Come proteggere il tuo conto corrente online

- **Come ti difende la banca Scegliere un conto**
- **Proteggerlo anche su mobile**
- **Le firme sui tablet: le garanzie da chiedere**

Nulla a questo mondo può essere considerato sicuro al 100%. Soprattutto quando si parla di movimentare del denaro. Negli ultimi anni numerosi istituti bancari si sono prodigati nell'offrire ai propri clienti conti correnti online con bassissimi - o nulli - costi di gestione, accessibili 24 ore su 24 dal computer di casa e con la possibilità di disporre operazioni in qualunque momento della giornata, con pochi click del mouse.

L'estrema praticità di queste soluzioni ha messo a dura prova i protocolli di sicurezza delle banche, indispensabili a garantire la sicurezza dei conti contro intrusioni non autorizzate e attacchi informatici.

Ma quanto effettivamente è sicuro operare con i sistemi di home banking? Quali sicurezze sono in grado di fornire le banche e quali accorgimenti invece devono applicare gli utenti per autotutelarsi contro le frodi? Con questa guida vogliamo offrire uno spaccato a 360° sul funzionamento dei più diffusi sistemi di home banking, approfondendo le tecnologie che ne regolano la sicurezza e i rischi legati alle attività del cybercrimine.

Tenendo ben presente che niente può essere considerato pienamente sicuro, nemmeno recarsi di persona alla filiale della propria banca.

Virus bancari: cosa sono e come possono svuotare il tuo conto

Il principale timore di chi opera sui sistemi home banking è quello di ritrovarsi dall'oggi al domani il conto corrente svuotato. Un rischio tutt'altro che remoto, reso concreto dalle tecnologie al servizio dei pirati informatici create per aggirare i sistemi di sicurezza e le precauzioni messe in campo dalle banche.

Tra i principali artefici delle frodi bancarie figurano i trojan informatici.

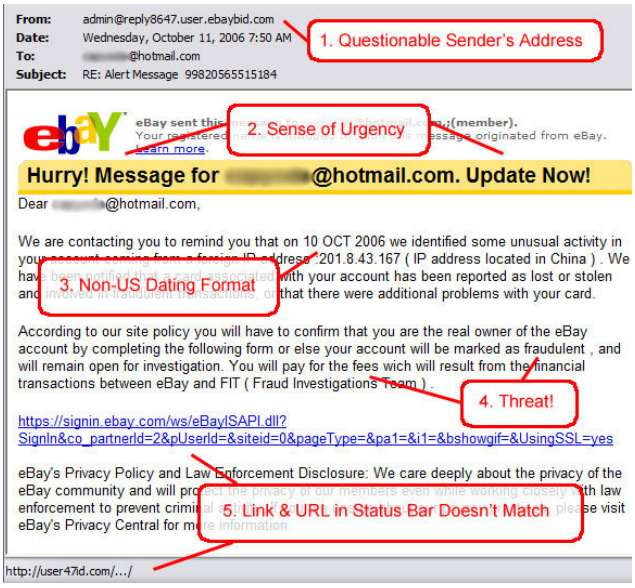
Come dice la parola stessa, si tratta di programmi dal funzionamento simile a quello del celebre Cavallo di Troia: un software penetra nel nostro computer, si installa, raccoglie una serie di dati (solitamente user, password, numeri di conto e di carta) e li trasmette a un altro computer. Dal quale probabilmente qualcuno ne farà usi alquanto spiacevoli per le nostre finanze.

Simili programmi circolano sulla Rete da ormai molti anni ma con il proliferare delle banche online i loro creatori si sono progressivamente orientati sulle nuove specie dei cosiddetti trojan bancari. **Il capostipite di questa famiglia di programmi è stato battezzato Zeus** e rappresenta un rischio concreto per quanti operano online con il proprio conto corrente. Il trojan in questione si comporta come un "man in the browser", installandosi nel software di navigazione dell'utente e monitorandone l'uso.

All'occorrenza, Zeus arriva a interferire con le pagine visualizzate intermediandole, modificandone intere porzioni e presentandone di nuove agli occhi del navigatore "infettato". In caso di connessione al sito della propria banca, oltre alle canoniche credenziali di accesso il trojan modifica il campo di login aggiungendo tra i codici da inserire anche le password dispositive. In altre parole, l'inserimento simultaneo di tutte le coordinate di accesso. A questo punto Zeus memorizza tutti i dati e li trasmette al suo creatore in modo da consentirgli il pieno controllo del conto della vittima. Ogni operazione a quel punto risulterà effettuata dall'indirizzo IP dell'ignaro cliente, durante il suo login, rendendo estremamente difficile dimostrare alle autorità l'estraneità dell'attività svolta durante la sessione.

La pericolosità di questo trojan è talmente alta da riuscire ad aggirare persino l'efficacia dei dispositivi otp, agendo sulle vulnerabilità dell'utente per penetrare i sistemi di sicurezza messi in campo dalle banche.

Anche in questo caso una sana azione di prevenzione attraverso antivirus aggiornati può contribuire efficacemente a ridurre il rischio di contagio da trojan e virus.



Truffe a larga diffusione: il phishing

Ogni giorno milioni di utenti ricevono nella propria casella mail comunicazioni a firma di una banca, attraverso le quali **si viene invitati a confermare o aggiornare i codici di accesso al proprio conto corrente.**

Si tratta ovviamente di truffe in piena regola, in quanto nessuna banca chiede alla clientela di confermare via mail le credenziali di accesso o qualsiasi dato personale. Il funzionamento della frode è semplice: i criminali informatici realizzano una serie di comunicazioni-tipo con la grafica degli istituti bancari più diffusi. Le comunicazioni, generalmente dal tono perentorio e pressante, intimano ai clienti di cliccare su un link contenuto nella mail stessa e quindi eseguire l'accesso al proprio conto.

Spesso e volentieri s**i tratta di indirizzi web graficamente molto simili al sito originale**, con l'inserimento nell'url di simboli di punteggiatura aggiuntivi o di domini diversi da quello istituzionale (per esempio un. org al posto di un .it), al fine di dare maggiore credibilità alla comunicazione. A questo punto l'incauto navigatore viene portato su un sito-clone in tutto e per tutto simile a quello originale, allestito con il solo scopo di rubare le credenziali di accesso al cliente per operazioni truffaldine.

Le nuove frodi: vishing e smishing

L'evoluzione delle truffe con metodo phishing ha portato negli ultimi anni all'elaborazione di nuovi metodi sempre più convincenti architettati per il medesimo fine: carpire alle ignare vittime dati di accesso bancari e coordinate delle carte di credito, al fine di intaccare le proprie finanze e sottrarre denaro.

Fra questi uno dei più rischiosi è rappresentato dal vishing, parola che deriva dalla contrazione fra il termine "VoIP" e "phishing" e che rappresenta una forma di phishing avanzato **basato sull'utilizzo di un finto call center telefonico** dove una persona molto affabile cercherà di fare di tutto per estorcere alle ignare vittime dati bancari come password e numeri di carta.

La truffa funziona secondo uno schema lineare: il malintenzionato di turno, o visher, spedisce alla vittima una finta e-mail costruita per sembrare il più possibile convincente.

Grafiche, caratteri e loghi replicano quelli della vera banca ma ad allarmare è solitamente il tono del messaggio: si parla di generici problemi con il conto corrente, addebiti di somme cospicue mai autorizzati dal cliente, presunte irregolarità a fronte delle quali si **invita la vittima a telefonare a un numero indicato come call center dell'istituto di credito**.

Queste truffe infatti mirano a "sparare nel mucchio": sistemi automatici inviano enormi quantità di messaggi dal contenuto identico a milioni di indirizzi di posta elettronica, cambiando di volta in volta la grafica e il nome della banca in questione. Per la legge dei grandi numeri, è statisticamente probabile che almeno uno dei destinatari abbia effettivamente attivato un conto presso quell'istituto di credito.

Tale numerazione corrisponde in gran parte dei casi a una linea VoIP dove a rispondere sarà un falso centralinista, generalmente molto affabile e cortese, che confermerà i timori dell'utente invitandolo quindi a collaborare per stroncare il problema sul nascere. In questo modo, facendo leva sulla paura dell'utente di vedersi ingiustamente derubato di una grossa cifra, il falso centralinista può riuscire con maggiore facilità ad estorcere dati personali e coordinate bancarie che verranno successivamente impiegate dal visher per accedere al conto e spostare a piacimento il denaro della vittima, o utilizzarlo per pagamenti.

Il "successo" di questa forma di frode si basa soprattutto sul rapporto umano che si instaura tra il truffatore e la vittima: a differenza del classico phishing il malcapitato non si vede richiedere i dati via mail da una macchina ma da una persona reale, istruita per essere il più possibile convincente e per assistere in modo preciso il cliente durante tutto il processo fraudolento. Una voce suadente, professionale e cortese può quindi riuscire a superare quel muro di diffidenza che molti utenti

alzano contro simili truffe, arrivando con la paura a demolirne le fondamenta inducendo così a comportamenti avventati come il fornire credenziali riservate a un perfetto sconosciuto senza prima averne verificato l'identità con la propria banca.

Con il proliferare del vishing e l'esplosione del mercato degli smartphone ha iniziato a prendere piede in tempi recenti anche **lo smishing, una nuova tecnica fraudolenta basata sull'invio di sms** e l'impiego sempre più articolato che i telefoni di nuova generazione hanno assunto nella vita quotidiana.

Il tutto parte con l'invio sullo smartphone della vittima di un sms malevolo o con l'installazione di una finta app in grado di simulare l'arrivo di tale sms. **Una volta letto il messaggio, si viene invitati a cliccare su un link e a visitare una pagina web** costruita ad arte dal truffatore o "smisher". A questo punto la truffa evolve secondo il solito schema: avvalendosi delle grafiche dell'istituto bancario per dare sicurezza alle vittime, si viene invitati ad effettuare un login con la semplice scusa di confermare l'account (pena minacce di blocco) o di controllare fantomatici pagamenti di cifre importanti. Da qui al furto delle credenziali, il passo è breve.

Anche in questo caso il cybercriminale punta sull'effetto sorpresa della comunicazione: la ricezione di un sms fraudolento rappresenta un sistema ancora poco conosciuto dagli utenti e conferisce a dare credibilità alla comunicazione, pensando all'improbabilità che un malintenzionato possa essere entrato in possesso del proprio numero di cellulare.

Al contrario gli smisher inviano quotidianamente milioni di comunicazioni a numeri di cellulare casuali alla ricerca di un utente reale con un conto corrente attivato presso una banca.

Cosa fanno le banche per proteggerti

Ogni banca, sotto questo profilo, ha i propri segreti. Attenti a non far trapelare nulla circa i propri sistemi di sicurezza, gli istituti bancari operano quotidianamente per rafforzare le difese e fronteggiare gli attacchi dei pirati informatici. La necessità è quanto mai evidente: una piattaforma di home banking violata mette a rischio tutti i conti correnti dei clienti, esponendo una grossa mole di denaro alla mercé degli hacker bancari.

Semplificando, gran parte delle piattaforme di **home banking ad oggi diffuse si fondano su tre livelli di sicurezza:** logica (elenco delle regole di accesso), perimetrale (la barriera fisica che disciplina l'accesso degli utenti in funzione delle regole) e applicativa (software che analizzano e monitorano in tempo reale i singoli accessi).

Tre componenti caratterizzati da sviluppo autonomo ma destinati a lavorare in sinergia per garantire all'utente le migliori condizioni di sicurezza possibili.

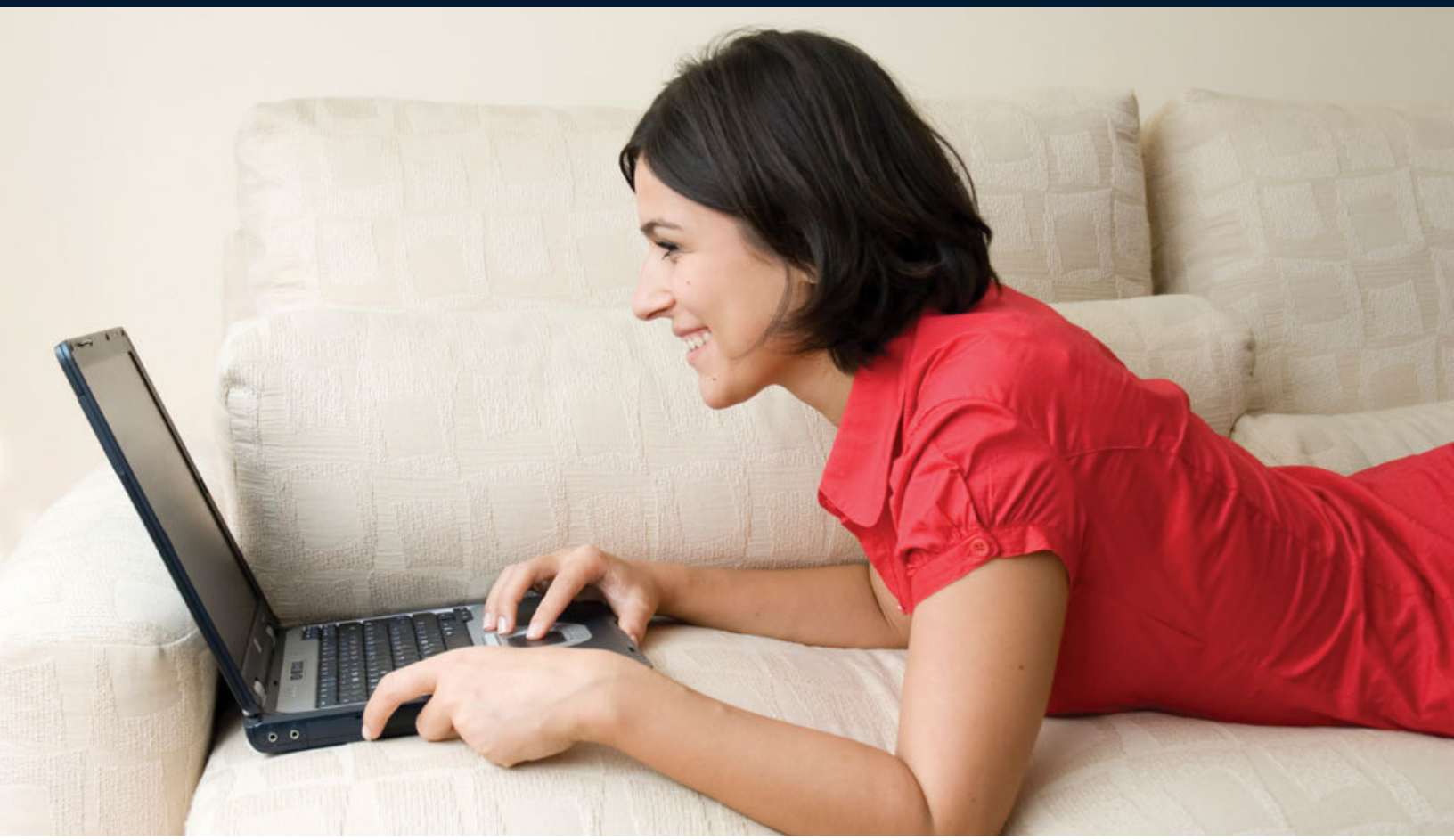
Negli ultimi anni un numero sempre maggiore di istituti bancari ha iniziato a rivolgersi ad aziende specializzate incaricandole di violare i propri sistemi di sicurezza, evidenziandone le lacune e individuando le migliori strategie di correzione. Una sana e continua competizione interna, mirata a fornire aggiornamenti di sicurezza periodici utili a ridurre il rischio di attacchi da parte del cybercrimine.

Un ulteriore "scudo" messo a disposizione dalle banche che operano online è fornito dalla cosiddetta sicurezza proattiva: una serie di accorgimenti e verifiche pensate per anticipare e stroncare sul nascere operazioni truffaldine o movimenti sospetti.

Grazie all'impiego di sistemi di monitoraggio in tempo reale molte banche sono in grado di rilevare anomalie nei comportamenti abituali dei correntisti, come ad esempio un improvviso bonifico estero dopo anni di esclusiva attività sul territorio nazionale o uno spostamento improvviso di grandi quantità di denaro. A quel punto un allarme blocca l'operazione e allerta la banca la quale, in brevissimo tempo, contatta il correntista chiedendo conferma dell'operazione stessa.

Altro aspetto della sicurezza proattiva è rappresentato dalla continua ricerca dei cosiddetti "siti bancari clone", portali ricreati da hacker a immagine e somiglianza di quelli originali e pensati per carpire i dati di conto di ignari utenti. Spesso e volentieri gli stessi indirizzi dei siti-truffa si differenziano da quelli reali soltanto per un piccolo segno di punteggiatura, per l'aggiunta di caratteri speciali o per domini diversi da quello istituzionale.

Grazie alla partnership con aziende specializzate diverse banche sono attive nello scandagliare la Rete alla ricerca di questi portali evitando così che i propri correntisti possano incappare in casi di phishing, o addirittura di assisterli nel caso in cui dovessero incautamente comunicare i propri dati su portali non autorizzati.



Home banking: le tipologie, i pro e contro di ogni scelta

Le tecnologie negli anni sono venute incontro agli istituti bancari nel fornire piattaforme di home banking sempre più curate sotto il profilo della sicurezza. La continua ricerca di strumenti capaci di fornire credenziali di accesso sempre meno rintracciabili ha facilitato di molto la protezione degli utenti, fornendo ad essi dispositivi mobili di autenticazione o l'invio di codici "usa e getta" da impiegare a ogni singolo accesso.

Accesso tramite credenziali statiche

Si tratta in questo caso del più elementare sistema di accesso, ormai scarsamente utilizzato dalle banche per via del suo irrisorio livello di sicurezza.

L'accesso al proprio conto avviene tramite l'inserimento di una username (parola di fantasia o numero di conto) e una password alfanumerica. Nel caso in cui le credenziali finiscano nelle mani sbagliate o vengano "spiate" sul nostro computer da occhi indiscreti, chiunque risulti in possesso dei dati di accesso può disporre liberamente del nostro servizio di home banking disponendo bonifici, operazioni e pagamenti.

PRO: facilità d'uso

CONTRO: bassissimo livello di sicurezza, alto rischio di furto delle credenziali e di phishing

Accesso tramite sms dispositivo o mail

variante del sistema otp che "scavalca" la necessità di un dispositivo fisico in grado di generare i codici temporanei.

Il procedimento prevede che ogni correntista associ, all'atto di sottoscrizione del servizio, un numero di cellulare al proprio conto online. Ad ogni tentativo di accesso tramite credenziali statiche la banca invierà al numero indicato dal cliente un sms contenente la one time password, con validità temporale limitata, in modo da perfezionare l'accesso.
All'utente può essere inoltre data la possibilità di ricevere il codice tramite mail, con procedimento analogo

PRO: elevata sicurezza, praticità di impiego

CONTRO: in caso di furto o smarrimento del cellulare (o di intrusioni nella casella mail) il codice dispositivo può essere inviato a terzi con conseguenti rischi per la sicurezza del conto.

Accesso tramite card fornite dalla banca

Accanto alle credenziali statiche, alcune banche hanno integrato nella procedura di accesso la richiesta di dati personali (es. data di nascita del cliente) e di un codice alfanumerico contenuto in un'apposita card fornita ai correntisti, organizzata in celle. Ad ogni accesso il sistema di login chiede all'utente di inserire il codice contenuto in una data cella (un meccanismo simile alla battaglia navale) senza il quale l'accesso all'home banking non viene autorizzato.

PRO: grande praticità, le card possono facilmente essere trasportate all'interno di borse e portafogli come una normale carta di credito

CONTRO: se individuata, la card può essere copiata e usata da terzi per accessi non autorizzati.

Accesso tramite credenziali statiche e codici "one time

Per ovviare alla vulnerabilità delle credenziali statiche da ormai qualche anno i principali istituti bancari hanno fornito ai propri correntisti i cosiddetti dispositivi OTP, piccoli display che alla pressione di un tasto mostrano per pochi secondi un codice numerico da inserire a ogni singolo accesso. Il codice in questione è caratterizzato da una validità temporale limitata, generalmente da 10 a 20 secondi, al termine dei quali viene sostituito da un nuovo codice casuale. In tal modo, in mancanza del dispositivo otp risulta pressoché impossibile inserire il codice corretto e quindi accedere al conto bancario di un utente.

PRO: elevata sicurezza, la vulnerabilità a un ipotetico attacco informatico è limitata alla durata del codice otp impiegato per l'accesso

CONTRO: ogni correntista è obbligato a portare con sé il dispositivo otp, senza il quale non è possibile accedere all'home

Accesso tramite verifica telefonica

Variante dell'sms dispositivo. Ogni volta che un utente effettua un accesso all'home banking attraverso le credenziali statiche, gli viene chiesto di inoltrare una chiamata verso un numero della propria banca concordato in fase di sottoscrizione di contratto. Il numero in questione può essere salvato nella rubrica con uno pseudonimo o con un nome di fantasia, rendendone praticamente impossibile l'individuazione da parte di malintenzionati.

PRO: elevata sicurezza e praticità di impiego

CONTRO: in caso di telefono sorvegliato o controllato, il numero della banca potrebbe essere rintracciato da terzi per effettuare accessi non autorizzati al proprio conto.

Tecniche e procedure per difendere il tuo conto

Se da un lato le banche dispongono di schiere di professionisti della sicurezza informatica, le statistiche confermano che 9 volte su 10 gli attacchi degli hacker si concentrano sull'anello debole del sistema: il cliente.

Spesso i correntisti accedono ai servizi di home banking da computer privi di antivirus, caratterizzati da sistemi operativi obsoleti e quindi altamente vulnerabili agli attacchi informatici o, nel peggiore dei casi, infettati da virus e trojan.

Il primo passo per operare online in sicurezza è quindi quello di attuare le pratiche di sana e prudente navigazione informatica, gestendo i propri apparati con cura e aggiornandoli periodicamente.

Ogniqualvolta si accede a un servizio di home banking è opportuno prestare la massima attenzione al modo in cui si opera. Di seguito illustreremo passo a passo tutti gli accorgimenti utili e le precauzioni indispensabili per non incappare in brutte sorprese.

1- Solo il tuo computer, e un solo browser. Reti pubbliche senza protezioni o linee di conoscenti delle quali si ignorano i requisiti di sicurezza potrebbero essere controllate da truffatori pronti a carpire i vostri dati. Per non incorrere in brutte sorprese, è bene accedere ai servizi di home banking esclusivamente dal proprio computer e non da quello di estranei, dedicando alla procedura di accesso un browser esclusivo (con il quale non si dovrà quindi navigare sul web) e tenendolo costantemente aggiornato sotto il profilo della sicurezza. In questo modo è possibile ridurre notevolmente il rischio legato a infezioni malevole e al furto dei dati.

2- Antivirus dedicati e aggiornati. Ricordarsi sempre che installare un antivirus e tenerlo aggiornato è come installare una serratura sulla porta di casa e ricordarsi di chiuderla ogni volta che si esce: un comportamento elementare che contribuisce a tener lontane le brutte sorprese. Analogamente anche il sistema operativo e i browser di navigazione dovranno essere aggiornati costantemente sotto il profilo della sicurezza. I produttori di questi sistemi rilasciano periodicamente aggiornamenti utili a tappare le "falle" di sicurezza insite in questi programmi, generalmente sfruttate dal cybercrimine per aggirare le normali protezioni e carpire i dati degli utenti.

Avviare scansioni periodiche del sistema può inoltre aiutare a identificare rapidamente una falla nella sicurezza del proprio computer: sia gli antivirus in commercio che le versioni free consentono di programmare scansioni automatiche secondo le esigenze specifiche dell'utente. Il mercato offre sotto questo aspetto un ampio ventaglio di soluzioni in versione free o a pagamento, dedicate ai privati e alle aziende: Symantec, Mcafee, Trend Micro, Kaspersky, Avg, F-Secure, Panda Security, Eset, Avast forniscono una grande mole di prodotti dedicati alla sicurezza informatica, calibrati sulla base delle specifiche esigenze degli utenti.

3- Porno, file sharing e materiale illegale: i siti più pericolosi per i conti bancari. Siti contenenti materiali illegali, piattaforme di file sharing, portali segnalati dai filtri anti-phishing rappresentano un ricettacolo di minacce informatiche sotto forma di virus, trojan e malware. Il rischio di essere contaminati e successivamente di vedersi sottrarre le credenziali bancarie è sempre presente: per tali ragioni è consigliabile effettuare l'accesso all'home banking solo da computer sicuri, meglio ancora se dedicati a questo genere di attività e non soggetti alla navigazione web intensiva.

4- Digitate sempre l'indirizzo della vostra banca. Ad ogni accesso l'indirizzo internet del vostro home banking dovrà essere digitato manualmente nella barra degli indirizzi. Per evitare che occhi indiscreti possano spiarvi, è preferibile infatti non salvarlo nell'elenco dei preferiti. In nessun caso si dovrà dare credito a link di accesso contenuti in messaggi email o sms: costituiscono sicuramente delle truffe.

5- Occhio al lucchetto. Anche quando si inserisce manualmente l'indirizzo della propria banca, prima di inserire le credenziali di accesso è necessario verificare la presenza del lucchetto accanto alla barra degli indirizzi del browser e la scritta https:// all'inizio del sito. Questi simboli ci comunicano che i dati inseriti saranno trasmessi al nostro istituto di credito tramite una connessione protetta, al riparo dagli occhi dei truffatori, fornendoci ampi standard di sicurezza.

Qualora il lucchetto non dovesse improvvisamente apparire è necessario evitare l'inserimento dei dati, controllare scrupolosamente l'indirizzo contenuto nella barra del browser ed eventualmente lanciare una scansione completa del computer con un programma antivirus alla ricerca di infezioni: programmi maligni potrebbero essere all'opera per sottrarvi i vostri dati bancari.

6- Scelta delle credenziali. Il primo passo per accedere al vostro conto online consiste nell'inserimento delle credenziali statiche, generalmente rappresentate da username e password. Preferite sempre codici alfanumerici di almeno 8 caratteri e rinnovateli periodicamente, evitando nomi o date strettamente legate alla sfera

personale in quanto facilmente rintracciabili da terzi. Non salvate mai user e password all'interno della memoria di computer, tablet o telefonini per evitare di esporle alla mercé di intrusi e prevenirne lo smarrimento.

Scegliete inoltre una piattaforma di home banking in grado di fornire sistemi di accesso aggiuntivi oltre alle classiche credenziali statiche. Statisticamente le banche che adottano sistemi otp o simili vedono crollare drasticamente il numero degli attacchi informatici e i tentativi di phishing verso i clienti.

7- Una volta all'interno dell'home banking, dedicatevi solo a quello. Per nessuna ragione è opportuno aprire programmi o indirizzi internet mentre è attiva la connessione con la propria banca. Prima di effettuare l'accesso all'home banking, è buona norma chiudere tutti i programmi in esecuzione sul computer e tutte le finestre (o le schede) di navigazione aperte.

Esaurite le attività è necessario provvedere sempre al log-out e alla conseguente chiusura della sessione mediante l'apposito tasto contenuto nella pagina. Non chiudere mail il browser senza aver prima eseguito questa semplice operazione.

8- Diffidate sempre da improvvise anomalie e cambiamenti. Se da un giorno all'altro la vostra banca modifica le modalità di accesso o le grafiche del sito senza darvene preventiva comunicazione, con ogni probabilità vi trovate davanti a un tentativo di truffa. Davanti a schermate di login diverse o richieste di inserimento di dati aggiuntivi è opportuno contattare telefonicamente la banca e chiedere i dovuti chiarimenti.

9- Controllate gli estratti conto cartacei e ogni tanto, andate di persona. Tutte le banche sono solite inviare al cliente via posta tradizionale gli estratti conto e le notifiche dei movimenti con cadenza mensile o trimestrale. È buona norma confrontare sempre questi documenti con gli estratti conto dell'home banking e comunicare eventuali anomalie alla propria banca. Ogni tanto, per eseguire un'operazione, telefonate alla banca o recatevi di persona allo sportello.

10 – In banca, ignorate le mail e verificate gli SMS. Anche a fronte di mail o sms che sembrano essere spediti da una banca è necessario attivare tutte le precauzioni possibili. Nessuna banca utilizza mail o messaggi sul cellulare per comunicare con la propria clientela. Generalmente per smascherare un tentativo di phishing via mail è sufficiente valutare pochi, semplici elementi:

A - Leggere attentamente il messaggio alla ricerca di errori di ortografia e/o sintassi: spesso gli artefici del phishing utilizzano traduttori automatici per diffondere un'unica comunicazione in decine di lingue diverse, ricorrendo inevitabilmente in imprecisioni o palesi errori grammaticali. Nessuna banca si sognerebbe mai di inviare una comunicazione con questo stile "maccheronico".

B - Controllare scrupolosamente gli indirizzi web linkati nella mail: una lettera in più, una virgola, qualsiasi carattere aggiuntivo rispetto all'indirizzo web canonico dell'istituto bancario costituisce una chiara prova di frode. Il messaggio dovrà quindi essere cestinato ed eventualmente segnalato alla polizia postale per le indagini del caso.

C - Non cliccare sui link contenuti nelle mail sospette: il rischio è quello di infettare il proprio computer e di comprometterne la sicurezza.

D - In caso di dubbio, anche lieve, contattare telefonicamente la propria banca per verificare l'effettiva provenienza delle comunicazioni.

Anche quando il pericolo arriva via sms basta rimanere calmi ma allerta: per proteggersi da questo tipo di truffa occorre prestare la massima attenzione all'SMS ricevuto analizzando il numero del mittente, valutando l'assenza di firme o l'indicazione del nominativo della propria banca, elementi per cui dovrebbero scattare fin da subito i primi campanelli di allarme. In molti casi è sufficiente telefonare alla propria banca ed esporre la questione per prevenire un pericoloso raggiro.

Mobile banking: tablet e smartphone, cosa installare

La possibilità di mobilitare i conti correnti anche al di fuori di case e uffici rappresenta una grande opportunità: pagare al supermercato attraverso smartphone o disporre un bonifico dal bancone del bar rappresenta l'ultima frontiera dei servizi bancari. Ma come tale deve essere tutelata.

Consentire di compiere operazioni così delicate ai propri correntisti da qualsiasi luogo e da qualunque device connesso a internet rappresenta una grande sfida per gli esperti di sicurezza. Specialmente considerando come i telefonini rappresentino ormai il top dell'intrattenimento, permettendo di mischiare l'attività ludica a quella ben più delicata del controllo delle proprie finanze.

Al fine di permettere una convivenza tra questi due mondi, sempre più banche stanno implementando sugli smartphone applicazioni proprietarie in grado di proteggere gli accessi e le operazioni di mobile banking secondo i più stringenti standard di sicurezza in materia di trasmissione dei dati, al riparo da sguardi indiscreti. A patto ovviamente di eseguire ogni accesso in modo da non essere visti da chi ci sta attorno.

A differenza dei normali computer, gli smartphone implementano sistemi operativi più complessi da penetrare e quindi meno "gettonati" dalle mire dei cyber criminali.

Anche in questo caso il panorama offerto dal mercato è abbastanza variegato: si passa dai più sicuri sistemi mobili con sistema chiuso e applicazioni firmate (iOS Apple) a quelli aperti (Android) che risultano maggiormente suscettibili ad attacchi. Un mercato considerato di nicchia fino a pochi anni fa ma in rapidissima crescita, dove non si può escludere per l'immediato futuro un'espansione di nuovi trojan più evoluti e capaci di bucare le difese dei dispositivi mobile.

Allo stato attuale, dunque, valgono le stesse raccomandazioni espresse per i computer tradizionali: proteggere lo smartphone con un codice pin e un antivirus dedicato, evitare di salvare nella memoria dello stesso le credenziali di accesso e tenere costantemente uno stretto controllo sul device. In caso di furto o smarrimento può essere utile installare preventivamente un software che consenta da remoto la cancellazione di tutti i dati sensibili, la formattazione del sistema operativo ai parametri di fabbrica o meglio ancora il blocco del dispositivo, tutelando così la nostra privacy.

Oltre alle funzioni native implementate nei device Android e Apple, il mercato offre un buon numero di app dedicate e implementate nei comuni software antivirus per il mondo mobile (come Avast! Mobile Security, Sophos Mobile Security, Norton Mobile Security).

Quando le banche chiedono di firmare su un tablet

Alcuni istituti di credito hanno acquisito l'abitudine di richiedere le firme dei propri clienti attraverso un tablet. Una procedura per certi versi scontata dato il crescente impiego di questi dispositivi nella vita quotidiana, ma che si presta invece a molteplici controversie. Il rischio in questo caso è che il protocollo di acquisizione delle firme risulti carente sotto il profilo della sicurezza, con potenziale rischio di uso improprio da parte di terzi. **Dal punto di vista normativo in Italia sono le stesse leggi a fare confusione** in tema di firme grafometriche acquisite via tablet.

Sotto un profilo strettamente normativo le firme non olografe (acquisite cioè su documento digitale) vengono classificate in due livelli di sicurezza. Il primo è la cosiddetta firma elettronica qualificata e si avvale di dispositivi informatici certificati da enti qualificati sui quali l'utente può mantenere uno stretto controllo (es. lettori smart-card o penne usb munite di apposito protocollo di certificazione).

In seguito c'è la firma elettronica avanzata, che sfrutta dei dati biometrici dell'autore e che legalmente è stata equiparata alla firma autografa. I device più diffusi consentono in genere l'acquisizione della firma del cliente con annessa registrazione delle informazioni biometriche (pressione, inclinazione della mano). Valori che, a detta dei produttori dei device, sarebbero sufficienti da soli a garantire l'originalità della firma. Tuttavia la definizione delle caratteristiche di tale firma è relegata ad una serie di linee guida ancora in attesa di stesura.

I dispositivi per la raccolta delle firme elettroniche avanzate rientrano in realtà allo stato attuale in una "zona grigia" della normativa, non rientrando nel pieno rispetto delle leggi vigenti ma nemmeno in una loro violazione. Diversi istituti bancari, alla prova dei fatti, le utilizzano per le firme di cassa e le operazioni ordinarie dei loro clienti, riservando la firma autografa ai contratti nei quali, fra l'altro, deve apparire chiaramente il consenso del cliente all'utilizzo della firma grafometrica e un'adeguata informativa circa l'utilizzo di questo sistema. La confusione sul tema è ancora grande e l'attuale quadro normativo non si è ancora adattato alla novità.

Per semplificare, ogni utente al quale venga chiesto di apporre una firma su di un tablet dovrà accertarsi che la procedura di acquisizione rispetti una serie di parametri: modalità di apposizione della firma, caratteristiche del sistema di acquisizione, modalità di acquisizione e quantità dei dati biometrici raccolti, possibilità di bloccare il documento firmato e di verificarne la non alterabilità dopo la firma, possibilità per il firmatario di ricevere copia di quanto sottoscritto, connessione univoca tra la firma e il firmatario. La sola disponibilità da parte della banca a richieste di questo tipo può essere una prima forma di risposta.

In presenza di tutti questi fattori, la firma eseguita su un tablet può essere equiparata a una firma elettronica qualificata e avere quindi valore probatorio legale. In attesa ovviamente che il quadro normativo in materia possa fornire regole precise e requisiti necessari per l'ottenimento giuridico dell'equiparazione.

Si ringraziano per la cortese collaborazione e la consulenza prestata **Sandro Tucci**, Responsabile IT e direttore dei sistemi informativi CheBanca!

Stefano Zanero, Ricercatore del dipartimento di elettronica, informazione e bioingegneria del Politecnico di Milano.

L'autore: **Roberto Bonfatti**

Giornalista, copywriter, scrittore per passione. Da anni seguo con interesse il mondo dell'IT, con un occhio sul mondo e uno sulla mia tastiera.