SwissBanking

Settembre 2009

Secure e-Banking

1 Sicurezza nell'e-banking

L'e-banking si è affermato come canale di comunicazione valido e conveniente nei rapporti tra la clientela privata e commerciale e la propria banca di riferimento. Lo strumento presenta infatti vantaggi per entrambe le parti: per il cliente non è più necessario recarsi in banca per effettuare un bonifico o visionare lo stato del proprio conto. Queste prestazioni di base sono infatti accessibili in rete 24 ore su 24, indipendentemente dagli orari di apertura degli sportelli. Le banche, dal canto loro, dispongono di uno strumento di comunicazione verso il cliente accessibile in qualsiasi momento. L'e-banking può dunque migliorare qualitativamente la relazione instaurata dal cliente con la propria banca di riferimento.

Accanto agli indubbi vantaggi, l'utilizzo di Internet comporta tuttavia anche una serie di rischi legati alla sicurezza, ad esempio quello che i dati possano essere letti, modificati o cancellati in sede di trasferimento oppure che persone non autorizzate possano fraudolentemente accedere a informazioni confidenziali.

Con questo opuscolo informativo desideriamo attirare l'attenzione di voi clienti e-banking sui rischi legati alla sicurezza e mostrarvi quali provvedimenti adottare per cautelarvi contro le principali minacce e i rischi insiti nell'utilizzo di Internet.

La sicurezza nell'e-banking è garantita a condizione di conoscere sufficientemente le minacce che gravitano sull'Internet e adottando, assieme alla propria banca, i correttivi per cautelarsi contro l'aumento della criminalità in rete.

Per proteggersi da eventuali manipolazioni nell'e-banking è indispensabile adottare un comportamento consapevolmente orientato alla sicurezza e monitorare regolarmente i propri movimenti sul conto. Se si sospetta di essere vittima di criminali informatici, la prima cosa da fare è bloccare l'accesso Internet al conto bancario e informare immediatamente la propria banca di qualsiasi movimento di conto sospetto.

2 Rischi e minacce in Internet

I rischi e le minacce che gravitano su Internet mutano costantemente e in modo spesso repentino. Tra i principali rischi telematici citiamo virus, vermi, cavalli di Troia, «phishing», «pharming» e infezioni drive-by. Di seguito illustriamo in maggiore dettaglio il significato di questi termini, spiegando quali misure adottare per tutelarvi.

2.1 Virus

I virus hanno le stesse caratteristiche di quelli che minacciano la nostra salute, ossia si diffondono autonomamente e possono provocare notevoli danni. Si va dal virus più innocuo, che modifica i contenuti dei file, a quello che cancella l'intero contenuto del disco fisso. I virus si trasmettono al disco fisso del PC per e-mail o attraverso file corrotti scaricati da Internet. Se attivati, si propagano molto velocemente con l'ausilio della posta elettronica o l'utilizzo della rete.

2.2 Vermi

I vermi causano più o meno gli stessi danni dei virus, ma sono programmi autonomi e quindi non necessitano di un programma ospite per attivarsi. I vermi sfruttano eventuali lacune di sicurezza o errori di configurazione nei sistemi operativi o nelle applicazioni (e-mail, Internet) per propagarsi autonomamente da un computer all'altro.

2.3 Cavalli di Troia

I cosiddetti «cavalli di Troia» sono programmi, scaricati sovente da Internet, che introducendosi in sordina nel computer causano danni informatici senza che possiate rendervene conto. L'obiettivo dei «cavalli di Troia» è di solito risalire a informazioni riservate, come le password, per poi inviarle ai loro proprietari o utilizzarle per manipolare direttamente le vostre operazioni in rete. Il «cavallo di Troia» permette al suo proprietario di accedere a processori di terzi e di assumere il controllo a distanza del vostro computer. L'utente scambia di norma il «cavallo di Troia» per un'applicazione o un file di comprovata utilità.

2.4 Phishing

Ricorrendo al «phishing», termine nato dalla contrazione delle due parole inglesi «password» e «fishing», persone con intenti disonesti vi chiedono di aggiornare o reimpostare i vostri dati confidenziali di accesso all'e-banking sul sito web del vostro istituto. La richiesta può avvenire per e-mail, ma anche mediante una pagina web contraffatta. L'obiettivo è carpire i vostri dati confidenziali, come la password di accesso all'e-banking o lo stato del vostro conto.

2.5 Infezione drive-by

Con l'«infezione drive-by» si trasmettono al computer software dannosi, chiamati «malware», semplicemente visitando un particolare sito. Si tratta di siti che, pur presentando spesso offerte serie, sono stati contaminati in modo da consentire la diffusione di programmi nefasti. Persone con intenti criminali introducono furtivamente codici dannosi sul sito e lo intaccano; la semplice navigazione sullo stesso basta quindi a contaminare il processore.

2.6 Pharming

Il «pharming» è un metodo fraudolento mediante il quale il vostro collegamento Internet viene dirottato su un sito web manipolato. In pratica, voi inserite l'indirizzo web corretto nel browser, ma accedete a una pagina contraffatta.

3 Provvedimenti a tutela del vostro e-banking

Aprite solo le e-mail di persone o aziende che conoscete e non aprite in nessun caso gli allegati di e-mail di cui non conoscete il mittente. In caso di dubbi prendete contatto con il mittente. Equipaggiate il vostro PC con un firewall personale e un software antivirus aggiornato. A tal proposito è importante aggiornare continuamente il software antivirus, scaricando e installando immediatamente gli aggiornamenti disponibili dal sito del vostro fornitore oppure utilizzando la modalità di aggiornamento automatica.

Verificate inoltre di aver installato un sistema operativo recente e l'ultima versione del browser e dei relativi plug-in. Installate anche regolarmente gli ultimi aggiornamenti di sicurezza delle vostre applicazioni; altrimenti potrebbero verificarsi punti deboli che, se noti, verrebbero facilmente sfruttati dai truffatori per attaccare il vostro PC.

3.1 Non eseguite operazioni e-banking con un indirizzo Internet non bancario

Inserite i vostri dati di accesso all'e-banking soltanto se siete sicuri di trovarvi effettivamente sulla pagina Internet protetta e autorizzata della vostra banca e se state utilizzando un collegamento criptato. Per riconoscerlo verificate che nell'URL del collegamento sia stata aggiunta una «s» (che sta per «secure», in italiano «sicuro») all'http. L'«https» attesta che per il sito in questione è stato adottato un certificato di sicurezza (ad es. https://www.sba.ch). L'autenticità del certificato di sicurezza può essere verificata come segue: doppio clic sul simbolo del lucchetto chiuso che si trova sulla barra di stato in fondo alla finestra del browser. Nella finestra di dialogo del certificato che si aprirà a questo punto dovrebbe apparire il nome della vostra banca. La maggior parte delle banche utilizza inoltre i certificati Extended Validation SSL, riconoscibili per il fatto che parte della barra dell'indirizzo URL con il nome della banca è visualizzata su uno sfondo verde. Cliccando sulla barra verde si apre una finestra di dialogo dalla quale si evince il nome dell'istituto bancario sul certificato e l'ente di certificazione. In questo caso potete partire dal presupposto di operare su un sito web affidabile. Purtroppo non tutti i browser sono già in grado di supportare l'Extended Validation SSL.

Se fate acquisti in rete («online shopping») vi raccomandiamo di non inserire i vostri dati di accesso personali né sulle pagine dell'e-shopping né su quelle di eventuali servizi per bonifici online. Non divulgate mai i vostri dati di accesso segreti, né su un sito web che non sia quello della vostra banca, né a terzi in genere. Se trasmettete i vostri dati di accesso e-banking ad altre aziende violate infatti l'obbligo di diligenza sancito nel contratto e-banking stipulato con la vostra banca.

3.2 Proteggete le informazioni sensibili

Proteggete i vostri dati di accesso all'e-banking da accessi e utilizzi indebiti. Non memorizzate le informazioni sensibili (password, dati di accesso all'e-banking, numeri di carte di credito ecc.) sul vostro computer, in quanto, se non lo utilizzate solo voi (ad es. sul posto di lavoro), i dati potrebbero essere accessibili ad altre persone.

Esistono anche particolari programmi di spionaggio che, se hanno intaccato il vostro computer, sono in grado di risalire alle informazioni sensibili e spedirle, ad esempio per e-mail. Se, per aumentare la sicurezza del vostro PC, vi servite di applicazioni supplementari, ad esempio di un lettore di carte chip con tastiera per l'inserimento del PIN, vi consigliamo di introdurre i relativi dati sensibili previsti solo se l'apparecchio in questione lo richiede espressamente. Soprattutto, non salvate mai da nessuna parte la vostra password.

La vostra banca non vi contatterà mai, né per e-mail né telefonicamente, per richiedere i vostri dati di accesso segreti. Non rispondete in nessun caso ad e-mail di questo tenore né seguite le annesse istruzioni, anche se minacciano conseguenze spiacevoli, ad esempio il blocco del vostro conto. In una simile eventualità non esitate ad informare la vostra banca.

Nel caso contrario, ossia se siete voi a contattare direttamente la vostra banca nell'ambito del «phonebanking», la banca potrebbe richiedervi i vostri dati di accesso segreti per identificarvi. Prima di assecondare l'eventuale richiesta, assicuratevi in ogni caso di aver chiamato il numero giusto e di essere sottoposti a una procedura conforme a quella che vi è stata illustrata dall'istituto.

Assicuratevi di inserire i vostri dati di accesso personali sempre e soltanto sull'effettivo sito web della vostra banca. Prestate inoltre attenzione ad eventuali modifiche nell'immagine che accompagna la pagina di accesso all'e-banking della vostra banca. Se attivate spesso il vostro sito e-banking non vi sfuggirà il seppur minimo cambiamento, anche se si tratta solo di lievi modifiche del logo o delle diciture.

3.3 Scegliete una password sicura

Utilizzate una password valida e sicura per le vostre operazioni e-banking. Essa dovrà contenere almeno otto caratteri, con una combinazione di lettere maiuscole, minuscole e numeri. Non utilizzate mai il vostro nome né quello di vostri conoscenti, né tantomeno la vostra o la loro data di nascita. Modificate regolarmente la vostra password, soprattutto se sospettate che qualcuno possa esservi risalito. In Internet, e probabilmente anche sul sito della vostra banca, troverete esempi di come scegliere una password valida e sicura.

4 Provvedimenti di carattere generale

Accedete all'e-banking solo da un PC utilizzato da voi. Se così non fosse, ad esempio se vi accedete da un Internetcafé, non potrete mai sapere con certezza in che misura l'accesso è protetto da software di sicurezza di sicurezza efficaci e quali programmi usa il computer. In effetti, anche la tastiera può essere contraffatta. Dunque, non aspettatevi mai sicurezza in questi luoghi e non utilizzate simili computer per le vostre operazioni e-banking.

Nell'accingervi a eseguire un'operazione di e-banking controllate che non sia aperta nessun'altra finestra del browser (nemmeno i «tab»), né il programma di posta elettronica.

Terminate sempre la vostra sessione e-banking con la funzione prevista allo scopo, ossia «Disattiva», «Logout» o «Chiudi» e cancellate immediatamente i file temporanei Internet presenti nel vostro browser nonché eventuali «cookie» (le istruzioni su come procedere dovrebbero trovarsi sul sito web della vostra banca).

Link utili:

- http://www.swissbanking.org/it/home/dossier-bankkunden.htm > Dossiers: Informazioni per clienti bancari

- Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI
  http://www.melani.admin.ch/themen/00103/index.html?lang=it

- Bundesamt für Sicherheit in der Informationstechnik
  http://www.bsi-fuer-buerger.de/
  (in tedesco)

Quest'opuscolo, disponibile anche in tedesco, francese e inglese, può essere ordinato all'Associazione svizzera dei banchieri su http://www.swissbanking.org/it/home/shop.htm

Su http://ww.swissbanking.org/it/home/dossier-bankkunden.htm è inoltre possibile scaricare l'opuscolo in formato PDF.

Associazione Svizzera dei Banchieri
Aeschenplatz 7
Casella postale 4182
CH-4002 Basilea
T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org