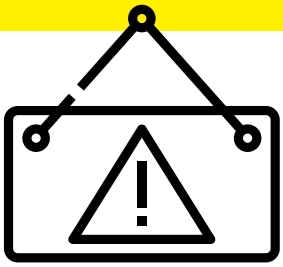
POZOR NA E-PODVODY!

Ombudsman upozorňuje: Nenechte se okrást!



Cílem podvodníků je vylákat z Vás údaje o Vaší platební kartě, internetovém bankovnictví či jiné citlivé informace nebo Vás navést na odkaz či stažení přiloženého souboru se škodlivým virem nebo malwarem.

Nebezpečné telefonáty

Na co si dát pozor?

- Útočník je schopný skrýt se za jakékoliv cizí telefonní číslo (typicky se může vydávat za pracovníka Vaší banky). Podvodníci dokáží napodobit jakékoliv telefonní číslo.

- Nikdy nikomu nesdělujte údaje z Vaší platební karty, ani přístupové údaje k Vašemu internetovému bankovnictví. Skutečný pracovník banky po Vás tyto údaje nikdy požadovat nebude.

- Své peníze nikam nepřevádějte! Falešný pracovník banky Vás může přesvědčovat, abyste své peníze převedli na jiný bankovní účet, který označí jako bezpečný. Bude Vám tvrdit, že se jedná pouze o dočasné bezpečnostní opatření, a že Vám peníze po odstranění nebezpečí vrátí zpět na Váš účet. Nikdy na to nepřistupte!

- Pokud si nejste jistí pravostí hovoru, ukončete ho a volajícímu řekněte, že zavoláte později. Na oficiálních stránkách instituce si vyhledejte telefonní číslo a instituci zavolejte. Nikdy však nevolejte přímo zpět na číslo, které Vás kontaktovalo.

Smishing aneb Podvodné SMS, WhatsApp a Facebook Messenger zprávy

Zprávy se často vztahují k

- vyzvednutí zásilky nebo
- koupi/prodeji zboží (mohou reagovat i na Vaši reálnou poptávku nebo nabídku!).

Pokud s prodejem/koupí souhlasíte, zašlou Vám odkaz na údajné stránky doručovací společnosti, která bude zprostředkovávat předání, ale půjde o podvodné stránky, jejichž cílem je opět vylákání Vašich údajů.

Nejčastěji jde o zprávy, které vypadají, jako by je zaslala

- některá z doručovacích společností,
- vaše banka či
- důvěryhodná osoba.

Popřípadě se jedná o zprávy, které Vás lákají na **vyzvednutí výhry**.

Na co si dát pozor?

- Pokud si pravostí zprávy nejste jisti, nereagujte na ni.

- Dále si nikdy na základě výzev v SMS nestahujte do telefonu aplikace, neklikejte na odkazy a nesdělujte své přihlašovací údaje ani citlivé údaje o Vaší platební kartě, přihlašovací údaje do profilů na sociální sítě, k e-mailu a už vůbec ne přístupové údaje do on-line bankovnictví.

- Nereagujte na výzvy o blokaci internetového bankovnictví nebo nedoplatku daně, ale raději se obraťte přímo na klientské centrum Vaší banky nebo finančního úřadu či jiné instituce a tuto informaci si ověřte.

Podvodné e-maily a zprávy

Na co si dát pozor?

- Zkontrolujte jméno a e-mailovou adresu odesílatele. E-mailová doména odesílatele (to, co následuje po @) by měla být shodná s názvem odesílatele e-mailu.

- Zaměřte se na obsah a gramatiku. Pokud zpráva obsahuje neobvyklé fráze nebo gramatické chyby, může se jednat o podvodný e-mail.

- Dejte si pozor na časový nátlak. Podvodný e-mail se často snaží navodit dojem, že je potřeba vykonat něco okamžitě, protože například došlo k zablokování bankovního účtu nebo je třeba obratem uhradit určitou částku, jinak spadnete do exekuce.

- Věnujte pozornost odkazům a přílohám. Přílohy mohou sloužit k maskování virů nebo malwaru, které po stažení nebo otevření mohou vést buď ke ztrátě osobních údajů, nebo k instalaci škodlivého softwaru.

Podvodné mobilní aplikace

Na co si dát pozor?

- Nestahujte nic z neoficiálních obchodů s aplikacemi a webových stránek. Bohužel podvodné aplikace se mohou nacházet i v oficiálním obchodu. Přesto stahujte aplikace jen z důvěryhodných zdrojů – nejlépe Google Play či App Store.

- Před stažením však věnujte pozornost recenzím a hodnocení aplikace a tomu, zda nejste mezi prvními, kdo aplikaci stahuje. Ověřte si i jméno vývojáře a to, zda vyvinul více aplikací. Podívejte se i na ostatní aplikace, na jejich recenze a počet stažení.

- Při udělování oprávnění aplikacím se řiďte heslem, že méně je někdy více. Dobře si rozmyslete, zda stahovaná aplikace opravdu potřebuje přístup k Vašim fotkám, kontaktům, úložišti, poloze apod.

ZÁSADY BEZPEČNOSTI V ELEKTRONICKÉ KOMUNIKACI

- Chraňte své přihlašovací údaje.

- Se svými přihlašovacími a osobními údaji zacházejte opatrně. Nikomu je nesdělujte a neukládejte je na počítačích ve veřejných sítích nebo ve škole.

- Banka Vaše přihlašovací údaje nikdy nežádá a už vůbec ne telefonicky, e-mailem anebo prostřednictvím sociálních sítí!
    - Nikdy nebude chtít, abyste se přihlásili přes zaslaný odkaz nebo odkaz ve vyhledávači.
    - Nikdy nebude chtít převést peníze na záchranný účet.
    - Nikdy nebude chtít sdělit citlivé údaje jako číslo karty, přihlašovací údaje, rodné číslo, číslo občanského průkazu a další.
    - Nikdy Vás nebude nutit nainstalovat cizí aplikaci.
    - Nepřeposílejte potvrzovací SMS kódy.
    - Nepotvrzujte transakce, které jste neprovedli.
    - Nikdy nepoužívejte stejné heslo pro různé služby (např. sociální sítě, e-mail a bankovní účet)!

- Mějte bezpečný PIN.
    - Je váš PIN datum narození nebo 1234? Rychle si ho změňte a zapamatujte.
    - PIN s nikým nesdílejte.
    - Pokud je to možné, zvolte k účtům dvoufaktorové ověřování.

- Pozor na neznámé přílohy.
    - Neotvírejte e-maily ani přílohy od neznámých a podezřelých odesílatelů.
    - Neklikejte na žádné odkazy v těle těchto e-mailů.
    - Vždy raději zkontrolujte e-mailovou adresu odesílatele a pravopis.