

Bezpečnosť elektronického bankovníctva

Bezpečnosť finančných prostriedkov je pre nás na prvom mieste. Pre dosiahnutie čo najvyššieho zabezpečenia využívame najmodernejšie technológie. K ochrane vašich financií môžete výraznou mierou prispieť aj vy dodržiavaním základných zásad bezpečnosti pri používaní elektronického bankovníctva.

Chráňte si heslo a PIN

Heslo a **PIN kód** sú súčasťou bezpečnostných prvkov umožňujúcich prístup do elektronického bankovníctva alebo vykonávanie aktívnych transakcií. Preto si ich chráňte a nikomu neprezradte. Pri vytváraní a používaní PIN kódu a hesla dodržiavajte nasledovné zásady:

- nepoužívajte jednoduchý alebo ľahko odvoditeľný kód,
- využite najväčšiu možnú dĺžku hesla a PIN-u,
- PIN a heslo si nikam nezaznamenávajúte,
- originál obálky s vygenerovaným PIN kódom alebo heslom znehodnoťte, prípadne uchovajte na bezpečnom mieste (trezor).

V žiadnom prípade nepoužívajte ako PIN kód alebo heslo dátum narodenia, časť telefónneho čísla či po sebe idúce číslice. Nezaznamenávajúte si ich na papieriky, platobnú alebo čipovú kartu, do počítača, telefónu či na iné miesta. Vaše bezpečnostné prvky nikomu neprezradte, a to ani vašim najbližším rodinným príslušníkom.

Dávajte si pozor na mobilný telefón

Ak si nechávate zasielať autorizačný kód pre platby cez SMS, prípadne využívate aplikáciu SmartBanking, chráňte si mobilný telefón. Nenechávajte ho bez dozoru a nepožičiavajte ho iným osobám.

Ochranu môžete zvýšiť nastavením uzamknutia obrazovky telefónu heslom, alebo biometriou. Neinštalujte si do telefónu neznáme aplikácie a aktualizácie sťahujte iba z dôveryhodných zdrojov. Odporúčané je aj používanie antivírusového programu pre smartfóny.

V prípade straty alebo odcudzenia mobilného telefónu čo najskôr kontaktujte naše Kontaktné centrum.

Ochraňujte si token

Ak pre prístup do elektronického bankovníctva alebo autorizáciu platieb využívate token, chráňte si tieto zariadenia a nenechávajte ich bez dozoru na voľne dostupných miestach. V prípade straty alebo odcudzenia čo najskôr kontaktujte naše Kontaktné centrum.

Skontrolujte si platobné príkazy, ktoré potvrdzujete

V žiadnom prípade **nepotvrdzujte platobný príkaz, ktorý ste sami nezaslali**. Všímajte si hlavne správnosť čísla účtu príjemcu, sumu a ďalšie detaily platby. Ak odhalíte nezrovnalosť údajov v potvrdzovacej správe s údajmi zadanými pri platobnom príkaze, nepotvrdzujte ho a kontaktujte nás prostredníctvom nášho Kontaktného centra.

Overte si, či sa nachádzate na stránke elektronického bankovníctva ČSOB

Nespoliehajte sa na vzhľad stránky, ale skontrolujte si vo vašom prehliadači adresu, na ktorej sa nachádzate. Pre prácu s elektronickým bankovníctvom ČSOB musí mať takýto tvar:

- <https://moja.csob.sk/prihlasenie/krok-1> – ak používate službu internetbanking Moja ČSOB
- <https://bb24.csob.sk/> – ak používate službu BusinessBanking.

Ďalej skontrolujte, či sa vedľa adresy stránky nachádza ikona bezpečnostného zámku.

Dvojklikom na túto ikonu overte, že ide o certifikát **GlobalSign Extended Validation CA**.

Nereagujte na podozrivé e-maily

Neotvárajte e-mailové správy od neznámych adresátov alebo s podozrivým názvom či obsahom. V žiadnom prípade nespúšťajte prílohy takýchto správ a bez otvárania ich vymažte. Nikdy nereagujte na e-mail, vyžadujúci poskytnutie vašich osobných údajov, hesla alebo PIN kódu. **ČSOB od vás nikdy nebude požadovať vaše údaje takouto formou**. Ak by ste takýto podozrivý e-mail našli vo svojej e-mailovej schránke, neváhajte a kontaktujte nás prostredníctvom nášho Kontaktného centra.

Využívajte zasielanie informačných SMS a e-mailov

V prostredí elektronického bankovníctva si môžete nastaviť **zasielanie informačných správ, tzv. Notifikácie** o akýchkoľvek operáciách. Včas sa tak dozviete o vykonaných platbách a v prípade zneužitia účtu môžete predísť strate finančných prostriedkov jeho zablokovaním.

Zabezpečte si počítač

Pre prácu s elektronickým bankovníctvom **používajte iba počítač, ktorého bezpečnosť viete ovplyvniť**. Pre maximálnu ochranu dodržiavajte nasledovné odporúčania:

- pravidelne inštalujte aktualizácie vydávané výrobcom operačného systému,
- používajte antivírusové a antispymware programy, ktoré tiež pravidelne aktualizujte,
- zapnite si firewall, ak používate operačný systém Windows alebo Mac OS, alebo si stiahnite osobný firewall,
- pre prihlásenie sa do elektronického bankovníctva používajte najnovšiu verziu prehliadača,
- nepovoľujte ukladanie prihlasovacích údajov do pamäte prehliadača.

Nesťahujte súbory z nedôveryhodných zdrojov

Dávajte si pozor na súbory, ktoré sťahujete do svojho počítača; **nesťahujte ich z nedôveryhodných stránok** a obzvlášť si dávajte pozor na súbory s príponou **.exe** - pri inštalácii môžu do počítača nahráť škodlivý a nebezpečný softvér.

Kontakt

Ak máte ďalšie otázky ohľadom zásad bezpečnosti používania elektronického bankovníctva, môžete nás kontaktovať:

- na čísle **0850 111 777** (z územia SR),
- na čísle **+421 2 5966 8844** (z územia mimo SR),
- e-mailom helpdeskEB@csob.sk.