

Bezpečnostní desatero



1.

Chraňte vždy a přede všemi přihlašovací údaje

Heslo nesdělujte nikomu za žádných okolností. Banka po Vás heslo nikdy nebude chtít.

2.

Chraňte autorizační zprávy a kódy

Autorizační zprávu ani autorizační kód nikomu nepřeposílejte. Banka to po Vás nikdy nebude chtít.

3.

Bezpečně se přihlašujte a odhlašujte

V adresním řádku prohlížeče musí být adresa začínající <https://ib.fio.cz/ib/> a vlevo od adresy je ikona zámku. Po ukončení činnosti se vždy odhlaste.

4.

Zvolte bezpečné heslo

Vyhýbejte se osobním jménům, přezdívkám či významným datům jako jsou např. narozeniny, rodné číslo apod. Vhodné je kombinovat malá a velká písmena, číslice a speciální znaky. Čím složitější a delší heslo zvolíte, tím obtížnější je jeho prolomení.

5.

Pravidelně aktualizujte operační systém a webový prohlížeč

Doporučujeme také chránit systém pravidelně aktualizovaným antivirovým programem.

6.

Používejte pouze bezpečná zařízení

Pro připojení do bankovníctví používejte pouze taková zařízení a sítě, o jejichž bezpečnosti nemáte pochyb.

7.

Chraňte se před phishingem

Útočníci používají různé metody, aby získali Vaše citlivé údaje — hesla, čísla platebních karet či přístup k bankovním aplikacím. Útoky probíhají skrze falešné e-maily, zprávy, telefonáty nebo webové stránky. Neklikejte na podezřelé odkazy, nevyplňujte své údaje na neověřených stránkách, nepotvrzujte transakce, o nichž nic nevíte, a neposkytujte citlivé informace ani po telefonu. Více informací nalezete na našich webových stránkách.

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 bankovníctví.

10.

Máte podezření, že jste se stali obětí podvodu? Ihned nás kontaktujte na +420 224 346 392