

Bezpečnostní pokyny užívání internetového bankovníctví

1 Zásady bezpečného chování na internetu a v internetovém bankovníctví (dále jen IB)

- Ujistěte se, že jste na oficiálních stránkách společnosti.
- Jsme schopni zajistit Vaši bezpečnost pouze na našich oficiálních stránkách díky šifrování komunikace.
- Do internetového bankovníctví se přihlašujte pouze přes oficiální www stránky.
- Další informace najdete na stránce www.citfin.cz

1.1 Hesla - základní informace k bezpečnosti

- Heslo si nikam nezaznamenávejte, neprozrazujte ho dalším osobám a pravidelně jej měňte.
- Heslo ideálně nesmí obsahovat standardní slovo, jméno, apod. Nejlepší je kombinace alfanumerických znaků.
- Přístupové heslo do internetového bankovníctví nesdělujte po telefonu, nezasílejte e-mailem

1.2 Internetové bankovníctví - základní informace k bezpečnosti

- Do internetového bankovníctví se přihlašujte pouze přes oficiální www stránky www.bankservis.cz
- Dodržujte bezpečnostní zásady vztahující se k Vaším přístupovým údajům, heslům.
- Nezapůjčujte Váš mobilní telefon a nenechávejte ho bez dozoru.

1.3 Všeobecné informace, E-mailová komunikace

- Operátor NIKDY nevyžaduje heslo do internetového bankovníctví.
- Společnost Citfin NIKDY neposílá údaje o změně hesla emailem, NIKDY nepožaduje jiné ověření prostřednictvím emailu.
- Pro korespondenci s Vámi využívá společnost Citfin výhradně adresu info@citfin.cz
- Společnost Citfin NIKDY nezasílá odkazy na stránky s logováním do internetového bankovníctví Bankservis.
- Společnost Citfin NIKDY nevyžaduje zaslání nebo potvrzování identifikace klienta, hesel ani PIN k platební kartě

1.4 Mobilní telefony

- Společnost Citfin NIKDY nezasílá na mobilní telefon klienta žádné bezpečnostní ani jiné certifikáty, které byste museli instalovat.
- Společnost Citfin NIKDY nežadá o instalaci certifikátů nebo bezpečnostních aplikací v mobilních telefonech.

2 Základní informace k bezpečnosti vašeho počítače

- Dbejte na aktualizace internetových prohlížečů.
- Používejte programy proti škodlivému kódu, tedy antivirové SW a pod.
- Provádějte pravidelné aktualizace operačního systému.
- Nestahujte podezřelé programy, nelegální kopie (warez) či aplikace umožňující nelegální využívání programů (cracky)
- Chraňte svůj počítač před neoprávněnými zásahy cizích osob.
- Používání programů ke sdílení souborů (P2P, torrenty) je bezpečnostním rizikem a mělo by být spojeno s vaší zvýšenou ostražitostí.
- Pro přihlášení k Vašemu počítači používejte pokud možno silné heslo, nebo jinou standardní metodu, např. otisk prstu, nebo hardwarové klíče pro přihlášení.

2.1 Internetový prohlížeč MS Internet Explorer

Pokud pro svou práci používáte aplikaci Microsoft Internet Explorer, zde uvádíme jednu z možností jeho bezpečného nastavení:

Otevřete si aplikaci Microsoft Internet Explorer, (pokud se Vám nezobrazuje nabídka Menu, stiskněte klávesu Alt, nabídka se dočasně zobrazí)

- Nástroje -> Možnosti internetu -> Obsah -> Automatické dokončování -> možnosti **Formuláře a Uživatelská jména a hesla na formulářích by neměly být zaškrtnuty**
- Nástroje -> Možnosti internetu -> Obecné -> Dočasné soubory internetu -> Nastavení -> **zadejte možnost Zjišťovat existenci novějších verzí uložených stránek – při každé návštěvě stránky**
- Nástroje -> Možnosti internetu -> Upřesnit -> část Zabezpečení: **zaškrtnutá volba „Neukládat šifrované stránky na disk“ a nezaškrtnutá volba v části Procházení: Povolit rozšíření prohlížeče třetích stran**

Informace o aktualizaci (většinou probíhá automaticky) a nejnovějších verzích prohlížeče se dovíte na stránkách <http://www.microsoft.com> Dále je možné použít aplikaci Windows Update. (Na operačním Systému Windows XP/Vista/7 použijete volbu Start->Všechny programy-> Automatické aktualizace pro verzi OS Windows 7, pro předchozí OS použijte volbu Start->Windows Update, nebo Microsoft Update.

Pokud používáte OS Windows XP, zcela jistě víte, že podpora tohoto operačního systému včetně vestavěné verze MS IE bude v roce 2014 ukončena!

2.2 Internetový prohlížeč Mozilla Firefox

Pokud pro svou práci používáte aplikaci Mozilla Firefox, zde uvádíme jednu z možností jeho bezpečného nastavení:

- Nástroje -> Možnosti -> Soukromí -> Historie: **možnost Pamatovat si údaje ve formulářích a vyhledávacím poli by neměla být zaškrtnuta**
- Nástroje -> Možnosti -> Zabezpečení -> Hesla: **možnost Pamatovat si na serverech hesla by neměla být zaškrtnuta**

Informace o aktualizaci (většinou probíhá automaticky) a nejnovějších verzích prohlížeče se dovíte na stránkách <http://www.czilla.cz>

2.3 Operační systém Windows obecně

Uživatelům operačního systému MS Windows doporučujeme sledovat varování a informace aplikace **Centrum bezpečnosti** počítače, případně navštívit internetovou stránku <http://www.microsoft.com/cze/security> a řídit se zde publikovanými doporučeními.