UPOZORNĚNÍ NA BEZPEČNOSTNÍ RIZIKA SOUVISEJÍCÍ S POUŽÍVÁNÍM INTERNETBANKINGU

Bezpečnostní upozornění související s využíváním Internetbankingu

1. V souvislosti s poskytováním služeb elektronických komunikací, si Vás dovolujeme informovat o některých bezpečnostních rizicích s tím spojených a upozornit Vás na základní možnosti, kterými můžete Vy, jako uživatel, ochránit svoje osobní údaje, přihlašovací jméno a přístupové heslo do Internetbankingu, elektronický klíč, případně zaslaný sms kód, telefonní číslo a jiné důvěrné nebo citlivé údaje (dále také "důvěrné informace") a počítač před jejich zneužitím. Jde o základní pravidla, která je třeba dodržovat k ochraně Vašich důvěrných údajů a Vašeho počítače.

2. Banka je povinna na své náklady provést ve své sféře vlivu taková technická a organizační opatření za účelem zajištění bezpečnosti důvěrných údajů, která jsou s ohledem na obvyklá rizika porušení ochrany důvěrných údajů technicky možná a přiměřená.

3. Klient je povinen na své náklady provést ve své sféře vlivu taková opatření za účelem zajištění bezpečnosti důvěrných údajů, která jsou s ohledem na obvyklá rizika porušení ochrany důvěrných údajů technicky možná a přiměřená. Klient bere na vědomí rizika spojená s poskytováním služeb elektronických komunikací a zavazuje se dodržovat zejména níže uvedené preventivní opatření a postupy k zajištění bezpečnosti důvěrných údajů. Nedodržení těchto pravidel a opatření může vést k zneužití důvěrných údajů a ke vzniku škody klientovi nebo třetí osoby.

4. S ohledem na co nejvyšší ochranu důvěrných údajů a majetku klienta doporučuje banka, aby si klient sjednal s bankou autorizaci elektronických pokynů pomocí sms zpráv nebo autorizaci prostřednictvím elektronického podpisu a využíval pro zadávání svého hesla při přihlašování do Internetbankingu grafickou klávesnici.

Rizika plynoucí z poskytování služeb elektronických komunikací

1. Služby elektronických komunikací jsou poskytovány prostřednictvím datových případně telefonních linek (dále také "datové linky"), které neprovozuje banka, ale třetí osoba odlišná od banky. Zabezpečení těchto datových linek je mimo sféru vlivu banky a banka není proto schopna zcela zabránit všem možným rizikům zneužití důvěrných údajů v průběhu přenosu prostřednictvím datové linky. Při přenosu důvěrných údajů nelze proto zcela vyloučit riziko neoprávněného získání důvěrných informací třetí osobou (např. hrozba tzv. hackerů, interní rizika provozovatele datové sítě, tzv. Man in the middle, tj. odposlouchávání komunikace třetí osobou předstírající protistranu komunikace, odposlouchávání telefonických hovorů, podvržení dat apod.).

2. Některá rizika plynoucí z poskytování služeb elektronických komunikací mohou být také ve sféře vlivu klienta. Mezi tato rizika patří zejména nedostatečné zabezpečení počítače klienta, který je používán pro

přihlášení do Internebankingu a k podávání pokynů bance a dále nesprávné nakládání s důvěrnými údaji klientem a z toho plynoucí možnost jejich zneužití ze strany třetích osob.

3. Banka neodpovídá za případnou škodu klienta nebo třetích osob vzniklou zneužitím důvěrných informací neoprávněně získaných z datových linek mimo sféru vlivu banky, počítače klienta nebo v důsledku nesprávného nakládání s těmito údaji klientem, pokud nejde o případ porušení povinnosti na straně banky.

Preventivní opatření prováděná bankou

1. Banka provádí ve své sféře vlivu preventivní opatření snižující riziko zneužití důvěrných informací. Mezi tato opatření patří zejména šifrování veškerých dat (tj. např. uživatelské jméno a heslo do Internetbankingu), která jsou přenášena mezi počítačem klienta a serverem Fio. Veškerá data jsou šifrována standardem SSL 128bit. Šifrování přenášených dat výrazně snižuje možnost zjištění důvěrných údajů o klientovi třetí osobou při přenosu datovou linkou a jejich následné zneužití.

2. Banka dále umožňuje klientovi využívat další bezpečnostní prvky chránící přístup do Internetbankingu, mezi které patří možnost využití grafické klávesnice pro zadávání hesla při přihlašování do Internetbankingu, což snižuje riziko neoprávněného zjištění těchto údajů třetí osobou a možnost potvrzování pokynů elektronickým způsobem podávaných klientem podle komisionářské smlouvy formou sms zpráv na individuálně stanovené telefonní číslo klienta nebo formou elektronického podpisu.

Utajení důvěrných údajů

1. Chraňte své důvěrné údaje před zveřejněním a zneužitím.

2. Důvěrné údaje si nezaznamenávejte. Pokud si důvěrné údaje přesto poznamenáte, uschovejte je na místě, které není volně přístupné dalším osobám.

3. Neuvádějte důvěrné údaje tak, aby se dala spojit s příslušným účtem (např. napsání důvěrných údajů v dokladech spojených s účtem, automatické zapamatování přihlašovacího jména a hesla do Internetbankingu počítačem).

4. Nezadávejte důvěrné údaje před jinou osobou, nesdělujte důvěrné údaje jiným osobám, a to ani rodinným příslušníkům a osobám blízkým.

5. Vaše heslo stanovte nejlépe jako kombinaci čísel a velkých a malých písmen, bez osobního vztahu k Vám nebo osobám blízkým. Jednoduché heslo s osobními rysy je snáze odhalitelné. Jako heslo nepoužívejte svoje datum narození, rodné číslo, telefonní číslo, po sobě jdoucí číslice apod. Heslo pravidelně měňte. Nikdy neměňte heslo do Internetbankingu na jiném formuláři, než v záložce Globální nastavení v Internetbankingu. Banka po Vás v žádném případě nebude vyžadovat jiný postup. Prvotní heslo musíte změnit při prvním přihlášení do Internetbankingu. Platnost následujícího hesla je z bezpečnostních důvodů omezena na 365 dnů. Vyprší-li tato lhůta, budete při nejbližším přihlášení do Internetbankingu vyzváni k jeho změně.

6. Nezasílejte důvěrné údaje pomocí e-mailu nebo sms, nezadávejte je na jiné internetové stránce, než na stránce určené k přihlášení do Internetbankingu, a to ani v případě že obdržíte e-mail případně sms, která napodobuje výzvu, zejména od banky, k zaslání důvěrných údajů nebo jejich vyplnění na jiné internetové stránce. Banka Vám takový druh zpráv v žádném případě nebude zasílat.

Uložení elektronického klíče

1. Chraňte svůj elektronický klíč, který používáte při zadávání pokynů, proti jeho zneužití, zejména proti jeho odcizení, okopírování apod. Zneužitím Vašeho elektronického klíče může jiná osoba předstírat Vaši identitu a zadávat pokyny Vaším jménem. Zneužití elektronického klíče Vám může způsobit škodu.

2. Elektronický klíč instalujte pouze na počítač, o kterém víte, že je chráněn proti možným hrozbám plynoucím z připojení k datové síti. Neinstalujte elektronický klíč na počítač, který je veřejně přístupný.

3. Uchováváte-li elektronický klíč na jiném přenosném médiu, ukládejte toto médium na místo, kde nedojde k jeho zneužití, zejména odcizení, okopírování nebo poškození.

Preventivní opatření ve sféře vlivu klienta, zabezpečení počítače klienta

1. Internetbanking používejte pouze na počítačích, které jsou řádně zabezpečené proti zneužití důvěrných údajů. Nepoužívejte Internetbanking zejména v internetových kavárnách a na jiných veřejně přístupných počítačích, ani na počítačích, u kterých nemáte jistotu, že jsou zabezpečeny proti zneužití důvěrných údajů.

2. Před přihlášením do Internetbankingu se řádně přesvědčte, že komunikujete se správným poskytovatelem služby. Adresa serveru banky je http://www.fio.cz/. Při přihlašování do aplikace Internetbanking a při zadávání pokynů prostřednictvím aplikace Internetbanking řádně zkontrolujte, že spojení je zabezpečeno (ověřte platnost certifikátu SSL zabezpečení) a dále ověřte identifikaci serveru banky. V případě pochybností o tom, že komunikujete s bankou nebo, že spojení není řádně zabezpečeno, neprovádějte žádné úkony, které by mohly vést k prozrazení nebo zneužití důvěrných údajů a bezodkladně kontaktujte klientského pracovníka banky.

3. Počítač, na kterém se rozhodnete používat Internetbanking, zabezpečte legálním firewallem, antivirovou a anti-spyware ochranou, a tyto ochranné prvky pravidelně aktualizujte. Programy aktualizujte standardním způsobem. Pravidelně sledujte informace o nových hrozbách, virech, spyware apod. a v souladu s tím zajistěte ochranu Vašeho počítače.

4. Používejte legální a pravidelně aktualizovaný operační systém ve Vašem počítači. Pravidelně sledujte zprávy výrobce Vašeho operačního systému o opravách chyb a nedostatků tohoto operačního systému a tyto opravy včas instalujte do Vašeho počítače.

5. Používáte-li internetbanking na určitém počítači, vyvarujte se stahování a instalování programů, které lze volně získat na internetu, u nichž si nejste jisti, zda neobsahují viry nebo spyware, případně nepocházejí ze zdroje, který je důvěryhodný. Navštěvujte pouze známé, důvěryhodné a bezpečné stránky na internetu. Neotvírejte nevyžádané emaily, emaily od neznámých adresátů a emaily s podezřelým názvem nebo obsahem na takovém počítači. Takové emaily bez otevření smažte. Ve své emailové schránce používejte spam filter.

6. Žádná licenční ujednání u volně šířeného softwaru Vám nemohou poskytnout jistotu, že software neobsahuje součásti, které mohou Váš počítač poškodit či jinak narušit bezpečnost Vámi ukládaných údajů.

7. Pro získání základních informací o možnostech zabezpečení Vašeho počítače a o rizicích, která hrozí Vašemu počítači, si prosím přečtěte informace na stránkách: http://www.microsoft.com/cze/athome/security/default.mspx

Zabezpečení sms

1. Pro přijímání autorizačních sms kódů je nejdůležitější SIM karta, která obsahuje telefonní číslo, které jste určili k přijímání autorizačních sms kódů od banky (dále jen „SIM karta“). Tuto SIM kartu mějte vždy pod dohledem, telefon bez SIM karty neumožní komunikaci s bankou a autorizaci.

2. Mobilní telefon se SIM kartou, neponechávejte ležet na místech, kde nad ním nemáte dohled.

3. Vyvarujte se půjčování mobilního telefonu s vloženou SIM kartou, třetím osobám, aniž byste měli přehled o jejich nakládání s telefonem a zejména SIM kartou.

4. V případě, že hrozí riziko, že byste mohli ponechat telefon se SIM kartou mimo Váš dohled, znemožněte jeho používání třetím osobám kódem PIN. Tento kód uchovávejte v tajnosti a nesdělujte ho třetím osobám, ani si ho nikam nepoznamenávejte.

5. Autorizační kód doručený Vám bankou si nikam nepoznamenávejte a sms autorizačním kódem žádné osobě nezpřístupňujte.

6. V závislosti na technickém pokroku v oblasti funkcí mobilních telefonů zajistěte funkce svého telefonu proti možnosti automatického připojení třetí osoby k Vašemu telefonu.

Kontaktujte klientského pracovníka

V případě, že obdržíte e-mail s upozorněním na jakoukoli změnu ve způsobu přihlašování do Internetbankingu nebo s informací o změně www adresy přihlašovací stránky, nebo v případě, že zjistíte netypické nebo jinak podezřelé chování přihlašovací stránky, včetně automatického přesměrování, nebo jiné podezřelé skutečnosti, neprovádějte žádné úkony, které by mohly vést k prozrazení nebo zneužití důvěrných údajů a bezodkladně kontaktujte telefonicky klientské pracovníky banky a vyžádejte si radu ohledně dalšího postupu.