DESATERO BEZPEČNÉHO POUŽÍVÁNÍ INTERNETBANKINGU

1. **Chraňte vždy a přede všemi přihlašovací údaje – heslo nesdělujte nikomu za žádných okolností.** Banka po Vás heslo nikdy nebude chtít. Pokud ano, jde o podvod a obraťte se na non-stop linku +420 224 346 777. Heslo nezadávejte nikam jinam než do internetového bankovnictví Fio banky. Nikomu nesdělujte Váš PIN k platební kartě.

2. **Chraňte autorizační zprávy a kódy.** Autorizační zprávu ani autorizační kód nikomu nepřeposílejte, banka je po Vás nikdy nebude chtít. Pokud ano, jde o podvod a obraťte se na non-stop linku +420 224 346 777. Pečlivě kontrolujte údaje o pokynu na autorizačním zařízení (zejména číslo cílového účtu a částku) a autorizační kód opisujte pouze pokud všechny údaje odpovídají a textu v autorizační zprávě jasně rozumíte.

3. **Bezpečné přihlášení a odhlášení.** V adresním řádku prohlížeče musí být adresa začínající https://ib.fio.cz a vlevo od adresy je ikona zámku. Po kliknutí na ikonu se zobrazí Certifikát vydán pro: Fio banka, a.s. (CZ). Při ukončení činnosti se vždy odhlaste.

4. **Zvolte bezpečné heslo.** Čím delší heslo zvolíte, tím obtížnější je jeho prolomení. Při volbě hesla se vyhýbejte osobním jménům, přezdívkám či osobně významným datům jako jsou např. narozeniny, rodné číslo apod. Vždy je vhodnější zvolit delší heslo z několika slov (oproti krátkému heslu se speciálními znaky), které si snadno zapamatujete a bude se vám snadno zadávat.

5. **Pravidelně aktualizujte operační systém a webový prohlížeč.** Pokud používáte Windows, doporučujeme také chránit systémem pravidelně aktualizovaným antivirovým programem.

6. **Používejte pouze bezpečná zařízení.** Pro připojení do bankovnictví používejte pouze taková zařízení a sítě, o jejichž bezpečnosti nemáte pochyb.

7. **Pozor na phishing.** Velkým rizikem jsou podezřelé emaily, které se mohou tvářit například jako upomínka, falešný příkaz k exekuci či zpráva o výhře v loterii. E-mail představuje pro bezpečnost Vašeho počítače jedno z největších rizik a je potřeba obezřetnosti při otevírání jeho příloh. Škodlivý software cílící na data z Vašeho počítače se může ukrývat právě v příloze emailu nebo pod odkazem na webové stránky.

8. **Neinstalujte aplikace z neověřených zdrojů.** Povolujte instalaci jen těm aplikacím, o jejichž původu a účelu nemáte žádné pochybnosti.

9. **Sledujte svůj účet.** Pravidelně kontrolujte pohyby na účtu. Není na škodu kontrolovat i historii přihlášení do Vašeho internetového bankovnictví.

10. **Při podezření na kompromitaci jednejte rychle, ale s rozvahou.** Pokud nabudete podezření, že Váš účet nebo Vaše zařízení bylo napadeno, neotálejte a bezodkladně nás kontaktujte. Pokud máte podezření, že byl napaden Váš počítač, nesnažte se situaci zachránit tím, že se pomocí tohoto počítače přihlásíte do IB za účelem změny hesla. Volejte na non-stop linku +420 224 346 777. Při podezření, že byl napaden Váš telefon, použijte (pokud možno) jiný telefon. Heslo po vás chtít nebudeme, nesdělujte nám ho.