3

TEXT 1

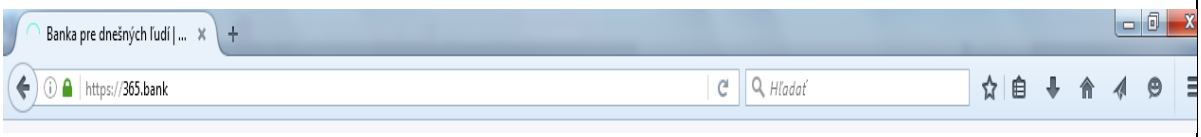
Nenechajte sa nachytať

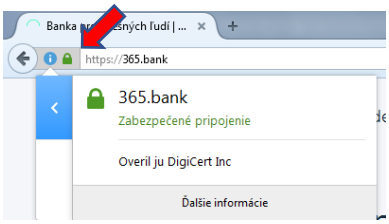
Sú naše peniaze v bankách bezpečné?

Je mobilné a online bankovníctvo bezpečné? Neprídem o svoje peniaze? Ako nenaletieť podvodníkom? Otázka bezpečnosti, pokiaľ ide o peniaze, je dôležitá a, prirodzene, zaujíma každého. Odpoveď na ňu je pomerne jednoznačná. Áno, mobilné bankovníctvo je dostatočne bezpečné. Samozrejme treba dodať, že samotná miera bezpečnosti závisí od nás, klientov. Podvodníci môžu byť všade okolo nás, na ulici, v pobočke, na zastávke, v online priestore, ale aj kdekoľvek inde.

Čo robia banky pre bezpečnosť klientov?

Banky robia pre bezpečnosť svojich klientov **všetko**. Používajú účinné technológie, šifrujú dáta, overujú klientov. Bankové systémy sú chránené účinnými bezpečnostnými bránami, tzv. firewall. Používajú zariadenia na autentifikáciu, notifikácie prostredníctvom SMS-správ či e-mailov a elektronické osobné kľúče s najvyšším stupňom ochrany. Pre klienta je dôležité overiť si, či je webová stránka zabezpečená bezpečnostným certifikátom SSL, a to prostredníctvom URL adresy. V riadku s adresou sa zobrazí na začiatku adresy protokol **https** (Hyper Text Transfer Protocol Secure).





Detaily certifikátu, vrátane názvu spoločnosti majiteľa stránky možno zobraziť kliknutím na symbol „zámku“ na lište prehliadača. Banka chráni vaše dáta pred nepovoleným prístupom tak, že ich zašifruje pred schválením na odoslanie.

Čo môžete urobiť pre svoju bezpečnosť vy?

Je veľmi dôležité, aby ste chránili svoje zariadenia, svoju identitu a aby ste pristupovali do služieb elektronického bankovníctva cez bezpečné pripojenia a cez siete, ktoré chránia vás i vaše transakcie pred možným sledovaním.

1. **Chráňte svoje zariadenia:**
   Váš počítač, notebook, tablet či mobilný telefón by mali mať pravidelne inštalované bezpečnostné aktualizácie. Chráňte tiež svoje internetové spojenie. Ak sa plánujete od počítača či mobilného zariadenia vzdialiť, nastavte si heslo a čas automatického zablokovania obrazovky.

2. **Používajte bezpečné pripojenia:**
   - Chráňte svoju bezdrôtovú sieť,
   - keď používate služby elektronického bankovníctva, nepoužívajte verejný počítač. Na žiadnej službe, ktorou otvárate účet, nezostávajte prihlásený na verejne prístupnom počítači.
   - nenahrávajte si do počítača programy z neznámych zdrojov a neinštalujte si do internetového prehliadača neznáme rozšírenia (tzv. „pluginy“),
   - buďte opatrní pri otváraní príloh alebo neznámych odkazov a e-maily od neznámych osôb vôbec neotvárajte,
   - ak dostanete elektronickú poštu alebo sa na obrazovke otvorí nové okno (tzv. „pop-up“ okno), kde máte uviesť svoje osobné, autorizačné alebo finančné údaje, neodpovedajte na tento e-mail a v otvorenom okne nevypĺňajte žiadne údaje,
   - hľadajte znaky odlišnosti ako napr. nemoderný dizajn, pravopisné a iné chyby,
   - ak sa chcete dostať na stránku internetového bankovníctva, adresu píšte na klávesnici, v žiadnom prípade nekopírujte linku zo správy, ani tú, ktorá sa otvorila v novom okne. Útočník dokáže vytvoriť stránku, ktorá je svojím vzhľadom veľmi podobná originálnej stránke banky. V skutočnosti vás však presmeruje na inú stránku bez toho, aby ste si to všimli.

3. **Chráňte svoju identitu a bankové účty:**
   - Nikdy nezverejňujte ďalším osobám svoje osobné údaje, na základe ktorých by vás bolo možné identifikovať,
   - nikomu (ani rodinným príslušníkom či neznámym osobám vydávajúcim sa za zamestnancov banky) neposkytujte svoje osobné identifikačné údaje do systémov, aplikácií, elektronických služieb, ku kartám (ako napr. prihlasovacie meno, heslo, PIN kódy, bezpečnostné kódy, čísla platobných kariet, kontrolné kódy a i.),
   - nikdy neprezraďte iným osobám vaše bankové informácie o vašom účte, prihlasovacie údaje, kódy pre služby elektronického bankovníctva alebo pre platobné karty.
   - pravidelne si meňte vaše heslo pre služby elektronického bankovníctva a nepoužívajte rovnaké bankové heslo v iných menej citlivých aplikáciách a internetových stránkach (najmä nie na sociálnych sieťach).
   - pri vytváraní hesla použite kombináciu čísiel, veľkých a malých písmen (bezpečnosť hesla znižuje napr. uvedenie svojho mena a priezviska, dátumu narodenia a pod.).

4. **Zabezpečte svoje mobilné zariadenie:**

- ☞ nepožičiavajte mobilné zariadenie cudzím ľuďom a nenechávajte ho bez dozoru,
- ☞ udržiavajte svoje mobilné zariadenie v aktualizovanom a bezpečnom stave,
- ☞ neinštalujte si do mobilných zariadení neoverené a nedôveryhodné aplikácie. Na komunikáciu s bankou používajte len aplikácie, ktoré banka odporúča,
- ☞ prístupové údaje k službám elektronického bankovníctva si neukladajte do mobilného zariadenia

Čo robiť v prípade problémov?

Dostali ste podozrivý e-mail? Máte zablokované konto do internetbankingu? V tom prípade kontaktujte klientské centrum svojej banky telefonicky, e-mailom alebo kontaktným formulárom! Opatrnosti nie je nikdy dosť.

Situácie, s ktorými sa môžete stretnúť:

- chcete zmeniť prihlasovacie heslo,
- dostali ste podozrivý e-mail,
- klikli ste na podvodný odkaz v e-maile,
- vyplnili ste údaje na podvodnej stránke,
- prezradili ste podozrivej osobe údaje o svojom účte,
- máte zablokované konto do Internetbankingu,
- zverejnili ste údaje o svojej karte,
- máte podozrenie na zneužitie údajov o vašom účte,
- prišli vám na účet peňažné prostriedky, ktorých pôvod vám je neznámy.

ÚLOHA

a) Rozhodnite, či v uvedených prípadoch ide o podvod, alebo nie. Odpoveď označte krížikom v tabuľke.
b) Svoju odpoveď potom stručne zdôvodnite.

	Je to podvod alebo nie?	ÁNO	NIE
1.	Dostali ste e-mail z neznámej banky, že ste vyhrali vysokú sumu, ale vy o tejto banke nič neviete.		
2.	Bývate na internáte a dostali ste mail od mamy, v ktorom vám oznamuje, že vám poslala na účet 50 €, aby ste mohli zaplatiť za internát.		
3.	Dostali ste list, v ktorom vám oznamuje neznáma inštitúcia, že ste vyhrali 50 000 €, ale vy ste s nimi nikdy nekomunikovali.		
4.	Požiadali vás e-mailom so žiadosťou o zaslanie prístupových údajov k vášmu účtu. Ak tak urobíte a pošlete sumu na uvedený účet 100 € na registráciu, pošlú vám výhru na váš účet.		
5.	Dostali ste sms správu, že máte urýchlene kontaktovať danú banku prostredníctvom daného 6-ciferného kódu, lebo na účte prebehla podozrivá transakcia. Vy však v tejto banke nemáte účet.		
6.	Chcete si kúpiť elektronicky letenku do Paríža, ale pri platbe musíte zadať číslo vašej platobnej karty, dátum platnosti a CVC kód, ktorý sa nachádza na zadnej strane karty.		
7.	Na vaše súkromné telefónne číslo sa ohlásila neznáma osoba, že ste vyhrali peňažnú cenu. Volajúca osoba vás veľmi presvedčivo pozýva na stretnutie v miestnej reštaurácií, pozvánka je aj s obedom a možnosťou získať ďalšie dary a výhody.		
8.	Neskoro večer vám na mobil zavolá neznáma osoba, že váš otec mal vážnu haváriu a na prevoz záchranárskym vrtuľníkom potrebujete súrne zaplatiť sumu 100 €. Oznámi vám, že pre sumu príde kuriér z nemocnice.		
9.	Zaregistrovali ste na podujatie a od organizátora vám príde e-mail, že máte za vstupenku zaplatiť prostredníctvom platobnej karty registračný poplatok 29,90 €.		
10.	Organizácia, ktorá vás oslovila, že ste vyhrali nejakú cenu, poskytuje len svoje P. O. Box číslo, ale neudáva adresu.		

11.	Na zábavnom podujatí ste si kúpili lístok v tombole. Pri losovaní oznámili číslo a kód vášho lístka, že ste vyhrali cenu.		
12.	Kúpili ste si stierací žreb a našli ste 3 rovnaké symboly, na základe ktorých idete do ďalšieho zlosovania, ale musíte poslať korešpondenčný lístok alebo sa prihlásiť na adrese udanej na lístku.		
13.	V lotérii ste podali žreb s vyplnenými číslami a pri losovaní vytiahli 5 platných čísel, ktoré máte na žrebe.		
14.	Neznámy človek vás požiadal, aby ste mu požičali mobil, že súrne potrebuje kamarátovi poslať nejakú dôležitú sms-správu. Vy však máte v mobile uložené prístupové údaje k svojmu účtu, aby ste ich nezabudli a mali ich vždy k dispozícii.		

3 – RIEŠENIE

1. Áno – cudzie banky nemajú vaše údaje a banky nekomunikujú s klientami prostredníctvom mailov
2. Nie – poznáte mailovú adresu vašej mamy a takýto postup máte zaužívaný
3. Áno – ide o jasný podvod s cieľom získať od vás citlivé údaje
4. Áno - ide o jasný podvod s cieľom získať od vás citlivé údaje
5. Áno – ide o jasný podvod s cieľom získať od vás citlivé údaje
6. Nie – je to bežný postup v prípade, že kupujete letenku cez oficiálnu stránku leteckej spoločnosti
7. Áno – snaha získať od vás citlivé údaje
8. Áno – takýmto spôsobom sa mimoriadna zdravotná starostlivosť neuhrádza a výdavky s ňou spojené sa hradia až po ukončení transportu
9. Nie – ak je v pozvánke na podujatie uvedený registračný poplatok
10. Nie – seriózna firma musí mať uvedené presnú adresu sídla firmy
11. Nie – výhru si prevezmete na podujatí
12. Nie – je to možné
13. Nie – ak je oficiálne žrebovanie overené notárom
14. Áno – je veľké riziko, že budú zneužité vaše osobné údaje

POUŽITÉ ZDROJE:

Spracované podľa: Finančná gramotnosť v kocke, dostupné na https://bit.ly/33yZoYx