INFORMACE K POUŽÍVÁNÍ INTERNETOVÉHO BANKOVNICTVÍ A BANKOVNÍ IDENTITY

ÚČINNÉ OD 9. 12. 2023

DODRŽOVÁNÍM NÁSLEDUJÍCÍCH DOPORUČENÍ PŘI VYUŽÍVÁNÍ SLUŽEB INTERNETOVÉHO BANKOVNICTVÍ ELIMINUJETE MOŽNOST ZNEUŽITÍ FINANČNÍCH PROSTŘEDKŮ NA VAŠEM ÚČTU V BANCE.

Následující doporučení se týkají Internetového bankovnictví a bankovní identity, tedy jak aplikací CREDITAS Banking a CREDITAS Banking Mobile, pro každou ze služeb Internetového bankovnictví a službu bankovní identity se tak níže uvedené zásady aplikují přiměřeně s ohledem na povahu dané služby. Tento dokument obsahuje výčet základních zásad a doporučení. Pro podrobnější informace k bezpečnému používání Internetového bankovnictví sledujte bezpečnostní informace na webových stránkách Banky - https://www.creditas.cz/ a řiďte se podrobnými pravidly pro Internetové bankovnictví a bankovní identity, obsaženými v příslušných Obchodních podmínkách.

PŘIHLAŠOVÁNÍ

Přihlašovací údaje v aplikaci CREDITAS Banking (personalizované bezpečnostní prvky) vkládejte pouze do formuláře na webových stránkách Banky https://banking.creditas.cz/ (přístup na tuto stránku je možný také skrze https://www.creditas.cz) nebo https://api.creditas.cz/oam/nia-saml-request-process, identitu webové stránky, do níž své přihlašovací údaje zadáváte, si můžete ověřit zobrazením certifikátu v internetovém prohlížeči. Hodláte-li využívat služeb Internetového bankovnictví ze svého mobilního telefonu (či jiného zařízení, pro které Banka poskytuje dedikovanou aplikaci), využijte přednostně služeb CREDITAS Banking Mobile prostřednictvím oficiální aplikace Banky.

Personalizované bezpečnostní prvky chraňte před zneužitím, nezapisujte si je, nesdělujte je třetím osobám a vždy dbejte zvýšené pozornosti, kam tyto údaje zadáváte. Banka **nikdy nepožaduje** po svých klientech sdělení těchto údajů emailem, při telefonní nebo jiné komunikaci. Současně chraňte před zneužitím a nesdělujte třetím osobám Vaše další osobní a bezpečnostní údaje (jména, data, čísla platebních karet, PIN, MPIN, ePIN, uPIN, SMS kódy apod.)

Používejte tzv. „silná“ hesla, která obsahují velká i malá písmena, číslice, speciální znaky (příklad: Qwo7-h3#), v případě podezření na vyzrazení nebo zneužití hesla, či jiného přihlašovacího údaje, proveďte jeho změnu a neprodleně informujte Banku.

NASTAVENÍ BANKOVNÍ IDENTITY

Bankovní identitu lze spravovat pomocí digitálních aplikací Banky CREDITAS, a to aplikace CREDITAS Banking nebo CREDITAS Banking Mobile.

V aplikacích je věnovaná bankovní identitě samostatná kategorie v sekci Správa, kde se pod Nastavením lze prokliknout do podsekce Bankovní identita.

Uživatel může spravovat svou bankovní identitu ve stavech:

- Nevytvořená
- Aktivovaná
- Pozastavená
- Zrušená

Pro zřízení bankovní identity je zapotřebí splnit následující podmínky:

- Aktivní přístup do internetového bankovnictví
- Fyzická identifikace s osobně ověřeným identifikačním dokladem na pobočce Banky CREDITAS a.s.
- Plnoletost
- Úspěšné ztotožnění vůči informačnímu systému základních registrů

Aktivní operace jako prvotní zřízení nebo aktivace bankovní identity je podmíněna silným ověřením klienta dle nastavení konkrétního uživatele.

- SMS OTP
- MPIN

BEZPEČNOST PŘI POUŽÍVÁNÍ INTERNETOVÉHO BANKOVNICTVÍ A PŘIHLÁŠOVÁNÍ BANKOVNÍ IDENTITOU

Pravidelně kontrolujte stav Vašeho účtu v Bance a nastavení souvisejících produktů a služeb, jakými jsou zejména limity plateb, trvalé příkazy a povolení k inkasu nebo bankovní identita. Využívejte upozornění o pohybech na Vašem účtu v Bance přes SMS/e-mail. V případě jakékoli neautorizované změny či nesrovnalostí na Vašem účtu kontaktujte Banku.

Ignorujte nevyžádanou emailovou komunikaci (neznámý odesílatel), neotevírejte neznámé přílohy, neklikejte na neznámé webové odkazy.

Pro přístup k Internetovému bankovnictví nebo přihlašování bankovní identitou nevyužívejte veřejné WiFi sítě (kavárny, nádraží apod.).

PRAVIDLA PRO KOMUNIKAČNÍ ZAŘÍZENÍ

Pro přístup k Vašemu účtu v Bance používejte pouze ověřené a zabezpečené komunikační zařízení (počítač, mobilní telefon, tablet), nevyužívejte veřejně přístupná zařízení – hotely, kavárny, knihovny aj.

Na Vašem komunikačním zařízení provádějte pravidelné aktualizace operačního systému, webového prohlížeče, antivirového programu, firewallu a dalších klíčových aplikací a prvků. Na zařízení instalujte programy pouze z ověřených zdrojů případně z oficiálních obchodů (např. App Store, Microsoft Store). V nastavení zařízení neumožněte zapamatování si přihlašovacích jmen a hesel.

Chraňte své komunikační zařízení heslem, či obdobným autentizačním prvkem, abyste zamezili jeho možnému využívání neoprávněnými osobami.

V souladu s technologickým a bezpečnostním vývojem může Banka omezit, či zcela vyloučit podporu některých komunikačních zařízení, platforem, či verzí softwaru.

V případě podezření na zneužití komunikačního zařízení, ať již ve formě jeho použití neoprávněnou osobou, přítomnosti škodlivého programu, či kódu, přerušte využívání Internetového bankovnictví a kontaktujte neprodleně Banku.

MINIMÁLNÍ TECHNICKÉ POŽADAVKY PRO VYUŽÍVÁNÍ INTERNETOVÉHO BANKOVNICTVÍ A BANKOVNÍ IDENTITY

CREDITAS Banking pro počítače a tablety

- Osobní počítač nebo tablet s připojením k internetu a s aktualizovanou verzí operačního systému.
- Internetový prohlížeč **Google Chrome, Mozilla Firefox, Opera, Safari nebo Microsoft Edge**. Podporované jsou poslední 2 vydané verze, z bezpečnostních důvodů však doporučujeme používat vždy verzi aktuální, kterou lze získat z oficiálních webových stránek jejich poskytovatelů. Prohlížeč Internet Explorer z bezpečnostních důvodů již není podporovaný.
- Mobilní telefon (pro příchozí SMS sloužící k přihlašování a autorizaci požadavků, zejména v spojení s přístupem skrze osobní počítač, případně mobilní telefon s internetem pro variantní způsob autorizace QR kódem s mobilní aplikací CREDITAS Banking).

CREDITAS Banking pro mobily

- Chytrý telefon s podporovaným systémem: iOS verze 14.0 a výše, Android verze 6 a výše.
- Mobilní aplikace CREDITAS Banking stažená z – App Store pro iOs, Google Play pro Android, App Gallery pro Huawei telefony.
- Připojení k internetu.