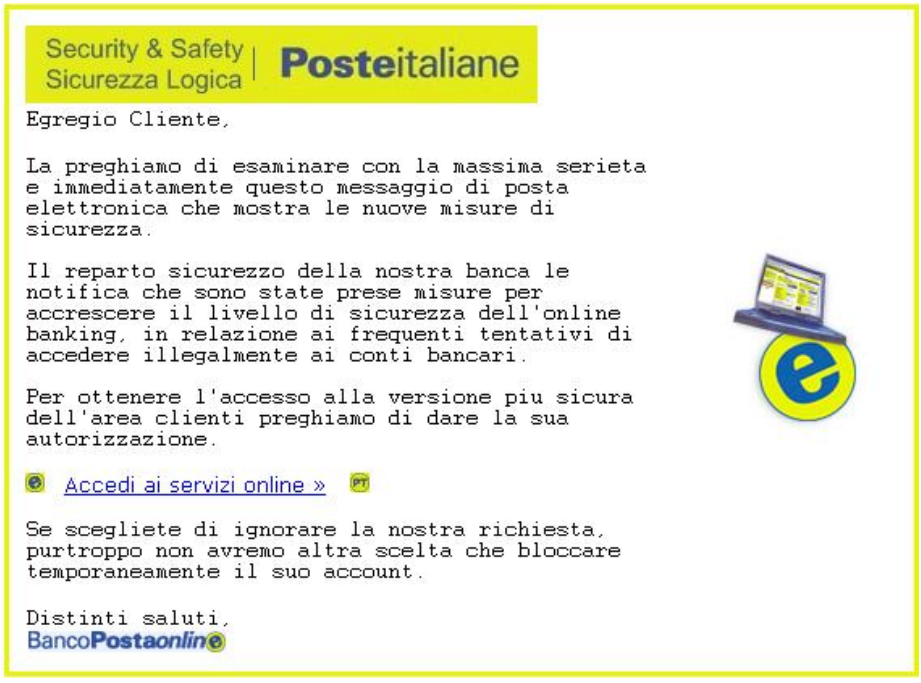
10 regole per difendersi dal furto di identità e dal phishing

di Sebina Pulvirenti

Uno su 4 italiani ne è vittima. Lo chiamano **furto d'identità** e ti riguarda **quando qualcuno riesce a rubarti informazioni personali a cui solo tu hai diritto di accesso**: il numero della tua carta di credito, il pin del tuo telefono, la password per accedere alle email, le credenziali per entrare su Facebook o su Windows Live Messenger, e via dicendo. Non è solo la tua privacy ad essere violata. Il furto d'identità spesso è seguito da altri tipi di reati: chi entra nel tuo conto bancario, per esempio, può effettuare trasferimenti di denaro, acquistare beni e servizi e compiere innumerevoli altri danni.

La vittima di un furto d'identità spesso non si accorge di nulla finché non inizia a ricevere addebiti che non riesce a spiegare sul conto bancario o telefonico o quando tenta invano di entrare sul proprio account Facebook o MSN con le solite credenziali. La miglior arma in casi come questo è la prevenzione. In questo post **ti diamo qualche consiglio su come proteggerti dal furto d'identità online e dal phishing**, che altro non è che il metodo pratico con cui si realizza il furto per via informatica.

Capita anche ai migliori. Basta un attimo di distrazione per cadere nella trappola. Nella mia famiglia è successo ben due volte. **Il phishing si verifica soprattutto via email o messaggi istantanei di chat.** Se sono un ladro e voglio ottenere le chiavi per accedere al tuo conto BancoPosta che faccio? Creo un'email quasi identica a quelle che invia *Poste.it*: stessa grafica, stesso logo, stesso tipo di testo e impaginazione. E dentro ci scrivo un messaggio di questo tipo:


Security & Safety
Sicurezza Logica | Posteitaliane

Egregio Cliente,

La preghiamo di esaminare con la massima serieta e immediatamente questo messaggio di posta elettronica che mostra le nuove misure di sicurezza.

Il reparto sicurezzo della nostra banca le notifica che sono state prese misure per accrescere il livello di sicurezza dell'online banking, in relazione ai frequenti tentativi di accedere illegalmente ai conti bancari.

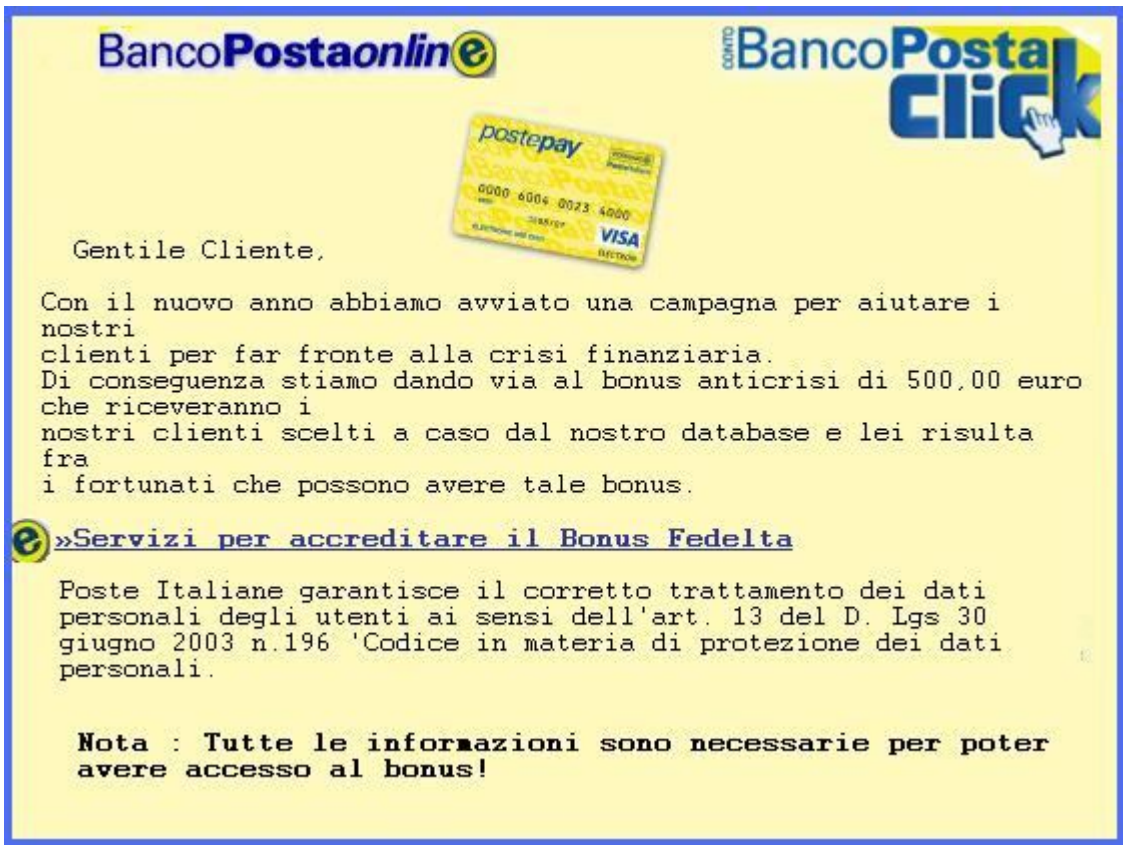
Per ottenere l'accesso alla versione piu sicura dell'area clienti preghiamo di dare la sua autorizzazione.

Accedi ai servizi online »

Se scegliete di ignorare la nostra richiesta, purtroppo non avremo altra scelta che bloccare temporaneamente il suo account.

Distinti saluti,
BancoPostaonline

Oppure scelgo un'esca ancora più allettante, come questa:



Tu cosa fai? Se non hai mai sentito parlare di phishing e furto d'identità su Internet ti fidi di quello che leggi: c'è il logo giallo di *Poste Italiane* e tutto! Quindi clicchi diligentemente sul link *Accedi ai servizi online*, che guardacaso redirige a un sito quasi identico a quello originale. Digiti la tua password e... segni l'inizio del dramma. Perché il truffatore fa leva proprio sulla fiducia che i risparmiatori ripongono nella propria banca: mentre tu digiti, lui registra i dati da te inseriti e li riutilizzerà per entrare nel tuo account e rubare i tuoi soldi! Che fare per proteggersi? In fondo è facile, basta essere informati e prudenti. Ecco un decalogo da diffondere tra amici e familiari.

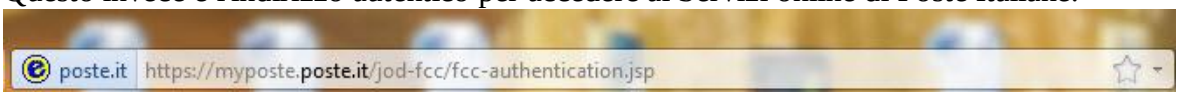
1.La grammatica ci salverà

Guarda attentamente le due immagini sopra, specialmente la prima: **noti gli errori grammaticali?** Se ricevi un messaggio simile dalle Poste o dalla tua banca Unicredit o Vattelapesca, cestinalo subito. Gli istituti di credito e altri enti pubblici dotati di un minimo di credibilità solitamente dispongono di abbastanza fondi da potersi permettere un copywriter che non fa errori di ortografia! Quello che hai davanti è al 99% un tentativo di phishing.

2.Sta' alla larga dagli indirizzi fasulli

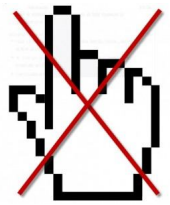
Se passi il puntatore del mouse sul link *Accedi ai servizi online* o *Servizi per accreditare il Bonus Fedelta* contenuti nei suddetti messaggi, visualizzerai un indirizzo simile al seguente:

Questo invece è l'indirizzo autentico per accedere ai Servizi online di Poste Italiane:



Noti la differenza? Il truffatore maschera il proprio indirizzo web che usa per registrare i dati delle vittime in maniera molto credibile. Tu vedi "*https://www.poste.it*", ma con un'indagine più approfondita noterai strani codici numerici o altri URL che nulla hanno a che vedere con il sito che ti viene richiesto di visitare. Questo è un caso di phishing al 100%.

3. Non cliccare sui link sospetti



Se ricevi un'email dalla tua banca o dalla compagnia telefonica o da Facebook che ti chiede di cambiare i tuoi dati personali (username e password) **non cliccare su alcun link presente nel messaggio**. Per proteggerti dal phishing, nessun ente pubblico ti chiederà mai di rivelare nome utente e password via email né tantomeno per telefono, SMS o via chat. Per accedere ai servizi online di qualsiasi sito dove hai un profilo privato **usa sempre e solo link sicuri salvati tra i tuoi preferiti** e non cliccare su alcun collegamento sospetto. Diffida e rispondi un secco "No!" a chiunque ti chieda queste informazioni.

4. Il furto di identità su Facebook e altri social network

Nomi utente e password, numeri di conto, di documenti e di carte di credito, codice fiscale, indirizzi email, codici PIN, numeri di telefono... Non per niente si chiamano *dati personali*: sono privati e non vanno rivelati a nessuno, nemmeno ad amici e parenti. Attenzione anche alle date di viaggi e spostamenti: ci sono persone che tornando dalle vacanze si sono ritrovate la casa svaligiata perché avevano rivelato la partenza su Twitter o su Facebook.

Se sei iscritto a Facebook, Badoo o un altro social network sappi che ci sono delle informazioni che è sempre meglio tenere per te e al massimo per i tuoi amici: **data di nascita, indirizzo, nome completo tuo e dei tuoi familiari, foto di casa o del posto dove lavori**. Controlla le impostazioni della privacy di Facebook, in questo tutorial ti spieghiamo come si fa a nascondere alcune informazioni di Facebook a chi non è tuo amico. E ricordati di non accettare mai le richieste di amicizia di perfetti sconosciuti!

5. Fidati della cartella di Posta indesiderata

I messaggi che si trovano nella cartella dello spam di Gmail, Yahoo! Mail, Hotmail, Libero Mail e Alice Mail al 90% sono junk mail o tentativi di phishing. Se includono link sospetti che ti richiedono dati sensibili **cestina le email senza alcuna pietà e non attivare i collegamenti e le immagini che contengono**. Se scarichi i messaggi di posta sul computer tramite programmi come Microsoft Outlook, Thunderbird o Incredimail assicurati che la cartella di posta indesiderata sia attiva e ben funzionante. Se il tuo client di posta non include una simile funzione scarica un apposito programma antispam.

6. L'antivirus è il tuo miglior amico, aggiornalo!

Installa nel tuo computer un antivirus che ti protegga anche dal phishing e tienilo sempre ben aggiornato. Ormai quasi tutti gli antivirus includono una funzione antiphishing: quello che fanno è avvertirti del pericolo ogni volta che clicchi su un collegamento truffaldino. Se non sei sicuro che il tuo antivirus ti protegga anche da questa minaccia scegli AVG Anti.Virus, Panda Cloud Antivirus o Avira AntiVir (sono gratuiti). E se vuoi esagerare con la protezione installa anche un'apposita toolbar come Web Security Guard o AVG LinkScanner: ti proteggono mentre navighi su Internet contrassegnando con un simbolo autoesplicativo i siti a rischio sui motori di ricerca.

7. Rafforza le tue password e... la memoria!

Meglio non usare programmi che salvano le password nel browser o le autocompletano: se il criminale riesce ad accedere al tuo PC sono guai! Usa password alfanumeriche, di almeno 6 caratteri e cambiale spesso (una volta al mese). Per accertarti che la tua password sia sicura puoi scaricare un programma di creazione di password solide come IameGen o uno che verifichi la sicurezza di quelle attuali: in questo articolo ti spieghiamo come scegliere una password sicura.

8. Comprare su Internet è sicuro solo se...

Se fai acquisti su Internet non usare carte di credito, **dai la preferenza a una prepagata** come la Postepay oppure, ancora meglio, apri un account PayPal che in caso di truffa ti permette anche di recuperare il denaro perduto. Accertati anche che il sito su cui fai acquisti sia affidabile e che usi sistemi di crittografia come le connessioni SSL/TLS, evidenziate sulla barra degli indirizzi del browser da un'icona a forma di lucchetto.

9. Una nuova minaccia: gli URL accorciati

Un occhio di riguardo anche agli indirizzi web accorciati tramite servizi come TinyURL o Google url shortener: potrebbero nascondere pericoli sotto sembianze innocue. Meglio visualizzare sempre l'indirizzo completo attraverso un programma come **Long URL Please**, prima di visitarlo.

10. Nel dubbio, chiedi a un esperto, sempre!

In ogni caso, sempre meglio esagerare con la prudenza che il contrario. Se sei in dubbio sulla sicurezza di un messaggio email prima di cliccarci sopra per aprirlo chiedi una consulenza gratuita a Google o a un amico esperto di Internet e computer (meno male che tutti ne abbiamo uno... E se non ce l'hai c'è sempre Softonic!). Puoi anche consultare l'ottimo servizio antibufala offerto dal blogger Paolo Attivissimo, che raccoglie indagini dal 2002 ad oggi.

In sintesi, attraverso queste semplici accortezze ci si può ritenere al sicuro. Ma la cautela non è mai troppa, **ecco qualche consiglio per quando sei offline**:

- Distruggi tutti i documenti che contengano dati sensibili prima di cestinarli: estratti conto, bollette, lettere, vecchi documenti e carte di credito.
- Se non ricevi più le bollette contatta l'istituto che le emette e chiedi spiegazioni: un ladro d'identità potrebbe aver cambiato il tuo indirizzo di residenza.
- Non inviare via posta i documenti personali, e se proprio devi farlo informati prima sulla maniera più sicura.
- Non portare con te troppi documenti.
- Usa il servizio di avviso SMS dei movimenti sul tuo conto bancario.
- Denuncia sempre il furto di qualsiasi documento personale, di agende e carte di credito.

Ladri di identità... tremate!