Buďte obezřetní, nedejte podvodníkům šanci.

Důvěryhodně znějící hlas v telefonu, e-mail psaný správnou češtinou nebo SMS poslaná finančním úřadem. Metody podvodníků, kteří se snaží vysát peníze z vašeho účtu, jsou stále rafinovanější. Není tedy divu, že se stále častěji nechají zmást i vzdělaní a zkušení lidé, kteří by se ještě nedávno dušovali, že jim se to stát nemůže.

Nejčastější způsoby podvodu:

Telefonát od bankéře nebo policie

Pachatel se vydává za pracovníka banky nebo policistu a varuje vás, že váš účet byl napaden a peníze jsou v ohrožení. Chce, abyste mu umožnili vzdálený přístup do svého počítače, peníze převedli na „bezpečný" účet nebo je vybrali v hotovosti a vložili třeba do bankomatu na bitcoiny.

- Co nejrychleji ukončete hovor, kontaktujte ČSOB a vše si ověřte.

E-mail v barvách banky

Pryč jsou časy, kdy podvodníci posílali špatně přeložený text z automatického překladače. Dnes vám do e-mailu přijde důvěryhodně znějící zpráva doplněná správnými logy, a dokonce i kontakty a obvyklým právním upozorněním na konci zprávy. Odesílatel v ní upozorňuje, že je potřeba aktualizovat přístupové údaje.

- Na odkazy neklikejte, přístupové údaje nikam nezadávejte a e-mail rovnou smažte. ČSOB nikdy e-mailem nevyžaduje důvěrné informace, např. číslo platební karty, heslo nebo PIN, ani neposílá odkazy na internetové stránky, kde jsou tyto údaje požadovány.

SMS od finančního úřadu

Na mobilní telefon vám přijde SMS podepsaná finančním úřadem, že vám vznikl přeplatek na dani nebo máte nárok např. na příspěvek na bydlení.

- Úřady tímto způsobem o přeplatku či nároku na příspěvek nikdy neinformují ani nepožadují přístupové údaje k účtu. Na zprávu nereagujte a smažte ji.

Základní pravidla, jak nenaletět podvodníkům

- Nikomu nesdělujte své citlivé informace (PIN, hesla, přístupové údaje, rodná čísla).
- Buďte obezřetní a nenechte se vmanipulovat do časové tísně, pokud se o čemkoli rozhodujete.
- Nevěřte zázračným nabídkám na bezpracné a bezrizikové zbohatnutí.
- Nikdy si do počítače neinstalujte nástroj na vzdálenou správu zařízení.

Devatero pro bezpečné bankovnictví

1. Používejte bezpečný počítač/telefon.
2. Chraňte své přihlašovací údaje.
3. Hesla volte pečlivě.
4. Mobilní telefon nedávejte z ruky.
5. Adresu internetového bankovnictví zadávejte ručně.
6. Neotvírejte podezřelé e-maily a soubory.
7. Průběžně kontrolujte historii plateb.
8. Čtěte komunikaci s bankou.
9. Neváhejte se kdykoli zeptat své banky.

Hlášení internetových podvodů

Máte podezření, že vám někdo přes internet napadl účet nebo se o to právě pokouší? Okamžitě volejte na NONSTOP tísňovou linku **Hlášení internetových podvodů** na číslo **+420 499 900 010**. U internetových podvodů jde často o minuty a naše nová linka je tu od toho, abyste se bez čekání dovolali rovnou specialistovi.

Kdy volat na tísňovou linku

- Narazíte na **podivnou platbu** v historii internetového bankovnictví nebo ČSOB Smart, a vůbec netušíte, kde se tam vzala.
- Zjistíte, že **máte zavirovaný počítač**, na kterém se běžně přihlašujete do internetového bankovnictví.
- Chcete si ověřit, že vám skutečně telefonoval **bankéř nebo policista**.
- Zadali jste **údaje o kartě do falešné platební brány**.
- Nechali jste se přesvědčit k až **podezřele výhodné investici** a odeslali jste už peníze.

Více informací získáte na www.csob.cz/branteserozumem.

ČSOB Private Banking

Vydání 04/2023