

Bezpečnostné desatoro



1.

Chráňte vždy a pred všetkými prihlasovacie údaje

Heslo neposkytujte nikomu za žiadnych okolností. Banka od Vás heslo nikdy nebude chcieť.

2.

Chráňte autorizačné správy a kódy

Autorizačnú správu ani autorizačný kód nikomu nepreposielajte. Banka to od Vás nikdy nebude chcieť.

3.

Bezpečne sa prihlasujte a odhlasujte

V adresnom riadku prehliadača musí byť adresa začínajúca <https://ib.fio.sk/ib/> a vľavo od adresy je ikona zámku. Po ukončení činnosti sa vždy odhláste.

4.

Zvoľte bezpečné heslo

Vyhýbajte sa osobným menám, prezývkam či významným dátumom ako sú napr. narodeniny, rodné číslo apod. Vhodné je kombinovať malé a veľké písmená, číslice a špeciálne znaky. Čím zložitejšie a dlhšie heslo zvolíte, tým ťažšie je jeho prelomenie.

5.

Pravidelne aktualizujte operačný systém a webový prehliadač

Odporúčame tiež chrániť systém pravidelne aktualizovaným antivírusovým programom.

6.

Používajte iba bezpečné zariadenia

Na pripojenie do bankovníctva používajte iba také zariadenia a siete, o ktorých bezpečnosti nemáte pochyb.

7.

Chráňte sa pred phishingom

Útočníci používajú rôzne metódy, aby získali Vaše citlivé údaje – heslá, čísla platobných kariet či prístup k bankovým aplikáciám. Útoky prebiehajú cez falošné e-maily, správy, telefonáty alebo webové stránky. Neklikajte na podozrivé odkazy, nevyplňajte svoje údaje na neoverených stránkach, nepotvrdzujte transakcie, o ktorých nič neviete, a neposkytujte citlivé informácie ani po telefóne. Viac informácií nájdete na našich webových stránkach.

8.

Neinštalujte aplikácie z neoverených zdrojov

Povoľujte inštaláciu len tým aplikáciám, o pôvode a účele ktorých nemáte žiadne pochybnosti.

9.

Sledujte svoj účet

Pravidelne kontrolujte pohyby na účte. Nie je na škodu kontrolovať aj históriu prihlásení do Vášho internetového bankovníctva.

10.

Máte podozrenie, že ste sa stali obeťou podvodu? Ihneď nás kontaktujte na +421 2 2085 0310