

Bezpečnosť Internet bankingu

Všeobecné bezpečnostné pravidlá pri práci s Internet bankingom

V tomto dokumente nájdete pokyny k dodržaniu bezpečného prístupu do Internet bankingu.

Ako chrániť svoj účet?

Základné pravidlá:

1. **Nikdy** neprezrádajte svoje identifikačné údaje (heslá, kódy, PINy, ...).
2. Banka **nikdy** nežiada citlivé identifikačné údaje od klienta e-mailom a ani telefonicky.
3. Banka **nikdy** nežiada údaje na platobnej karte e-mailom a ani telefonicky.
4. **Nikdy** neukladajte svoje heslá do pamäti prehliadača. Používajte programy na bezpečné uchovanie hesiel ako napr. KeePass, LastPass, 1Password a pod.
5. Používajte len overené a chránené PC. Počítač chráňte pravidelnou inštaláciou bezpečnostných záplat, nainštalovaním aktuálnych verzií antimalware a antispyware programov, a firewallom.
6. **Nikdy** nepoužívajte ľahko uhádnuteľné heslá.
7. **Nikdy** nepoužívajte rovnaké heslo pre rôzne služby a pravidelne si ho meníte.

Vždy si overte či komunikujete priamo s bankou:

1. Overte v prehliadači, či adresa prihlasovacej stránky v prehliadači začína „https://sso.365.bank/“
2. Overte, či je prihlasovacia stránka zabezpečená šifrovaním, čo indikuje obrázok „zámčoka“
3. Overte platnosť šifrovacieho certifikátu kliknutím na „zámček“ a skontrolovaním vydavateľa GeoTrust EV a cieľového servera „sso.365.bank“
4. Po prihlásení overte, že adresa stránky začína na „https://my.365.bank/“
5. Overte platnosť šifrovacieho certifikátu kliknutím na „zámček“ a skontrolovaním vydavateľa GeoTrust a cieľového servera „my.365.bank“

Ako sa brániť pred phishing/vishing útokmi pri práci s internet bankingom?

Akými najčastejšími spôsobmi sa môže pokúsiť útočník získať Vaše údaje (napr. prihlasovacie meno a heslo do Internet bankingu)?

- telefonicky postupným presviedčaním o možnosti vyriešenia neexistujúceho a zvyčajne urgentného problému. Cieľom útočníka je získať Vaše osobné údaje, prihlasovacie meno a heslo, prípadne iné zneužiteľné informácie (napr. údaje z platobnej karty).
- odosielaním nevyžiadaných emailov obsahujúcich vírusy a spyware, ktoré sú schopné sledovať Vašu činnosť na počítači, či dokonca odchytiť stlačenia kláves pri zadávaní prihlasovacích údajov nielen do Internet bankingu.
- odosielaním nevyžiadaných emailov, ktoré vizuálne pripomínajú komunikáciu z banky a požadujú vyplnenie falošných webových formulárov, prípadne falošnej prihlasovacej stránky, ktorá vyzerá ako prihlasovacia stránka internetového bankovníctva.

Ako sa chrániť pred pokusmi o získanie Vašich údajov pre prístup do Internet bankingu?

1. Nikdy neprezrádajte svoje identifikačné údaje (heslá, kódy, PINy ...). Banka nikdy nežiada citlivé identifikačné údaje od klienta e-mailom a ani telefonicky.
2. Pripájajte sa do Internet bankingu iba zo zabezpečených počítačov a sietí
 - s nainštalovaným a pravidelne aktualizovaným antimalware softvérom

- s nainštalovaným a pravidelne aktualizovaným antispymware softvérom
 - s automatickým preberaním a inštalovaním bezpečnostných aktualizácií operačného systému
 - s ochranou softvérovým alebo hardvérovým firewallom
3. Pre prístup do Internet bankingu používajte iba pravidelne aktualizované internetové prehliadače.
 4. Zapnite si vo svojom internetovom prehliadači službu na ochranu pred phishingovými útokmi a škodlivým softvérom (postup nájdete na stránkach jednotlivých výrobcov prehliadačov).
 5. Preberajte súbory iba z dôveryhodných zdrojov.
 6. Neotvárajte prílohy nevyžiadaných e-mailov alebo e-mailov od neznámych odosielateľov.
 7. Udržiavajte svoju domácu sieť bezpečnú.
 - kontaktujte pravidelne dodávateľa/predajcu Vášho internetového smerovača (modemu alebo routera) a uistite sa, že zariadenia Vašej domácej siete majú aktuálny a bezpečný softvér/firmvér.
 - preverte si, že na správu modemu/routera Vašej siete je použité silné heslo dostatočnej dĺžky. Slabé heslo na správu domácej siete výrazne uľahčuje útočníkom ovládnutie Vašej komunikácie s internetom.
 8. Nepodceňujte vynaliezavosť útočníkov a pred každým prihlásením do Internet bankingu si overte, že adresa do Internet bankingu začína <https://my.365.bank/> a adresa s prihlasovacím formulárom do Internet bankingu začína na <https://sso.365.bank/> bez akýchkoľvek ďalších znakov, ako sú napríklad _ - ? , opakujúcich sa písmen a iných odlišností.

Základné pojmy

Phishing – podvodný email, ktorý vyzerá akoby ho zaslala banka. Písaný väčšinou zdvorilo a v záujme klienta. Môže obsahovať aj vírus.

Vishing – (kombinácia slov voice-over fishing, t.j. lovenie „prostredníctvom hlasu“) - je podvodný postup s využitím telefonického rozhovoru, pomocou ktorého sa útočník snaží od klienta získať citlivé údaje (osobné údaje, prístupové heslá do internet bankingu, čísla platobných kariet a pod.)

Pharming – podvodne vytvorená webová stránka podobajúca sa na originálnu stránku banky.

Social engineering – podvodné telefonáty, pri ktorých volajúci predstiera, že pracuje v banke a snaží sa získať citlivé identifikačné údaje od klienta.

Vírus, malware, spyware – škodlivý kód resp. program, ktorý poškodzuje funkčnosť PC. Môže sťahovať a odosielať citlivé údaje z PC cudzej osobe, alebo zašifrovať vaše dáta.

V prípade akéhokoľvek podozrenia okamžite kontaktujte banku na **0850 365 365**, resp. **hello@365.bank**.