

ÚČINNÉ OD 1. 9. 2018

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

Následující doporučení se týkají Internetového bankovníctví, tedy jak aplikace IB, tak Mobilního bankovníctví, pro každou ze služeb Internetového bankovníctví 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 bankovníctví sledujte bezpečnostní informace na webových stránkách Banky - <https://www.creditas.cz/> a řiďte se podrobnými pravidly pro Internetové bankovníctví, obsaženými v příslušných Obchodních podmínkách.

PŘIHLAŠOVÁNÍ

Přihlašovací údaje v aplikaci IB (personalizované bezpečnostní prvky) vkládejte pouze do formuláře na webových stránkách Banky <https://www.creditas.cz/>, identitu webové stránky, do níž své přihlašovací údaje zadáváte, si můžete ověřit zobrazením certifikátu v internetovém prohlížeči. Hodláte-li využívat služeb Internetového bankovníctví ze svého mobilního telefonu (či jiného zařízení, pro které Banka poskytuje dedikovanou aplikaci), využijte přednostně služeb Mobilního bankovníctví 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, 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.

BEZPEČNOST PŘI POUŽÍVÁNÍ INTERNETOVÉHO BANKOVNICTVÍ

Pravidelně kontrolujte stav Vašeho účtu v Bance a nastavení souvisejících produktů a služeb, jakými jsou zejména limity plateb, trvalé příkazy a povolení k inkasu. 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.

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

Pro přístup k Internetovému bankovníctví 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, přerušete využívání Internetového bankovníctví a kontaktujte neprodleně Banku.