

Klikli jste na podvodný odkaz? Rozhoduje prvních 10 minut

4.9.2026 - | Air Bank

Pípne zpráva o nedoručeném balíčku, nedoplatku za elektřinu nebo zablokovaném účtu. Ze zvyku klepnete na přiložený odkaz, stránka se načte a v tu chvíli vám to dojde: Sakra, to byl podvodný odkaz! A srdce vám vyletí až do krku. Úplně nejdůležitější je v tuhle chvíli nepanikařit. Samotné kliknutí na odkaz v 99 % případů ještě neznamená, že vás někdo okradl. To, co rozhoduje o bezpečí vašich peněz, jsou vaše další kroky během následujících pár minut.

Nic dalšího nevyplňujte ani nepotvrzujte

Ať už vás podvodná stránka láká na cokoli, zastavte se. Než začnete něco řešit, dodržte pár základních rad.

- **Nezadávejte** přihlašovací jméno, heslo ani PIN.
- **Nevyplňujte** číslo karty, datum platnosti ani CVC kód ze zadní strany.
- **Neklikejte** na žádná další tlačítka na stránce, například Stáhnout, Potvrdit nebo Přihlásit.
- A **neschvalujte** žádné notifikace, které vám v tu chvíli pípou v mobilu.

Pokud jste na stránce ještě nic nevyplnili, máte vyhráno a podvodník z vás nedostal vůbec nic.

Zavřete stránku a nevracejte se na ni

Jakmile si uvědomíte, že jste na falešném webu, okamžitě zavřete okno prohlížeče. Nedívejte se, co na stránce je, nezkoušejte klikat na kontakty a rozhodně nevolejte na telefonní čísla, která jsou na tomto webu uvedena. Stejně tak nestahujte žádné soubory, které vám falešná stránka nabízí ke stažení, například údajný „bezpečnostní certifikát“ nebo „aktualizaci bankovníctví“.

Zkontrolujte, jestli jste něco zadali

Ted' si v klidu promítněte, co jste udělali za posledních pár vteřin. Reakce, jak jednat po kliknutí na [podvodný odkaz](#), se totiž odvíjí právě od toho, jak daleko jste na falešném webu došli.

Pokud jste zadali heslo nebo přihlašovací údaje

Jestli jste vepsali svoje heslo do bankovníctví nebo mailu směřovaného na falešný web, musíte toto heslo okamžitě změnit. Otevřete si v mobilu oficiální aplikaci nebo zadejte adresu banky ručně do nového okna prohlížeče a heslo hned změňte. Pokud to vaše bankovníctví umožňuje, odhlaste v nastavení všechna ostatní aktivní zařízení, jako chytré hodinky, notebooky, další telefony nebo tablety.

Pokud jste zadali údaje z karty

Pokud jste vyplnili číslo karty, CVC kód nebo datum platnosti, útočník je má plně k dispozici. Na nic nečekejte. Otevřete [bankovní aplikaci](#) a kartu okamžitě zablokujte nebo dočasně zamkněte. Zneužití karty nejrychleji zamezíte včasným zamknutím v mobilu. Pro jistotu zkontrolujte karetní transakce,

zda mezi nimi není podezřelá platba.

Pokud jste zadali kód nebo něco potvrdili v aplikaci

Tohle je ta nejrizikovější situace. Pokud jste podvodníkům nadiktovali autorizační kód z SMS nebo potvrdili požadavek v bankovní aplikaci, pravděpodobně jste jim právě schválili převod peněz nebo přihlášení. **Hned [zablokujte kartu](#) a pak bez prodlení [kontaktujte banku](#)**, počítá se každá vteřina. Banka vám pomůže a řekne, jak dál postupovat.

Zkontrolujte účet a poslední transakce

Teď je čas na rychlou revizi. Otevřete si svou bankovní aplikaci, a to vždy ručně přes ikonku v mobilu, nikdy ne přes odkaz ve zprávě. A projděte si účet. Zkontrolujte odchozí platby i blokové karetní transakce. Podívejte se, zda nevidíte jakoukoli neznámou nebo podezřelou transakci. Koukněte i na to, zda se v nastavení účtu nezměnilo vaše telefonní číslo nebo mail pro zasílání notifikací.

Kdy hned kontaktovat banku

Kdy je potřeba vytočit klientskou linku nebo napsat na chat? Vždycky, když jste na podvodném webu nechali jakékoli citlivé údaje. Tedy pokud jste zadali přihlašovací údaje nebo číslo karty, přišel vám SMS kód a vy jste ho někde vyplnili, potvrdili jste neznámou notifikaci v mobilu nebo se vám z účtu strhla podvodná platba.

TIP: V Air Bank z toho neděláme vědu a nikdo vás nebude poučovat. Volejte nebo pište do chatu hned. Určitě platí, že je mnohem lepší zavolat zbytečně než pozdě.

Co nedělat po kliknutí na podvodný odkaz

Když člověk jedná ve zmatku, snadno udělají chybu i ti nejschopnější z nás. Když už se stalo a klikli jste, těmto věcem se vyhněte:

- **Nikam nevyplňujte žádné své údaje:** Pokud vám rychle dojde, že jde o falešný odkaz, je nejlepší ho hned zavřít a nikam nic nevyplňovat.
- **Nevracejte se na stránku:** Nezkoušejte zjišťovat, jestli web pořád funguje.
- **Nijak dál už nekomunikujte:** I kdyby se s vámi podvodník snažil spojit, ignorujte to.
- **Nemazte zprávu s odkazem:** Podvodná SMS nebo e-mail slouží jako důkaz pro banku i Policii ČR.
- **Nepřeposílejte odkaz známým:** Chcete-li někoho varovat, pošlete mu jen snímek obrazovky, ne samotný klikatelný odkaz.
- **Neinstalujte žádné aplikace:** Pokud vás web nebo volající nutí stahovat jakýkoli software, hned to utněte.

Shrnutí: kliknutí není konec světa, rozhodují další kroky

Samo o sobě to, že jste klikli na podvodný odkaz, ještě neznamená katastrofu. Důležité je, jak zareagujete v následujících minutách. Raději nic nevyplňujte a hned stránku zavřete. Neodesílejte žádné údaje, proveďte, co přesně jste na webu zanechali, zkontrolujte svůj účet a v případě pochybností rovnou kontaktujte banku. Když zachováte chladnou hlavu, podvodníci odejdou s prázdnou.

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/klikli-jste-na-podvodny-odkaz>