UPOZORNENIE NA BEZPEČNOSTNÉ RIZIKÁ SÚVISIACE S POUŽÍVANÍM INTERNETBANKINGU

Bezpečnostné upozornenia súvisiace s používaním Internetbankingu

1. V súvislosti s poskytovaním elektronických komunikačných služieb, si Vás dovoľujeme informovať o niektorých bezpečnostných rizikách s tým spojených a upozorniť Vás na základné možnosti, ktorými môžete Vy, ako užívateľ, ochrániť svoje osobné údaje, prihlasovacie meno a prístupové heslo do internetbankingu, elektronický kľúč, prípadne zaslaný SMS kód, telefónne číslo a iné dôverné alebo citlivé údaje (ďalej tiež "dôverné informácie") a počítač pred ich zneužitím. Ide o základné pravidlá, ktoré treba dodržiavať k ochrane Vašich dôverných údajov a Vášho počítača.

2. Banka je povinná na svoje náklady vykonať vo svojej sfére vplyvu také technické a organizačné opatrenia na zabezpečenie bezpečnosti dôverných údajov, ktoré sú s ohľadom na obvyklé riziká porušenia ochrany dôverných údajov technicky možné a primerané.

3. Klient je povinný na svoje náklady vykonať vo svojej sfére vplyvu také opatrenia za účelom zaistenia bezpečnosti dôverných údajov, ktoré sú s ohľadom na obvyklé riziká porušenia ochrany dôverných údajov technicky možné a primerané. Klient berie na vedomie riziká spojené s poskytovaním elektronických komunikačných služieb a zaväzuje sa dodržiavať najmä nižšie uvedené preventívne opatrenia a postupy na zabezpečenie bezpečnosti dôverných údajov. Nedodržanie týchto pravidiel a opatrení môže viesť k zneužitiu dôverných údajov a ku vzniku škody klientovi alebo tretej osoby.

4. S ohľadom na čo najvyššiu ochranu dôverných údajov a majetku klienta odporúča banka, aby si klient dohodol s bankou autorizáciu elektronických pokynov pomocou SMS správ alebo autorizáciu prostredníctvom elektronického podpisu a využíval pre zadávanie svojho hesla pri prihlasovaní do internetbankingu grafickú klávesnicu.

Riziká vyplývajúce z poskytovania elektronických komunikačných služieb

1. Elektronické komunikačné služby sú poskytované prostredníctvom dátových, prípadne telefónnych liniek (ďalej tiež "dátové linky"), ktoré neprevádzkuje banka, ale tretia osoba odlišná od banky. Zabezpečenie týchto dátových liniek je mimo sféru vplyvu banky a banka nie je preto schopná úplne zabrániť všetkým možným rizikám zneužitia dôverných údajov počas prenosu prostredníctvom dátovej linky. Pri prenose dôverných údajov nemožno preto úplne vylúčiť riziko neoprávneného získania dôverných informácií treťou osobou (napr. hrozba tzv. hackerov, interné riziká prevádzkovateľa dátovej siete, tzv. Man in the middle, tj odpočúvanie komunikácie treťou osobou predstierajúcou protistranu komunikácie, odpočúvanie telefonických hovorov, podvrhnutie dát a pod).

2. Niektoré riziká vyplývajúce z poskytovania elektronických komunikačných služieb môžu byť tiež vo sfére vplyvu klienta. Medzi tieto riziká patrí predovšetkým nedostatočné zabezpečenie počítača klienta, ktorý je

používaný pre prihlásenie do Internebankingu a podávanie pokynov banke a ďalej nesprávne nakladanie s dôvernými údajmi klientom a z toho plynúca možnosť ich zneužitia zo strany tretích osôb.

3. Banka nezodpovedá za prípadnú škodu klienta alebo tretích osôb vzniknutú zneužitím dôverných informácií neoprávnene získaných z dátových liniek mimo sféru vplyvu banky, počítača klienta alebo v dôsledku nesprávneho nakladania s týmito údajmi klientom, ak nejde o prípad porušenia povinnosti na strane banky.

Preventívne opatrenia vykonané bankou

1. Banka vykonáva vo svojej sfére vplyvu preventívne opatrenia znižujúce riziko zneužitia dôverných informácií. Medzi tieto opatrenia patrí najmä šifrovanie všetkých dát (tj napr. užívateľské meno a heslo do internetbankingu), ktoré sú prenášané medzi počítačom klienta a serverom Fio. Všetky dáta sú šifrované štandardom SSL 128bit. Šifrovanie prenášaných dát výrazne znižuje možnosť zistenia dôverných údajov o klientovi treťou osobou pri prenose dátovou linkou a ich následné zneužitie.

2. Banka ďalej umožňuje klientovi využívať ďalšie bezpečnostné prvky chrániace prístup do internetbankingu, medzi ktoré patrí možnosť využitia grafickej klávesnice pre zadávanie hesla pri prihlasovaní do internetbankingu, čo znižuje riziko neoprávneného zistenia týchto údajov treťou osobou a možnosť potvrdzovania elektronicky podávaných pokynov formou SMS správ na individuálne stanovené telefónne číslo klienta alebo formou elektronického podpisu.

Utajenie dôverných údajov

1. Chráňte svoje dôverné údaje pred zverejnením a zneužitím.

2. Dôverné údaje si nezaznamenávajte. Ak si dôverné údaje napriek tomu poznamenáte, uschovajte ich na mieste, ktoré nie je voľne prístupné ďalším osobám.

3. Neuvádzajte dôverné údaje tak, aby sa dala spojiť s príslušným účtom (napr. napísanie dôverných údajov v dokladoch spojených s účtom, automatické zapamätanie prihlasovacieho mena a hesla do internetbankingu počítačom).

4. Nezadávajte dôverné údaje pred inou osobou, neprezrádzajte dôverné údaje iným osobám, a to ani rodinným príslušníkom a blízkym osobám.

5. Vaše heslo stanovte najlepšie ako kombináciu čísiel a veľkých a malých písmen, bez osobného vzťahu k Vám alebo osobám blízkym. Jednoduché heslo s osobnými rysmi je ľahšie odhaliteľné. Ako heslo nepoužívajte svoj dátum narodenia, rodné číslo, telefónne číslo, po sebe idúce číslice a heslo pravidelne meňte. Nikdy nemeňte heslo do internetbankingu na inom formulári, než v záložke Globálne nastavenia v internetbankingu. Banka od Vás v žiadnom prípade nebude vyžadovať iný postup. Prvotné heslo musíte zmeniť pri prvom prihlásení do internetbankingu. Platnosť nasledujúceho hesla je z bezpečnostných dôvodov obmedzená na 365 dní. Po vypršaní tejto lehoty budete pri najbližšom prihlásení do internetbankingu vyzvaní k jeho zmene.

6. Neposielajte dôverné údaje pomocou e-mailu alebo SMS, nezadávajte ich na inej internetovej stránke, než na stránke určenej na prihlásenie do internetbankingu, a to ani v prípade že dostanete e-mail prípadne SMS, ktorá napodobňuje výzvu, najmä od banky, k zaslaniu dôverných údajov alebo ich vyplnenie na inej internetovej stránke. Banka Vám taký druh správ v žiadnom prípade nebude zasielať.

Uloženie elektronického kľúča

1. Chráňte svoj elektronický kľúč, ktorý používate pri zadávaní pokynov, proti jeho zneužitiu, najmä proti jeho odcudzeniu, skopírovaniu a pod. Zneužitím Vášho elektronického kľúča môže iná osoba predstierať Vašu identitu a zadávať pokyny Vašim menom. Zneužitie elektronického kľúča Vám môže spôsobiť škodu.

2. Elektronický kľúč inštalujte iba na počítač, o ktorom viete, že je chránený proti možným hrozbám plynúcim z pripojenia k dátovej sieti. Neinštalujte elektronický kľúč na počítač, ktorý je verejne prístupný.

3. Ak uchovávate elektronický kľúč na inom prenosnom médiu, ukladajte toto médium na miesto, kde nedôjde k jeho zneužitiu, najmä odcudzeniu, skopírovaniu alebo poškodeniu.

Preventívne opatrenia vo sfére vplyvu klienta, zabezpečenie počítača klienta

1. Internetbanking používajte iba na počítačoch, ktoré sú riadne zabezpečené proti zneužitiu dôverných údajov. Nepoužívajte internetbanking najmä v internetových kaviarňach a na iných verejne prístupných počítačoch, ani na počítačoch, u ktorých nemáte istotu, že sú zabezpečené proti zneužitiu dôverných údajov.

2. Pred prihlásením do internetbankingu sa riadne presvedčte, že komunikujete so správnym poskytovateľom služby. Adresa servera banky je http://www.fio.sk/. Pri prihlasovaní do aplikácie internetbanking a pri zadávaní pokynov prostredníctvom aplikácie internetbanking riadne skontrolujte, že spojenie je zabezpečené (overte platnosť certifikátu SSL zabezpečenia) a ďalej overte identifikáciu serveru banky. V prípade pochybností o tom, že komunikujete s bankou alebo, že spojenie nie je riadne zabezpečené, nevykonávajte žiadne úkony, ktoré by mohli viesť k prezradeniu alebo zneužitiu dôverných údajov a bezodkladne kontaktujte klientskeho pracovníka banky.

3. Počítač, na ktorom sa rozhodnete používať internetbanking, zabezpečte legálnym firewallom, antivírovou a anti-spyware ochranou, a tieto ochranné prvky pravidelne aktualizujte. Programy aktualizujte štandardným spôsobom. Pravidelne sledujte informácie o nových hrozbách, vírusoch, spyware a pod. a v súlade s tým zaistite ochranu Vášho počítača.

4. Používajte legálny a pravidelne aktualizovaný operačný systém vo Vašom počítači. Pravidelne sledujte správy výrobcu Vášho operačného systému o opravách chýb a nedostatkov tohto operačného systému a tieto opravy včas inštalujte do Vášho počítača.

5. Ak používate internetbanking na určitom počítači, vyvarujte sa sťahovaniu a inštalovaniu programov, ktoré možno voľne získať na internete, u ktorých si nie ste istí, či neobsahujú vírusy alebo spyware, prípadne pochádzajú zo zdroja, ktorý je dôveryhodný. Navštevujte len známe, dôveryhodné a bezpečné stránky na internete. Neotvárajte nevyžiadané emaily, emaily od neznámych adresátov a emaily s podozrivým názvom alebo obsahom na takomto počítači. Takéto emaily bez otvorenia zmažte. Vo svojej emailovej schránke používajte spam filter.

6. Žiadne licenčné ustanovenia u voľne šíreného softvéru Vám nemôžu poskytnúť istotu, že softvér neobsahuje súčasti, ktoré môžu Váš počítač poškodiť či inak narušiť bezpečnosť Vami ukladaných údajov.

7. Pre získanie základných informácií o možnostiach zabezpečenia Vášho počítača a o rizikách, ktoré hrozia Vášmu počítaču, si prosím prečítajte informácie na stránkach:
http://windows.microsoft.com/sk-SK/windows/products/security-essentials

Zabezpečenie SMS

1. Pre prijímanie autorizačných SMS kódov je najdôležitejšia SIM karta, ktorá obsahuje telefónne číslo, ktoré ste určili na prijímanie autorizačných SMS kódov od banky (ďalej len "SIM karta"). Túto SIM kartu majte vždy pod dohľadom, telefón bez SIM karty neumožní komunikáciu s bankou a autorizáciu.

2. Mobilný telefón so SIM kartou, nenechávajte ležať na miestach, kde nad ním nemáte dohľad.

3. Vyvarujte sa požičiavaniu mobilného telefónu s vloženou SIM kartou tretím osobám bez toho, aby ste mali prehľad o ich nakladaní s telefónom a najmä SIM kartou.

4. V prípade, že hrozí riziko, že by ste mohli ponechať telefón so SIM kartou mimo Váš dohľad, znemožnite jeho používanie tretím osobám kódom PIN. Tento kód uchovávajte v tajnosti a neprezrádzajte ho tretím osobám, ani si ho nikam nezaznamenávajte.

5. Autorizačný kód doručený bankou si nikam nezaznamenávajte a SMS s autorizačným kódom žiadnej osobe nesprístupňujte.

6. V závislosti na technickom pokroku v oblasti funkcií mobilných telefónov zaistite funkcie svojho telefónu proti možnosti automatického pripojenia tretej osoby k Vášmu telefónu.

Kontaktujte klientskeho pracovníka

V prípade, že dostanete e-mail s upozornením na akúkoľvek zmenu v spôsobe prihlasovania do internetbankingu alebo s informáciou o zmene www adresy prihlasovacej stránky, alebo v prípade, že zistíte netypické alebo inak podozrivé správanie prihlasovacej stránky, vrátane automatického presmerovania, alebo iné podozrivé skutočnosti , nevykonávajte žiadne úkony, ktoré by mohli viesť k prezradeniu alebo zneužitiu dôverných údajov a bezodkladne kontaktujte telefonicky klientskych pracovníkov banky a vyžiadajte si radu ohľadne ďalšieho postupu.