E-banking, miniguida di sicurezza

Le transazioni bancarie effettuate via Internet, comodamente da casa o dall'ufficio, sono un grande risparmio di tempo e contribuiscono a ridurre gli spostamenti, con ricadute positive sul traffico e quindi sull'inquinamento. Tuttavia molti utenti temono che i criminali informatici possano derubarli o spiarli via Internet e sono quindi riluttanti a usare l'e-banking. Per tutti costoro, questo vedemecum proposto da Paolo Attivissimo può essere molto utile.

In realtà la situazione svizzera della sicurezza su questo fronte è piuttosto serena, specialmente se confrontata con quella degli altri paesi. Gli istituti di credito hanno adottato soluzioni tecniche valide e procedure efficaci per la risoluzione di eventuali sottrazioni sospette. I criminali sono pigri e preferiscono bersagli meno difficili, come le carte di credito e di debito, il cui uso corretto su Internet esula dall'ambito di questa miniguida. Ecco qualche regola semplice per l'uso sicuro delle transazioni bancarie via computer.

1. Se possibile, riservate un computer solo per l'e-banking.

Può sembrare una raccomandazione eccessiva, ma un computer dedicato, sul quale non si fa nulla a parte comunicare con la banca (niente e-mail, niente giochi, niente visite ad altri siti), è la migliore difesa in assoluto: mette al riparo da quasi tutti i problemi. Oggi un computer portatile usabile per l'e-banking costa meno di trecento franchi ed è facile metterlo al sicuro anche fisicamente (chiudendolo in cassaforte o mettendolo sotto chiave, per esempio).

2. Non usate mai un computer altrui.

I computer degli alberghi e degli Internet café possono conservare tracce dei vostri codici di accesso all'e-banking o delle vostre transazioni.

3. Evitate l'uso del Wifi.

L'accesso a Internet senza fili tramite Wifi è comodo ma è facilmente intercettabile e dirottabile verso siti-trappola. È più sicuro usare il cavo tradizionale. Se è necessario fare e-banking in viaggio o in luoghi pubblici, potete connettere il vostro computer a Internet attraverso il telefonino o le apposite chiavette USB cellulari: in questo caso la comunicazione è più difficile da intercettare.

4. Non usate i tablet (iPad e simili) o gli smartphone.

La loro sicurezza è alta solo se non vi installate altre applicazioni (che possono rubare dati) e se vi connettete usando la rete cellulare invece del Wifi; inoltre sono facili da smarrire o rubare insieme al loro contenuto di codici d'accesso, che può essere particolarmente prezioso per il ladro se il vostro istituto finanziario manda sul cellulare dei codici di autenticazione temporanei tramite SMS (i cosiddetti "mTAN").

5. Quando avete finito, chiudete sempre la sessione di e-banking; meglio ancora, spegnete il computer.

Una delle tecniche più usate dai criminali informatici è infettare il computer della vittima in modo da poterne prendere il controllo a distanza e poi aspettare che da quel computer vengano effettuate transazioni bancarie; dopo che l'utente ha finito senza chiudere la sessione, il criminale prende le redini della comunicazione con la banca e ha già le password e i codici d'accesso perché li ha digitati per lui la vittima.

6. Respingete qualunque mail, messaggio elettronico o telefonata che dice di provenire dalla vostra banca e vi chiede di verificare i codici di e-banking.

Si tratta di truffe pensate per sottrarvi con l'inganno i codici d'accesso. Nessuna banca seria manderà mai richieste di questo genere. Ricordate che il mittente di una mail è facilmente falsificabile.

7. Respingete qualunque programma o "app", specialmente se per e-banking, che non sia di fonte assolutamente certa.

Spesso questi programmi sono veri e propri cavalli di Troia. Se non vi vengono forniti direttamente dalla vostra banca o da un produttore affidabile, non installateli. Evitate i programmi piratati.

8. Fate attenzione ai siti-clone.

È molto facile creare siti Internet che somigliano in tutto e per tutto a quelli veri delle banche e poi usare espedienti psicologici (mail o SMS di falsa allerta di sicurezza) per indurre le vittime a visitarli. Se immettete i vostri codici in questi siti, li regalate al truffatore. Per difendersi è utile digitare a mano il nome del sito della banca oppure memorizzarlo nei "preferiti". Molti programmi di navigazione (browser) oggi hanno un'indicazione visiva (bandierina, semaforo o sfondo colorato) che avvisano sull'affidabilità del sito che si sta visitando e segnalano i siti-clone.

9. Controllate che l'indirizzo visualizzato durante la sessione di e-banking inizi sempre con "https", non "http".

La S indica che la comunicazione è cifrata e quindi maggiormente protetta. Non fate transazioni economiche se non c'è l'indicazione "https".

10. Usate password robuste e custoditele bene.

Evitate date di nascita, nomi di animali domestici o figli o altre informazioni facilmente reperibili da terzi. Usate password composte da lettere e numeri, che non siano parole di senso compiuto e siano lunghe almeno otto caratteri. Non datele a nessuno e non scrivetele da nessuna parte senza cifrarle, e non usate per altri siti la password dell'e-banking. Trucco per creare password robuste ma facili da ricordare: prendere le iniziali di una frase ("La mia gatta Pallina ha 13 anni" diventa "LmgPh13a").

11. Aggiornate sempre prontamente il sistema operativo, l'antivirus e il programma di navigazione del computer usando solo aggiornamenti autentici.

Evitate di scaricare antivirus e aggiornamenti da siti mai sentiti nominare: se non sapete come procedere, chiedete a un amico o collega esperto e ricordate che i falsi antivirus sono oggi una delle esche maggiormente usate dai criminali della Rete.

12. Se non avete agito con grave negligenza, le banche di norma compensano eventuali danni subiti.

Informatevi sulle procedure offerte dal vostro istituto in caso di contestazione di addebiti anomali o transazioni sospette effettuate tramite e-banking.