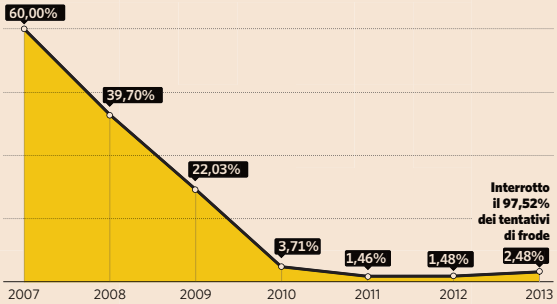
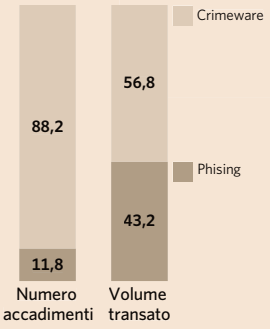
CLIENTI RETAIL ATTIVI CHE HANNO PERSO DENARO PER LA PERDITA DI CREDENZIALI
Trend 2007-2013. *Valori in %*

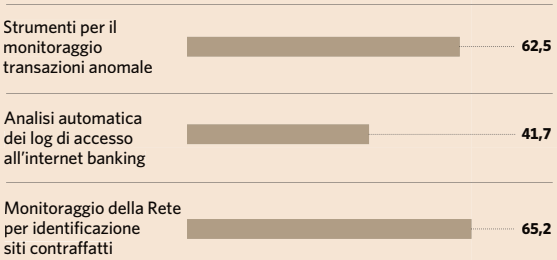


MODALITÀ DI ATTACCO
Tentativi e volume per tipologia. *In %*



COSÌ LE BANCHE INFORMANO I CLIENTI
Strumenti utilizzati, risp. multiple. *In %*

IL MONITORAGGIO DELLE TRANSAZIONI: LE DOTAZIONI TECNOLOGICHE UTILIZZATE
Strumenti messi in campo delle banche. *Risposte in % sul campione*



Fonte: ABI Lab, 2014

Serve buon senso per tutelarsi da sé

Aggiornare l'antivirus, evitare di cliccare su siti, codici e link ignoti, usare password diverse Occhio ai social network

Gabriele Petrucciani

Dal *phishing* al *malware*, fino ad arrivare al *crimeware*. Gli attacchi degli *hacker* ai nostri dati personali sono molteplici. Oggi ci sono talmente tanti virus che l'attenzione deve rimanere sempre alta. Certo, le nuove generazioni sono più preparate, soprattutto da un punto di vista informatico. Ma non basta per sentirsi protetti al 100 per cento. A volte anche i più esperti, per fare un esempio, disabilitano, seppure per un attimo, l'antivirus sul proprio computer per accelerarne le prestazioni e concludere più velocemente una transazione. In questo modo, però, ci si espone all'attacco dei pirati informatici, che può avvenire nei modi più disparati.

«Con una mail – fa notare Domenico Raguseo, manager delle vendite tecniche per l'Europa dei sistemi di sicurezza di Ibm – ma anche attraverso gli *short link*, nati per facilitare l'utilizzo dei dispositivi mobili, o ancora attraverso i *QR code* (i codice a barre bidimensionali, spesso a forma di quadrato, *ndr*)», che potrebbero ricondurre a siti malevoli in grado di infettare il proprio dispositivo, mobile o fisso.

Per tutelarsi al meglio occorre in primis buon senso. «Parlando di *fishing* – sottolinea Paolo Frizzi, amministratore delegato di Libraesva, società attiva nell'ambito delle soluzioni avanzate di *email security* – bisogna sempre ricordarsi che le società con cui siamo legati, tipo le banche per il conto corrente o le compagnie telefoniche, hanno già i nostri dati. Quindi dobbiamo sempre diffidare dalle email che per esempio riceviamo dal nostro istituto di credito e in cui ci viene chiesto di inserire nuovamente i dati personali». Inoltre, quando si naviga sul web, o si fanno delle transazioni nel mondo virtuale, è fondamentale accertarsi dell'esistenza di un protocollo di sicurezza, «che può essere verificato controllando che all'inizio dell'indirizzo internet ci sia la sigla https:// o il simbolo del lucchetto», aggiunge ancora Frizzi.

In linea generale, comunque, per evitare di incappare in *malware* o *crimeware* è consigliabile dotare il proprio pc di un buon antivirus, mantenendolo sempre aggiornato. «Una pratica da seguire anche sui dispositivi mobili – puntualizza il ceo di Libraesva – soprattutto su quelli Android. Sui device Apple, che adottano un sistema operativo chiuso, prendere un virus è quasi impossibile. Android, invece, è un sistema aperto, e il processo di approvazione delle applicazioni è meno severo. Quindi è più facile imbattersi in App malevole».

Al di là degli aspetti più tecnologici, ci sono anche una serie di buone pratiche che è consigliabile seguire, «evitando, per esempio, di utilizzare la stessa password per social network e applicazioni, anche bancarie – continua Raguseo di Ibm –. Ancora, le *password* non dovrebbero mai richiamare i propri dati, come la propria data di nascita o quella dei figli. Inoltre, bisogna prestare molta attenzione a cliccare *short link* o a fotografare *QR code* provenienti da sconosciti». Potrebbero contenere un virus capace di catturare, attraverso *screenshot* o la registrazione delle sequenze dei tasti digitate, i dati di accesso all'*home banking*. Occhio, infine, a collegarsi a reti wi-fi aperte; dietro potrebbe nascondersi uno dei tanti hacker spia.

IL DECALOGO PER LA SICUREZZA ONLINE

1. **Attivare gli sms alert**
Si riceve un sms quando si accede al conto Internet, quando si fa un bonifico o quando si usa la carta.

2. **Proteggere i dati personali**
I dati come il pin delle carte o le password di accesso al proprio conto online vanno sempre protetti.

3. **Affidarsi a un antivirus**
Per proteggere i propri device, mobili e fissi, dai malware è consiglibile dotarsi di un buon antivirus.

4. **Selettivi sui social**
Numerosi social network, inclusi i più recenti, sono tra i principali bersagli per i tentativi di phishing.

5. **Verificare se il sito è sicuro**
Controllare che l'indirizzo web sia preceduto dalla sigla di sicurezza https:// e non da http://.

6. **Evitare link sospetti**
Diffidare delle email in cui la banca chiede di cambiare i propri dati personali cliccando su un link.

7. **Utilizzare reti wi-fi protette**
Dietro agli hotspot aperti si possono nascondere hacker che spiano le attività per rubare dati.

8. **Affidarsi a più password**
Utilizzare un'unica password per siti di e-commerce, conto online e social è altamente rischioso.

9. **Prudenza nell'uso del cloud**
È consigliabile agire con prudenza prima di mischiare documenti personali e di lavoro nel cloud.

10. **Controllare l'estratto conto**
Con un controllo regolare è possibile verificare che le transazioni riportate siano quelle effettuate.

«Più hi-tech per offrire maggiori garanzie»

INTERVISTA

Pietro Giordano
Presidente nazionale Adiconsum

Utilizzare l'*home banking* o una carta di credito sui siti di *e-commerce* oggi è più sicuro rispetto a quale anno fa. Le banche hanno rafforzato molto i sistemi di sicurezze e gli stessi consumatori sono molto più attenti. «Ma il problema del *phishing* e del furto di *password* e dati personali c'è ancora», puntualizza Pietro Giordano, presidente nazionale di Adiconsum.

Come giudica i sistemi di sicurezza delle banche?

Sono buoni, ma non all'avanguardia, nel senso che un *hacker* bravo, sebbene con delle difficoltà, sarebbe in grado di violare il sistema.

Dove gli istituti di credito sono ancora deficitari?

Per esempio, una delle cose che le banche non fanno è distruggere con il tritacarte i documenti che contengono dati sensibili. Nella maggior parte dei casi vengono semplicemente buttati nel classico cestino, che è una delle principali fonti per il furto d'identità.

E sul fronte del *phishing*?

Anche in questo caso i sistemi di sicurezza degli istituti di credito non sono efficienti al 100 per cento. Per esempio, non tutte le banche hanno un sistema anticontraffazione del logo. Eppure, con un logo difficilmente riproducibile i casi di *phishing* si ridurrebbero notevolmente.

Come aumentare la sicurezza, allora?

Investendo di più in nuove tecnologie. Se le banche si agganciassero all'agenda digitale potrebbero investire anche 10 miliardi di euro su questo fronte, offrendo quindi una maggiore garanzia al consumatore. Ma gli istituti di credito non si stanno muovendo in tal senso. O meglio, non tutti. — **G. Pe.**