

## Zásady bezpečného užívání Internet Banky

Společnost Wüstenrot (dále jen Banka) vyvíjí snahu o zajištění maximálně bezpečného provozu Internet Banky (dále jen IB). Rizikem při užívání IB se může stát zejména nedostatečné zabezpečení počítače, na němž uživatel IB využívá, případně nedostatečné utajení bezpečnostních prvků, kterými jsou přihlašovací jméno (tj. klientské číslo), heslo a mobilní klíče, a z toho plynoucí možnost jejich zneužití ze strany jiných osob.

Vzhledem k tomu, že osoba zodpovědná za zabránění zneužití dat potřebných pro používání IB je především uživatel, důrazně doporučujeme přečíst si a postupovat dle následujících informací týkajících se bezpečnosti dat a jejich ochrany před zneužitím ze strany třetí osoby. Nedodržení níže uvedených pravidel může usnadnit vznik škody, proto je nezbytné je dodržovat. Uváděná pravidla jsou však pravidly základními a možností ochrany je více.

### Hesla

Heslo je bezpečnostní osobní prvek a obecný prostředek k autentizaci uživatele. Základní doporučení pro uživatelské heslo:

- Pro heslo jsou zcela nevhodná jednoduchá slova nebo jejich obměny, data narození, jména partnerů, dětí, psů aj. Takové heslo lze odhalit pomocí tzv. slovníkového útoku nebo informovaného útočníka.
- Heslo si nikam nezaznamenávejte. Zcela nevhodný je záznam na papírky, do počítače, v peněžence, do diáře, v telefonu. V počítači nikdy nepovolujte zapamatování hesla. Heslo nikomu nesdělujte, a to ani nejbližším příbuzným. Nezasílejte heslo před jinou osobou.
- V případě, že si přece jen chcete důvěrné údaje poznamenat, uložte je do trezoru nebo jiné místo, kam máte přístup pouze Vy.
- Heslo pravidelně měňte. Nikdy neměňte heslo na jiném formuláři, než v sekci „**Změny a nastavení**“. Banka po Vás v žádném případě nebude vyžadovat jiný postup (telefonicky, elektronicky ani osobně), proto na jakékoli takové výzvy nereagujte a případně na ně Banku upozorněte.
- Nezasílejte heslo ani jiné údaje k účtu pomocí elektronické pošty nebo sms, nezasílejte je na jiné internetové stránce, než na stránce určené k přihlášení k IB.
- Banka Vás nikdy nepožádá o Vaše důvěrné informace (např. heslo pro přihlášení do IB) prostřednictvím e-mailové korespondence. Proto nikdy nereagujte na případné e-mailové zprávy, které Vás žádají o poskytnutí Vašich osobních dat, jedná se o tzv. Phishing. **Banka Vám nebude zasílat takový druh zpráv.**
- Heslo k IB nikdy nepoužívejte jinde (např. pro přístup k e-mailu, k sociálním sítím apod.).

### Ověření webových adres

Pro zajištění bezpečnosti je nutné, abyste byli vždy přesvědčeni, že komunikujete se serverem Banky. Kontrolujte na stránkách řádek pro zadání internetové adresy. Vždy se přesvědčte, že se jedná opravdu o stránku, kterou požadujete zobrazit, že nebyla přesměrována na jinou stránku. Komunikace se serverem je zabezpečená pomocí SSL protokolu, který zajišťuje bezpečný přenosu dat přes internet pomocí šifrování. Stránku zabezpečenou pomocí protokolu SSL poznáte podle toho, že webová adresa obsahuje prefix <https://> a v prohlížeči je ve stavové liště zobrazen symbol uzavřeného zámku.

- Pro přihlášení k IB využívejte oficiální stránky společnosti <http://www.wuestenrot.cz/> nebo přímo na adrese <https://internetbanka.wuestenrot.cz/>. Komunikace je zabezpečena certifikátem s těmito údaji: vystaveno pro - internetbanka.wuestenrot.cz, vystavitel - thawte Extended Validation SSL CA.
- Pokud při přihlašování nebo při využívání služeb IB budete mít jakékoliv pochybnosti, kontaktujte prosím neprodleně asistenční klientskou linku Banky na telefonním čísle 800 225 555.

### Počítač

Pro práci se službami IB používejte pouze bezpečné počítače, které máte plně pod kontrolou, tzn. máte možnost ovlivnit jejich bezpečnostní nastavení.

- Pravidelně sledujte a instalujte opravy vydávané výrobcí operačních systémů, které odstraňují některé jejich chyby a omezují bezpečnostní rizika.
- V případě, že používáte operační systém z rodiny Windows, doporučujeme zapnout automatickou aktualizaci systému. Na adrese <http://www.microsoft.com/cze/security/protect/> jsou také popsány základní kroky k zabezpečení systému.

- V žádném případě nedoporučujeme používat k přístupu k IB počítače, o kterých nic nevíte, tj. například v internetových kavárnách.
- Neinstalujte si do počítače software z nedůvěryhodných zdrojů.

### **Bezpečnostní programy**

Používejte programy, které umí ochránit počítač, jako jsou antivirové programy, anti-spyware programy a firewall.

- Vždy mějte na svém počítači nainstalovaný antivirový program, který zvyšuje ochranu před škodlivými programy. Stejně tak je vhodné používat anti-spyware program, jehož úkolem je odstraňovat či blokovat spyware (program, jež se bez vědomí uživatele může dostat do jeho počítače a který využívá internetu k odesílání dat z počítače). Antivirový a anti-spyware program pravidelně aktualizujte.
- Připojte se k internetu přes firewall, což je program nebo technické zařízení, které minimalizuje rizika neoprávněného přístupu k počítači z internetu. Firewall zpracovává pouze uživatelem povolené dotazy do internetu a všechna ostatní potenciálně nebezpečná data odfiltruje.

### **Další doporučení**

- Veškeré tištěné podklady, které jste obdrželi od Banky uchovejte na bezpečném místě.
- Neotvírejte e-mailové zprávy od odesílatelů, které neznáte nebo zprávy s podezřelým názvem či obsahem.
- Navštěvujte na internetu pouze známé a důvěryhodné stránky a neklikejte na odkazy v podezřelých e-mailech. Vyvarujte se stahování neznámých souborů z internetu na počítač, které mohou společně se svým původním účelem nainstalovat i nebezpečné programy. Zejména stránky s erotickým obsahem a nelegálním software obsahují spyware a viry, které mohou infikovat počítač a následně provádět činnost, kterou nemáte pod kontrolou.