

Bezpečnostní report Air Bank: Jaké podvody klienti nejčastěji hlásili v roce 2025/2026

1.10.2026 - | Air Bank

Když se v médiích mluví o kybernetických podvodech, často to zní jako vzdálené nebezpečí nebo scény z filmu o hackerech. Jenže online podvody nejsou jen abstraktní riziko. Jsou to konkrétní situace, se kterými se naši klienti reálně potkávají v běžném životě. Při prodeji starého kočárku na bazaru, při čekání na balíček nebo během večerního odpočinku u telefonu.

V Air Bank situaci na trhu neustále sledujeme. Analyzovali jsme nahlášené případy za rok 2025 a první polovinu roku 2026 a sestavili přehledný report. Ne proto, abychom vás děsili čísly, ale abyste přesně věděli, na jaké triky podvodníci sázejí nejčastěji a jak se jim s přehledem vyhnout.

A data ukazují zajímavý vývoj: počet evidovaných škod meziročně vzrostl přibližně o 77 %, jejich celkový finanční objem ale naopak klesl zhruba o 13 %. V přepočtu na jeden evidovaný případ tak průměrná škoda klesla přibližně o polovinu.

Podvody, které klienti opravdu řešili

[Nejčastější podvody](#) posledních měsíců nemají nic společného s tím, že by se útočníci prolomili do bankovních systémů. [Bankovní bezpečnost](#) je dnes na špičkové úrovni. Podvodníci proto zkoušejí jinou cestu, útočí přímo na člověka, jeho emoce a nepozornost.

Potvrzují to i naše data. Přibližně 27 % reklamovaných transakcí proběhlo bez vědomí klienta. U zbývajících zhruba 73 % transakcí nebo související činnosti provedl sám klient. To samozřejmě neznamená, že chtěl podvodníkovi peníze poslat. Často jednal právě pod jeho vlivem — například uvěřil falešnému bankéři, zadal údaje na podvodném webu nebo sám potvrdil převod.

Když typické scénáře podvodníků rozpoznáte včas, výrazně tím snižujete šanci, že uspějíte.

Které podvody způsobují největší škody

Jednotlivé typy podvodů se výrazně liší tím, jak velké finanční škody způsobují. V roce 2026 mají největší podíl na celkovém objemu evidovaných škod investiční podvody.

Typ podvodu	Podíl na celkovém objemu škod v roce 2026	Jak scénář typicky vypadá
Investiční podvody	50 %	Podvodník láká na výhodnou investici, například do kryptoměn nebo akcií. Oběť může přesvědčit k převodu peněz nebo instalaci aplikace pro vzdálený přístup.
Falešní bankéři a policisté (vishing)	11 %	Volající tvrdí, že jsou vaše peníze v ohrožení, a snaží se vás přesvědčit k převodu na údajně „bezpečný“ účet, výběru hotovosti nebo jiné operaci.
Zneužití debetní karty	11 %	Údaje z karty se dostanou k podvodníkovi, který je následně využije k neoprávněným transakcím.

Poznámka: Procenta v této části vyjadřují podíl na celkovém objemu evidovaných škod, nikoliv podíl na počtu podvodných případů.

Tyto tři kategorie dohromady představují přibližně **72 % celkového objemu evidovaných škod**. Samotné investiční podvody přitom stojí za **polovinou všech evidovaných škod**.

Ve srovnání s rokem 2025 se jejich význam ještě mírně zvýšil — tehdy investiční podvody představovaly přibližně **47 % celkového objemu škod**.

Nejčastěji reklamujeme převody

Zajímavý obrázek nabízí také pohled na to, **jakých transakcí se reklamace týkají**.

V roce 2026 tvořily největší skupinu **převody s podílem přibližně 53 %**. Následovaly **online karetní transakce s přibližně 19 %**. Zahraniční transakce a výběry z bankomatu představovaly shodně přibližně **11 %**.

Oproti roku 2025 navíc podíl převodů vzrostl z přibližně **45 % na 53 %**. Zvýšil se také podíl online karetních transakcí, přibližně z **15 % na 19 %**.

Co mají tyto podvody společné

Ať už jde o [falešného bankéře](#) na telefonu nebo [podvodnou SMS o balíčku](#), všechny typy podvodů stojí na několika stejných manipulačních technikách. Podvodníci pracují s psychologií a nejčastěji sázejí na tyto prvky:

- **Vyvolání stresu a spěchu:** „Musíte jednat hned, do 10 minut vám zablokujeme účet.“ Cílem je, abyste zpanikařili a nedali si čas na rozmyšlenou.
- **Strach o peníze:** Útočníci vás vystraší tím, že vám údajně někdo bere peníze, a pak se nabídnou jako váš „záchranář“.
- **Podvržená identita:** Využívají tzv. spoofing — dokážou napodobit telefonní číslo banky, pošty i policie, takže příchozí hovor nebo SMS vypadá naprosto důvěryhodně.
- **Snaha dostat vás mimo bezpečí:** Vždy se vás snaží dostat pryč z oficiální aplikace nebo webu banky. Posílají vám odkazy na podvržené stránky nebo vás nutí instalovat programy pro vzdálený přístup (jako AnyDesk nebo TeamViewer).

Kde klienti nejčastěji udělali chybu

Rozumíme tomu, že v krizové situaci nebo při náročném dni je snadné udělat překlep. Ochrana před podvody ale začíná tím, že si ukážeme, v jakém momentě se podvodníkům podařilo klienta dotlačit k chybě. Ve **82 % nahlášených případů** totiž nebyla příčinou sofistikovaná chyba v softwaru, ale fakt, že klient sám podvodníkovi pomohl.

A to tak, že **klikl na odkaz z neznámého zdroje** a přešel na stránku, která vypadala jako přihlašovací obrazovka banky, ale v adrese měla překlep. Nebo **zadal citlivé údaje**, vyplnil čísla karty, CVC kódu nebo hesla na stránce, která s bankou nemá nic společného. Klasikou je také, že klient **potvrdí bankovní operaci bez přečtení**, a tím schválí notifikaci v aplikaci, ve které bylo napsáno „Odeslání platby“, ačkoliv si klient myslel, že peníze jen „přijímá“. Dalším velkým průšvihem je **instalace vzdáleného přístupu**, kdy klient povolil podvodníkovi, aby viděl obrazovku telefonu

nebo počítače. A celé to završuje fakt, že většina lidí vše **nahlásí pozdě** a ke zjištění podvodu dojde až po několika dnech, což bance komplikuje možnost platbu zachránit.

Co z toho plyne pro klienty

Aby vám tyto poznatky reálně pomohly, přeložili jsme naše data do pěti základních pravidel pro bezpečné bankovníctví:

1. **Nikdy neklikejte na odkazy na banku ze zpráv:** Do mobilního bankovníctví vstupujte výhradně přes svoji aplikaci a do internetového zadání oficiální adresy airbank.cz do prohlížeče.
2. **Při prodeji na bazaru číslo karty nedáváte:** Když peníze přijímáte, kupujícímu stačí **jen číslo vašeho účtu**. Číslo karty spolu s CVC kódem slouží pouze k tomu, aby z vaší karty peníze odešly.
3. **Čtěte, co potvrzujete:** Než přiložíte prst na čtečku nebo zadáte kód v aplikaci My Air, podívejte se na displej. Je tam napsáno *Přihlášení*, nebo *Odeslání platby*?
4. **Banka po vás nikdy nechce peníze převádět jinam:** Pokud vám volající „bankéř“ tvrdí, že máte peníze vložit do bitcoinu nebo poslat na rezervní účet, je to stoprocentně podvodník.
5. **Hesla a kódy z SMS si nechte pro sebe:** Pracovníci Air Bank po vás nikdy nebudou chtít vaše heslo, PIN ani potvrzovací SMS kódy.

Kdy se ozvat bance

Stalo se? Klikli jste na podezřelý odkaz, zadali údaje z karty nebo poslali platbu a teď máte špatný pocit? **Ozvěte se nám okamžitě.** V bezpečnosti totiž hraje čas zásadní roli. Pokud nás kontaktujete během prvních minut nebo hodin, máme mnohem vyšší šanci zneužití karty zastavit, blokovat odchozí transakce nebo zachránit vaše úspory.

Co udělat hned: Otevřete [aplikaci My Air](#) a **zamkněte** nebo **zablokujte kartu**.

Kam nahlásit podvod Air Bank: Zavolejte přímo na naši [klientskou linku](#) nebo napište do chatu v aplikaci. Nikdo vás nebude soudit ani vám nic vyčítat, jsme tu od toho, abychom vám pomohli situaci vyřešit.

Shrnutí: největší riziko je jednat ve stresu

Metody podvodníků se neustále proměňují, zkoušejí nové technologie i věrohodnější příběhy. Co se ale nemění, je jejich závislost na **vyvolání stresu, spěchu a strachu**.

Kdykoliv na vás bude někdo po telefonu nebo ve zprávě tlačit, abyste jednali hned, předávali kódy, klikali na odkazy nebo někam posílali peníze, zastavte se. Zhluboka se nadechněte, hovor zavěste a situaci si v klidu ověřte. Věcnost, klid a jedna rychlá kontrola v aplikaci jsou tou nejlepší obranou, jakou můžete mít.

Tento článek má obecnou povahu a slouží pouze k informativním účelům. Článek nenahrazuje odborné ani právní poradenství. Každá situace je individuální, a proto v případě nejasností doporučujeme konzultaci s příslušným odborníkem.

<https://www.airbank.cz/novinky/bezpecnostni-report-airbank>