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 neprezrádzajte svoje identifikačné údaje (heslá, kódy, PINy, ...)
2. Banka NIKDY nežiada citlivé identifikačné údaje od klienta mailom a ani telefonicky
3. NIKDY neukladajte svoje heslá do pamäti počítača.
4. Používajte len overené a chránené PC. Počítač chráňte nainštalovaním aktuálnych verzií antivírusových a antispyware programov, firewallom.
5. NIKDY nepoužívajte ľahko uhádnuteľné heslá.

VŽDY si overte či komunikujete priamo s bankou:

1. Overte v prehliadači, či adresa prihlasovacej stránky v prehliadači začína "https://my.365.bank/#/login"
2. Overte, či je prihlasovacia stránka zabezpečená šifrovaním, čo indikuje obrázok "zámočku"
3. Overte platnosť šifrovacieho certifikátu kliknutím na "zámoček" a skontrolovaním vydavateľa GeoTrust a cieľového servera 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 často neexistujúceho problému. Cieľom útočníka je získať Vaše osobné údaje, prihlasovacie meno a heslo, prípadne iné zneužiteľné informácie.
- odosielaním nevyžiadaných emailov obsahujúcich vírusy a spyware schopný sledovať Vašu činnosť na počítači, prípadne požadovaním vyplnenia falošných webových formulárov.
- odosielaním nevyžiadaných emailov obsahujúcich vírusy a spyware schopný sledovať Vašu činnosť na počítači, prípadne požadovaním vyplnenia falošných webových formulárov.

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

1. Nikdy neprezrádzajte 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 z zabezpečených počítačov
   - s nainštalovaným a pravidelne aktualizovaným antivírusovým softvérom
   - s nainštalovaným a pravidelne aktualizovaným antispyware softvérom
   - s automatickým preberaním a inštalovaním bezpečnostných aktualizácií operačného systému
   - s povoleným softvérovým alebo hardvérovým firewallom
3. Pre prístup do Internet bankingu používajte iba pravidelne bezpečnostne aktualizované internetové prehliadače.
4. Zapnite vo svojom internetovom prehliadači službu na ochranu pred phishingovými útokmi a škodlivým softvérom
   - v Internet Explorer-e 10 a vyššom cez menu Bezpečnosť/Filter SmartScreen/Zapnúť filter SmartScreen
   - v Firefox 28 a vyššom cez menu Nástroje/Možnosti/záložka Bezpečnosť vybrať voľby "Blokovať nahlásené útočné stránky" a "Blokovať nahlásené podvodné stránky"
   - v prehliadači Google Chrome 34 a vyššom cez menu Nastavenia/linka zobraziť Rozšírené nastavenia/sekcia Súkromie vybrať voľbu "Povoliť ochranu pred phishingom a malware"
5. Preberajte súbory iba z dôveryhodných webov.
6. Neotvárajte prílohy nevyžiadaných e-mailov.
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/ 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, spyware – škodlivý kód resp. program, ktorý poškodzuje funkčnosť PC. Môže sťahovať a odosielať citlivé údaje z PC cudzej osobe.

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