

Ce este *Phishing-ul*?

Phishing-ul este o forma de furt de identitate online care presupune atat practici de social engineering cat si mijloace tehnice pentru a va fura datele dvs. personale impreuna cu mijloacele de acces la conturile dvs.

Social engineering inseamna actul de manipulare a unei persoane astfel incat aceasta sa faca o actiune dorita de initiator sau ca aceasta sa isi divulge informatiile confidentiale.

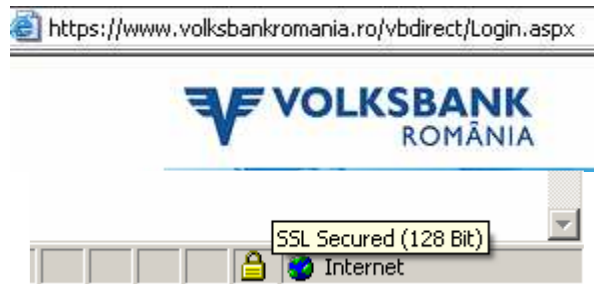
Furtul de identitate este o infractiune care presupune o persoana care se pretinde a fi altcineva pentru a obtine in numele acesteia beneficii materiale sau de alta natura.


Ce fac de obicei *Phisher-i*?

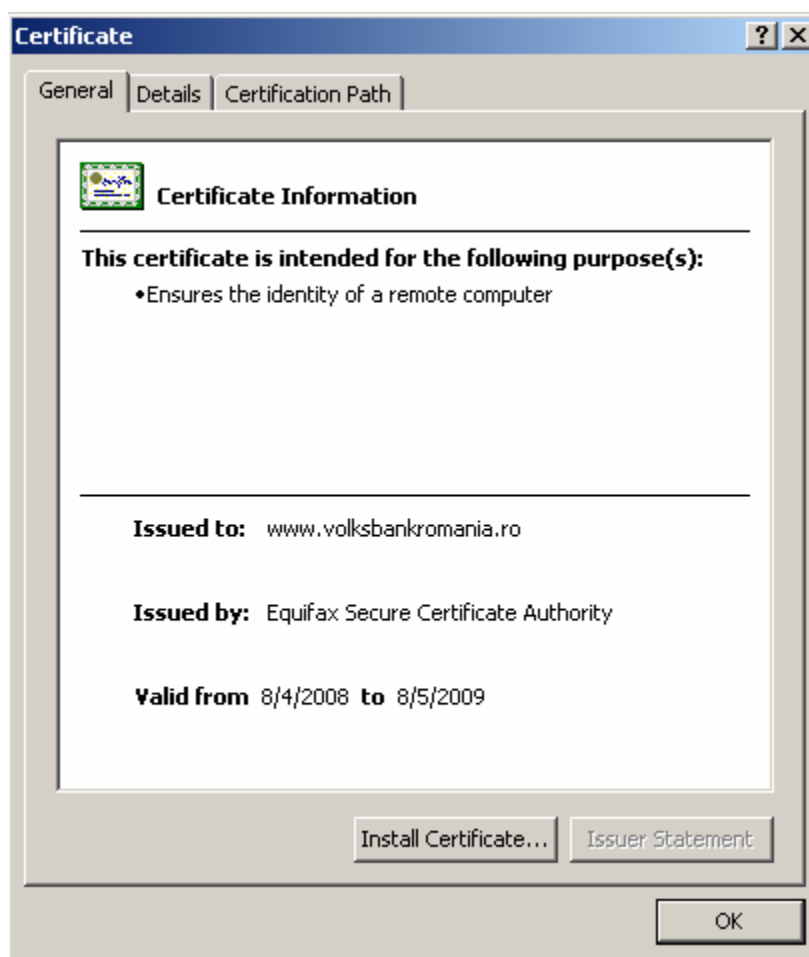
- Va trimit un mesaj e-mail ce se pretinde a fi trimis de catre o sursa legitima, mesaj care contine un link catre un site unde sunteti rugati sa va introduceti datele dvs. personale (datele de acces la internet banking, detaliile de card, PIN-ul dumneavoastra etc).
- Va trimit un mesaj e-mail ce se pretinde a fi trimis de catre o sursa legitima, mesaj in care vi se cere sa raspundeti la e-mail cu datele dvs. personale (datele de acces la internet banking, detaliile de card, PIN-ul dumneavoastra etc) spunandu-va ca datele sunt necesare pentru actualizarea urgenta a bazei de date a bancii sau ca scopul este verificarea datelor dvs. de catre banca.
- Va trimit un mesaj e-mail in care va felicitati pentru castigarea unui premiu important dar in acelasi timp va cer sa platiti in avans, in contul indicat in continutul mesajului, un comision pentru a putea intra in posesia premiului.
- Va suna pretinzand ca reprezinta banca si ca o problem tehnica tocmai a aparut sau ca ati castigat un premiu important oferit de banca si va cer sa va dezvaluiti datele dvs. personale (datele de acces la internet banking, detaliile de card, PIN-ul dumneavoastra etc).
- Construiesc site-uri false care impersonoaza site-urile originale ale institutiilor financiare (si nu numai), pe care apoi le promoveaza prin intermediul unor mesaje e-mail de tip spam, sau mesaje tip SMS pentru a le sugera clientilor sa viziteze aceste site-uri ca sa isi actualizeze informatiile cu caracter personal (datele de acces la internet banking, detaliile de card, PIN-ul etc).
- Se folosesc de slabiciunile tehnice ale computer-ului dvs. ca sa instaleze programe software cu scop malitios pentru a-i ajuta sa colecteze datele dvs. personale (ex: user si parola) si de asemenea sa altereze configuratia de navigare pe Internet a computer-ului dvs. pentru a va conduce catre site-uri de tip phishing sau catre site-uri autentice dar conexiunea facandu-se printr-un proxy controlat de ei cu scop de monitorizare si interceptare a datelor tastate de dvs.

Cum va protejeaza Volksbank Romania?

- Va ofera un site securizat de internet banking (securizat https si SSL) astfel incat conexiunea dvs sa fie sigura.



- Foloseste un certificat digital de la o autoritate de certificare de incredere pentru a va permite sa verificati autenticitatea site-ului de internet banking. Faceti dublu click pe  din fereastra de logare in internet banking si verificati cine a emis certificatul digital si catre cine a fost el emis. Dupa ce faceti dublu click ar trebui sa vedeti fereastra de mai jos, cu aceleasi detalii.



- Foloseste un mecanism de autentificare bazat pe doi factori de autentificare (ceva ce dvs. stiti – numele dvs. de utilizator si parola aleasa de dumneavoastra – plus ceva ce detineti – token-ul VASCO oferit de banca).
- Identifica in timp real abuzurile de identitate pe site-ul de internet banking.
- Va ofera posibilitatea tehnica sa raportati orice incident de tip phishing.

- o Folositi pagina de contact - <http://www.volksbank.ro/index.asp?pag=contact>, categoria Phishing;

Cum va puteti proteja dvs.?

- Pastrati numai pentru dvs. datele cu caracter personal (datele de acces la internet banking, detaliile de card, PIN-ul dumneavoastra etc). Folositi-le numai pe canale de comunicatie sigure.
- Verificati site-ul de Internet banking inainte de a va loga. Pentru aceasta folositi indicatiile de mai sus.
- Trebuie sa stiti ca Volksbank Romania foloseste urmatoarele practici de comunicare:
 - o **Niciodata** banca nu va cere sa va folositi datele dvs. personale (datele de acces la internet banking, detaliile de card, PIN-ul dumneavoastra etc) in mesaje e-mail sau la telefon. Fluxul datelor personale intre dvs. si banca se face numai pe canale sigure de comunicatie (folosind criptare sau factori suplimentari de autentificare si protectie);
 - o **Niciodata** banca nu va trimite un mesaj cu adresare generala (ex. Draga Client). Toate mesajele trimise de Volksbank Romania catre clientii sai sunt personalizate.
 - o **Niciodata** banca nu va insera in mesajele e-mail link-uri catre site-uri de internet banking sau site-uri la care sa vi se ceara date personale.

E bine sa aveti in vedere si sa folositi urmatoarele bune practici referitoare la echipamentele dvs. personale pe care le folositi in activitatile legate de internet banking (fie ca e vorba de computer personal sau terminal mobil):

- o Folositi un program software de tip anti-virus actualizat, cu modul de anti-spyware.
 - o Activati firewall-ul computer-ului dvs. personal.
 - o Folositi numai programe software cu licenta si de la producatori de incredere.
 - o Pastrati-va programele software actualizate cu ultimele actualizari furnizate de catre producator.
 - o Activati si folositi software de tip anti-spam pentru contul dvs. personal de email.
- Pentru intrebari si sugestii folositi pagina de contact, **categoria Phishing**
→→ <http://www.volksbank.ro/index.asp?pag=contact>