (acquisto con carta di credito, disposizione per bonifico, prenotazione viaggio aereo, ecc...) sarà protetta.

A ciò si aggiunge il tema dell'integrità dei dati, poiché il certificato può garantire che le informazioni inviate arrivino al destinatario senza aver subito modifiche. Qualsiasi modifica alla comunicazione, eventualmente apportata da un pirata informatico, farà immediatamente terminare la comunicazione e genererà un messaggio di allerta. Nella pratica, una volta entrati in un'area protetta di un sito web, cliccando due volte sul lucchetto, presente nella "status bar" del desktop, comparirà una finestra con le caratteristiche di sicurezza del certificato digitale; qui si potranno controllare il nominativo del certificato e la data di scadenza, vedi figura 1. Analogamente ci potremmo accorgere se la pagina web non ha un certificato digitale (lucchetto aperto): in questo caso meglio non fidarsi, in quanto tutti i dati che invieremo su Internet viaggeranno in chiaro.

L'area protetta di un sito web: da Http:// a Https://

All ‘ingresso di una pagina sicura o di un’area riservata di un sito web, solitamente appare un “Avviso di protezione”, indicante che da quel momento in poi l’utente si trova in una zona difesa dagli attacchi esterni. Le aree protette sono utilizzabili tramite il protocollo https:// che costituisce l’evoluzione sicura dal noto http://, dove la “s” sta per “Secure Socket Layer”. Molti siti possiedono un’area generica non protetta, come la home page di benvenuto, ed una zona riservata e protetta, per l’operatività dei clienti. Spesso la prima pagina di un’area protetta contiene i campi per effettuare il login, ovvero l’inserimento del nome dell’utente e della password, affinché il sito web possa identificare il cliente. Un sito web sicuro deve essere protetto fin già nella pagina riservata al login. In altre parole è sicuro quel sito in cui appare il “lucchetto chiuso” già al momento dell’inserimento delle credenziali: ciò garantisce che l’username e la password viaggino criptate sul canale, affinché nessun pirata possa impossessarsene.

OTP (One Time Password)

Un altro dispositivo che offre una sicurezza per le transazioni su Internet è l’OTP (One Time Password). L’OTP è uno strumento poco costoso, sicuro e di semplice utilizzo, delle dimensioni di un portachiavi, che alla pressione di un pulsante visualizza un numero di 6 o 8 cifre, da utilizzare come password di secondo livello, vedi figura 2. La password di secondo livello è molto utilizzata nell’home bancking per la conferma delle disposizioni bancarie, come bonifici o giroconti. La sequenza di cifre generata dall’OTP deriva da una serie di grandezze segrete, scritte nell’hardware dell’OTP stesso, ed è in funzione di un orario fornito da un “real time clock” interno al dispositivo.

Come scegliere una password sicura

La scelta di una password è un tema importante per accedere ai servizi web protetti. La password deve essere un codice difficilmente intercettabile, affinché nessuno possa scoprirlo e utilizzarlo per scopi fraudolenti. Molti utenti hanno la tentazione di scegliere per comodità qualcosa di facile e breve; invece è indispensabile attuare un compromesso tra l’importanza dei dati da proteggere e lo sforzo nella ricerca e memorizzazione. Purtroppo sono tanti i numeri che un adulto deve sforzarsi di ricordare (telefoni, indirizzi, pin code, ecc ...), per cui a volte si assiste alla disdicevole operazione di veder scritte le password sotto la tastiera o su un fogliettino appiccicano nel monitor. Nel seguito sono elencate alcune semplici linee guida che tutti gli utenti dovrebbero osservare per scegliere una password, come definito ai sensi del D.Lgs 196/2003 e successive modificazioni ed integrazioni:

- scegliere una password di lunghezza pari ad 8 o più caratteri; evitare parole comuni di senso compiuto: esistono numerosi programmi software gratuiti che, basandosi su dizionari internazionali, tentano di forzare i sistemi utilizzando i termini comuni; tale tecnica è denominata “brute force”;
- inserire nelle password numeri, lettere e simboli. Ad esempio, utilizzare il sostantivo “mare” come password è inadeguato; possiamo creare una password sicura inserendo prima, dopo o all’interno della medesima una serie di numeri. In tal modo “12mare?!” è estremamente più sicura della precedente, per lunghezza e complessità.;
- evitare i nomi dei figli, del coniuge o di un animale domestico, le date di nascita dei parenti stretti e tutte quelle parole che derivano da informazioni personali;
- non usare una password che contenga il nome utente o l’indirizzo e-mail;
- non utilizzare la stessa password per servizi diversi. Sebbene sia un escamotage per non dover ricordare decine di password diverse, alla fine la probabilità che venga identificata aumenta enormemente. Usando la medesima password per il pc, per la posta elettronica, per i giochi, gli account dell’ufficio ed i database aziendali, c’è un’alta probabilità che questa venga violata, per una banale vulnerabilità di uno di questi software. E’ possibile verificare, seppur in maniera empirica, la sicurezza di una password utilizzando un qualsiasi motore di ricerca (es. Google): se digitando la password nel campo di ricerca il motore restituisce meno di 10 risultati, allora la password è sufficiente sconosciuta, quindi sicura. Sempre su Internet, esistono programmi che gratuitamente generano password della complessità e lunghezza desiderate. I consigli sopra esposti rendono sicura la scelta della password ma la sicurezza deve proseguire con una corretta conservazione.

A tal fine può essere utile, ad in alcuni casi è obbligatorio, seguire questi criteri:

- non digitare la password in presenza di estranei, che magari si trovano alle vostre spalle mentre la componete sulla tastiera. Un occhio attento, o peggio una videocamera, può seguire i movimenti delle nostre mani; non trascrivere la password su un foglio di carta, agenda, o in altro luogo. La password va tenuta a mente, o al limite custodita in un luogo protetto in caso la scordassimo; n non archiviarla in un file di un computer, ne sul telefonino;
- non memorizzare la password nei tasti funzione di un computer;
- modificare la password frequentemente: l’uso abitudinario della solita password è un comportamento rischioso. Il D.Lgs 196/2003 obbliga a cambiare la password di accesso a sistemi che gestiscono dati personali ogni 6 mesi, ed il tempo è dimezzato se la password consente l’accesso a dati sensibili. Attenzione: i siti che permettono transazioni on line non chiedono mai attraverso e-mail o contatti telefonici le credenziali di accesso ai propri clienti. Qualora si ricevessero richieste di questo tipo, segnalatelo immediatamente alle autorità preposte ed al gestore del sito stesso, in quanto si tratta probabilmente di un attacco informatico.

Il social engineering

Nel campo della sicurezza informatica il social engineering è lo studio del comportamento individuale e l'insieme delle strategie psicologiche usate dagli aggressori al fine di ottenere dall'utente dati personali o sensibili oppure di indurlo a compiere una serie di azioni pericolose, superando le sue barriere di sicurezza. Conoscere le tecniche di social engineering è il modo migliore per non diventarne noi stessi vittime. I pirati informatici agiscono camuffando la propria identità, ingannando per infondere fiducia nella vittima, sfruttando la sua disponibilità, la buona fede ed anche un pizzico di umana curiosità. Nella maggioranza dei casi sono abilissimi nei rapporti umani, risultano affascinanti, educati e simpatici. Per convesso, la maggior parte degli utenti pensa di essere sufficientemente scaltro da non cadere in trappole di questo genere. L'hacker che sferra l'attacco è conscio di questa ingenuità comune e riesce a far sembrare tanto ragionevole la sua richiesta da non sollevare il minimo sospetto. La rassegna delle astuzie escogitate da chi ordisce raggiri telematici è piuttosto variegata. Soventemente l'aggressore si spaccia per un amico, per un collega, per la segretaria di un amministratore, per il funzionario di una ditta o un ente pubblico autorevole (per esempio la Polizia municipale, la vostra banca ...), al fine di indurvi a rivelare segreti o informazioni confidenziali. Se cediamo a queste tecniche l'hacker potrà agire per nostro conto, fin quando non verrà scoperto o fintantoché non cambieremo la credenziali di accesso; anche per questo le password hanno per legge una scadenza.

Il phishing

Il phishing è una delle più comuni tecniche di social engeneering; il suo nome deriva dal verbo inglese 'to fish' (pescare) e consiste in un raggiro ideato per carpire le informazioni personali e i dati sensibili direttamente dagli utenti. Come i pesci in mare, anche gli utenti devono prestare molta attenzione alle esche che vengono preparate dai phisher. La principale vittima di questa pesca informatica, che si presenta solitamente sotto forma di e-mail, è chi usufruisce dei servizi di home banking ed e-business. Apparentemente inviate da una fonte nota ed autorevole, queste e-mail avvertono di un imprecisato problema tecnico, di un disguido o di un altro valido problema per risolvere il quale è necessario collegarsi al sito dell'ente stesso ed effettuare un nuovo login, cioè fornire username e password . Se l'utente abbocca, il pirata potrà agire nella rete per suo conto. Spesso il pirata informatico costruisce una pagina web simile a quella del sito affidabile che usa come esca; cliccando sul link riportato nella e-mail, l'utente viene apparentemente trasportato in un sito sicuro, mentre si trova nella pagina costruita da phisher.

I dati sensibili che l'utente immette vengono così inviati al pirata informatico, che potrà così accedere ai servizi dell'utente, per esempio dando disposizioni bancarie o acquistando oggetti per suo conto. Inoltre i siti di phishing nascono e muoiono molto velocemente, giusto il tempo di trarre in inganno qualche utente per poi sparire senza lasciare tracce. Per evitare il fishing è

necessario essere scrupolosi e ricordare i seguenti consigli: n gli istituti bancari e le aziende di e-businness non richiedono mai informazioni personali tramite e-mail; n non utilizzare il collegamento contenuto nelle e-mail sospette. Posizionando il mouse sul link, senza cliccare, potremmo osservare sulla barra di navigazione il nome dell'indirizzo verso il quale ci condurrebbe il collegamento. Leggendo attentamente quell'indirizzo potremmo verificare se corrisponde a quello del sito ufficiale, o se si differenzia da esso anche solamente per l'aggiunta o l'assenza di una lettera. Per raggiungere un sito web digitiamo sempre l'indirizzo a noi noto: guidiamo noi, non facciamoci guidare dai pirati; n esaminare regolarmente i rendiconti bancari e quelli della carta di credito, in modo da accorgersi prontamente di un qualsiasi movimento sospetto. Nonostante tutti gli accorgimenti, il fenomeno del phishing è in continuo aumento.

** Tesoriere dell'Ordine degli Ingegneri di Pesaro e Urbino*