Desatero bezpečného internetového bankovnictví

Při dodržování zásad desatera bezpečného internetového bankovnictví minimalizujete riziko jeho zneužití.

1. **Počítač**: operační prostředí počítače nebo notebooku (ve většině případů Windows) je potřeba pravidelně aktualizovat. Velmi doporučujeme instalovat některý z antivirových programů a zapnout firewall Windows. Při aktualizacích nezapomínejte i na instalované aplikace a internetový prohlížeč včetně jeho doplňků.
   Překlad ZDE

2. **Programy**: promyslete, zda na počítači, na kterém provozujete internetové bankovnictví, musíte mít instalované rizikové programy (např. Adobe reader) nebo Javu, která je velkým zdrojem zranitelnosti.
   Překlad ZDE

3. **Chytré telefony a tablety:** pro přenosná zařízení s operačním prostředím Android také instalujte antivirovou ochranu, mnohem důležitějším pravidlem je ale stahování a instalace aplikací pouze z oficiálního tržiště Google Play. Buďte velmi pozorní, jaká přístupová práva aplikace při instalaci vyžaduje, a to zvláště v případech, kdy žádá např. přístup k vašim kontaktům či službám zařízení – fotoaparátu nebo kameře. Pokud banka nabízí vlastní aplikaci na mobilní prostředí, instalujte ji.
   Překlad ZDE

4. **Internetový odkaz (adresa) internetového bankovnictví:** při vstupu do prostředí elektronického bankovnictví nikdy neklikejte na cizí odkazy, adresu zadávejte do adresního řádku vždy ručně, nebo použijte vytvořenou záložku. Většina bankovních domů provozuje internetové bankovnictví na zabezpečené stránce, jejíž adresa začíná zkratkou https://, ve většině moderních verzí prohlížečů se adresa v adresním řádku zobrazí zeleně anebo se celé pole adresního řádku vybarví zeleně.
   Překlad ZDE

5. **Platný certifikát:** pokud není něco v pořádku s platností certifikátu bezpečného připojení k aplikaci internetového bankovnictví, zobrazí se bezpečnostní upozornění.
   Překlad ZDE

6. **Pečujte o svá hesla:** pro přístup do internetového bankovnictví volte dostatečně silné heslo. To je takové heslo, které je kombinací písmen, číslic a speciálních znaků (např. *@*, *$*, *&*). Své heslo pravidelně měňte. Nepoužívejte triviální hesla, což jsou jména nebo obecné názvy (např. *heslo*, *banka*, *peníze*) a jednoduché číselné kombinace (*1234*, *1111*…). Taková hesla se dají velmi snadno prolomit např. použitím tzv. slovníkového útoku.
   Překlad ZDE

7. **Kódy mTAN:** před potvrzením finanční transakci nebo jiné operace v prostředí internetového bankovnictví si vždy v příchozí SMS ověřte, zda především částka a číslo cílového účtu odpovídají vámi zadaným datům z internetového bankovnictví.
   Překlad ZDE

8. **Pravidelná kontrola:** v pravidelných intervalech, alespoň jednou týdně, kontrolujte, zda na vašem účtu neproběhla podezřelá aktivita a transakce, které jste nezadali. Pokud je to možné, zkuste občas provést kontrolu svého účtu z prostředí jiného bezpečného PC.
   Překlad ZDE

9. **Riziko veřejných sítí:** nepoužívejte internetové bankovnictví v prostředí nezabezpečených sítí, např. veřejných WiFi v kavárnách, hotelových pokojích nebo čerpacích stanicích.
   Překlad ZDE

10. **Nouzové kontakty:** uložte si pro každý případ nouzové kontakty na vaši banku, důležitá telefonní čísla a e-maily. V případě jakýchkoliv pochybností okamžitě kontaktujte banku a poraďte se.
    Překlad ZDE

ORBI PONTES, z.s.

Spolek vedený Městského soudu v Praze ve spolkovém rejstříku pod spisovou značkou L 24448.

Pravidelně na konci září pořádáme celorepublikový festival Týden komunikace osob se sluchovým postižením (TKOSP).

Šíříme osvětu v oblasti sluchového postižení, informace o simultánním přepisu a tlumočení do znakového jazyka, bořímе mýty o komunikaci s lidmi se sluchovým postižením.

Více na www.orbipontes.cz a facebookovém profilu.

Do českého znakového jazyka přeložila Pavlína Spilková, vyrobili: Deaf Friendly 2016.