Bezpečnostní pokyny užívání internetového bankovnictví

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

- Ujistěte se, že jste na oficiálních stránkách společnosti.
- Vaši bezpečnost Jsme schopni zajistit pouze na našich oficiálních stránkách, a to díky šifrování komunikace.
- Do internetového bankovnictví se přihlašujte pouze přes oficiální www stránky.
- Další informace najdete na stránce www.rondafinance.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 bankovnictví nesdělujte po telefonu, nezasílejte e-mailem

1.2 Internetové bankovnictví - základní informace k bezpečnosti

- Do internetového bankovnictví se přihlašujte pouze přes oficiální www stránky https://ib.rondafinance.cz.
- Dodržujte bezpečnostní zásady vztahující se k Vašim 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 bankovnictví.
- Společnost RONDA FINANCE NIKDY neposílá údaje o změně hesla emailem, ani NIKDY nepožaduje jiné ověření prostřednictvím emailu.
- Pro korespondenci s Vámi využívá společnost RONDA FINANCE výhradně adresu helpdesk@rondafinance.cz.
- Společnost RONDA FINANCE NIKDY nezasílá odkazy na stránky s logováním do internetového bankovnictví Bankservis.
- Společnost RONDA FINANCE NIKDY nevyžaduje zaslání nebo potvrzování identifikace klienta, sdělení hesla nebo PIN kódu k platební kartě.

1.4 Mobilní telefony

- Společnost RONDA FINANCE NIKDY nezasílá na mobilní telefon klienta žádné bezpečnostní ani jiné certifikáty, které byste museli instalovat.
- Společnost RONDA FINANCE NIKDY nežádá 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 apod.

- 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 nastránkách 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.

3. Podpora uživatelů

V případě jakýchkoliv dotazů klientů ohledně bezpečnosti, a také pro hlášení podezření na narušení bezpečnosti nebo na podvodné jednání, jsou klientům k dispozici pracovníci call centra na emailu helpdesk@rondafinance.cz nebo na telefonu +420 234 768 990, kteří poskytnou asistenci nebo radu v oblasti bezpečnosti informací, případně zajistí pomoc od bezpečnostního manažera RONDA FINANCE.

V případě, že jsou identifikovány akutní nové hrozby, bezpečnostní manažer RONDA FINANCE prostřednictvím portálu internetového bankovnictví upozorňuje klienty na nebezpečí a vhodná opatření.