UniCredit Bank

ZÁSADY BEZPEČNEJ KOMUNIKÁCIE A OCHRANY DÁT

Dodržiavanie jednoduchých pravidiel vám umožní bezpečne ovládať účty prostredníctvom produktov internetového bankovníctva a minimalizovať riziko zneužitia vašich osobných údajov neoprávnenými osobami.

Prihlasovacie údaje, heslá, PIN-y

- nikdy nezdieľajte s ďalšou osobou svoje bezpečnostné údaje (ID užívateľa, heslo, PIN, bezpečnostný kód)
- vyvarujte sa používania produktov internetového bankovníctva na verejnosti (napríklad v dopravných prostriedkoch) alebo v monitorovaných miestnostiach (napríklad v blízkosti bezpečnostných kamier)
- predovšetkým pri prihlasovaní dbajte na svoje súkromie a skontrolujte, či ďalšie osoby nemôžu zaregistrovať vaše prihlasovacie údaje
- nepoužívajte internetové bankovníctvo na počítačoch, pri ktorých si nemôžete byť istí, či v nich nie sú nainštalované škodlivé programy (napríklad vo verejných internetových kaviarňach)
- nenechávajte svoj počítač či mobilný telefón bez dozoru; používajte zámky klávesníc a prístupové kódy k zariadeniu

E-mail

- Banka nikdy nezasiela e-maily s výzvou na poskytnutie identifikačných údajov klienta, hesiel, PIN-ov atď., na takéto výzvy nereagujte a informujte infolinku UniTel
- otvárajte iba dôveryhodné e-maily od známych a očakávaných odosieľateľov; pokiaľ sa vám e-mail zdá podozrivý, je rizikové ho otvárať

Internet

- navštevujte na internete iba známe a dôveryhodné stránky
- vyvarujte sa sťahovania neznámych súborov z internetu do počítača; môžu skrývať nebezpečné programy a vírusy
- buďte obzvlášť opatrní pri používaní otvorených bezdrôtových sietí (dôveryhodnosť Wi-Fi pripojenia)
- pokiaľ sa vám zdá prihlasovacia obrazovka k produktom priameho bankovníctva akokoľvek podozrivá, neprihlasujte sa a kontaktujte infolinku UniTel

Aplikácie v mobile

- do mobilných telefónov inštalujte iba aplikácie z oficiálnych obchodov s aplikáciami – Google Play (Android), App Store (iOS)

Vírusy

- program pravidelne aktualizujte
- odporúčame používať najnovšie verzie antivírusových programov, ktoré majú implementované i detektory škodlivého softvéru
- zároveň odporúčame na počítači používať firewall
- aj smartfóny a tablety by mali byť vybavené antivírusovou ochranou

UniCredit Bank

Operačný systém, internetový prehliadač

- aktualizujte operačný systém počítača pomocou bezpečnostných záplat, prípadne pomocou aktualizačných balíčkov vydávaných výrobcom
- pravidelne aktualizujte svoje programy, obzvlášť dôležité je aktualizovať internetový prehliadač a tzv. zásuvné moduly (napríklad prehrávač Flash)
- pre smartfóny a tablety odporúčame používať najnovšiu verziu operačného systému (tzv. firmvér), ktorú výrobca pre zariadenie oficiálne ponúka

Pravidelne kontrolujte zostatky účtov a transakcie napríklad formou automaticky zasielaných SMS či e-mailov s príslušným obsahom.

Pri podozrení z podvodu, pri podvode alebo pri bezpečnostnej hrozbe Banka informuje klienta vhodným spôsobom, využívajúc primárne kontaktné informácie, ktoré klient uviedol pri vstupe do zmluvného vzťahu s Bankou, zohľadňujúc bezpečnosť zdieľaných informácií medzi Zmluvnými stranami.