BEZPEČNOST NA INTERNETU

NA CO SI DÁVAT POZOR A JAK POZNAT ON-LINE PODVODNÍKY

ZÁKLADNÍ PRINCIPY

Při komunikaci na internetu je potřeba, stejně jako v životě, **být obezřetný**. Na internetu jsou důvěryhodné stránky i stránky podvodné. Internet dává prostor podvodníkům, kteří **zneužívají lidské důvěřivosti** a vydělávají na ní.

Zároveň nabízí internet i velké množství služeb, které usnadňují každodenní život. Proto je důležité naučit se v tomto novém a „divokém“ prostředí pohybovat.

- **Nevěřte cizím lidem** ani webovým stránkám, které neznáte. Ověřte, kdo píše nebo volá.
- **Nedávejte nikomu za žádných okolností své heslo**. Je to jako dát někomu klíče od domu.
- **Každá nabídka,** která zní příliš výhodně, **je podezřelá**. Ověřte si ji.
- Kdykoli si nejste jistí, **zeptejte se někoho, kdo dané oblasti rozumí.**

V návodu najdete základní pravidla a doporučení, která vám pomohou nenaletět na podvody.

JAK MĚ POZNAJÍ?

V běžném životě se musíte často identifikovat. Vrátný nebo soused vás pozná podle toho, jak vypadáte, auto odemknete klíčem, který máte jen vy, na letišti musíte ukázat občanku nebo pas.

Na internetu dokazujete svou identitu tím, že znáte své **uživatelské jméno a heslo**.

HESLO JE JAKO KLÍČ OD DOMOVA. NEDÁVEJTE HO NIKOMU, KOMU NEMŮŽETE PLNĚ DŮVĚŘOVAT.

Protože komunikace na webu probíhá zprostředkovaně, je velmi důležité, aby se k vašemu jménu a heslu někdo nedostal. Mohl by se totiž za vás vydávat, zneužít vašeho jména k podvodům nebo získat přístup k vašim datům a penězům.

HESLO JE JEN VAŠE

1. **Dostatečně „silné“ heslo**: Vaše hesla nesmí být nijak uhodnutelná, nemělo by to být existující slovo, nemělo by být kratší, než deset znaků.
2. **Neopakovat hesla:** Je velmi těžké pamatovat si více hesel. Přesto je nesmírně důležité, abyste neměli všude jedno a to samé heslo. Nainstalujte aplikaci na správu hesel, abyste mohli používat unikátní he
3. **Dvojité zabezpečení**: Tam, kde je to možné, používejte dvoukrokovou autentizaci.
4. **Heslo nikam nepište**: Za žádných okolností své heslo nepište jinam než do přihlašovacího formuláře na stránce, ke které se přihlašujete.

Pozor na stránky, které nemají zabezpečení **HTTPS**, prohlížeč před nimi varuje například vedle adresy. Ani fungující HTTPS ale **není samo o sobě známka důvěryhodnosti**.

KOMUNIKACE ON-LINE

Internet je především komunikačním nástrojem. Problém internetu je, že často vůbec nevíme, s kým komunikujeme.

NA INTERNETU JE JEDNODUCHÉ VYDÁVAT SE PRAKTICKY ZA KOHOKOLI.

- **E-mailová adresa** odesílatele může být **podvržená** nebo zavádějící
- **Zpráva** na sociálních sítích může být z **falešného** nebo ukradeného účtu
- **Webová stránka** může být **podvržená** nebo zcela lživá
- **Telefonní číslo** je také možné podvrhnout.

Ke každé zprávě, každému e-mailu, každé SMS, každému telefonátu a každé stránce přistupujte skepticky. Zvláště, pokud se vyznačuje některým z následujících podvodných rysů…

ČASTÉ TRIKY PODVODNÍKŮ

Neúplný výčet obvyklých podvodů on-line:

- ⚠ **Spam** aneb nevyžádaná pošta, obvykle nabízí nákup nějakého zboží.
- ⚠ **Phishing** vás přesměruje na falešný web, který se tváří jako oficiální ve snaze vylákat z vás vaše údaje, číslo karty či heslo.
- ⚠ **Falešný kurýr** slibuje vyzvednutí zboží
- ⚠ **Falešné články** tvářící se jako publicistika, jde ale o „advertoriál“, smyšlený příběh, který vás má přesvědčit ke koupi přípravku
- ⚠ **Falešná faktura** nebo **falešné upozornění** ohledně nedostatku peněz má za cíl vyděsit vás a vylákat z vás vaše údaje nebo rovnou peníze. Umí falšovat i telefonní hovor.
- ⚠ **Falešné seznámení**, kde podvodník předstírá, že je žena/muž toužící po vaší blízkosti, po několika dnech nebo měsících z vás lstí tahá peníze.
- ⚠ **Vydírání** údajnými citlivými záběry, které útočník zveřejní, pokud mu nezaplatíte výkupné.

ČASTÉ TRIKY PODVODNÍKŮ (POKRAČOVÁNÍ)

- ⚠ **Nabídka zboží v bazaru**, kdy chce podvodník peníze předem nebo zadat kartu
- ⚠ **Nabídka rychlého výdělku** bez práce: kryptoměny, binární opce, gambling, vícestupňový marketing, investice...
- ⚠ **Manipulátoři a trollové** mohou pomocí textů, videa či obrazů šířit nepravdivé či zkreslené informace s cílem vyvolat emocionální reakci nebo nedůvěru v systém

BUĎTE PODEZŘÍVAVÍ KE VŠEM SOUBORŮM. MOHOU SE V NICH SKRÝVAT VIRY NEBO ŠKODLIVÝ ČI VYDĚRAČSKÝ SOFTWARE.

- ⚠ **Falešný profil** na sociálních sítích z vás může lákat informace, které lze později použít k podvodu či krádeži
- ⚠ **Výhra, dědictví, soutěž** či jiná historka o nabytí peněz, ve skutečnosti podvod k vylákání peněz
- ⚠ **Falešná technická podpora** bude chtít na váš počítač nainstalovat software pro vzdálený přístup a tak jej ovládnout
- ⚠ **Žádost o pomoc v nouzi** může být falešná snaha o získání finančních prostředků pod záminkou smyšlené situace nebo neexistující charity
- ⚠ **Falešný policista nebo bankéř** bude tvrdit, že nesmíte nikomu o hovoru říci

Kdykoli máte nějaké podezření, zbystřete! **Požádejte o radu někoho, komu věříte.**

PENÍZE NA INTERNETU

Přes internet můžete snadno nakupovat nebo posílat peníze. Této jednoduchosti zneužívají i podvodníci. Buďte velmi obezřetní.

JAK VYBRAT E-SHOP

Česká obchodní inspekce radí vybírat takové e-shopy, které splňují následující:

- Uvádějí svou adresu, IČO, kontakt, mailovou adresu a nejlépe i telefon
- Obchod nabízí kromě platby předem i dobírku nebo osobní vyzvednutí
- Informují zákazníka o jeho právech

PO NÁKUPU V ČESKÉM E-SHOPU MŮŽETE **DO 14 DNŮ** OD PŘEVZETÍ ZBOŽÍ ODSTOUPIT OD SMLOUVY A **VRÁTIT** ZAKOUPENÉ ZBOŽÍ **BEZ UDÁNÍ DŮVODU**.

PODVODNÉ E-SHOPY ČASTO:

- ⚠ „Tlačí“ na zákazníka odpočítáváním času či falešnými recenzemi
- ⚠ Nabízejí „zázračné“ výrobky
- ⚠ Ohánějí se fiktivními doporučeními autorit
- ⚠ Neuvádějí adresu provozovatele
- ⚠ Nemají zabezpečení HTTPS
- ⚠ Neuvádějí složení výrobku
- ⚠ Doména neodpovídá nabízenému zboží
- ⚠ Prodávají za podezřele nízkou cenu

PORADNA ČESKÉ OBCHODNÍ INSPEKCE: **222 703 404** (PO – PÁ, 8 AŽ 16H)

BANKY A KARTY

Často se podvodníci snaží nabourat přímo do vašeho bankovního účtu. Na co dát pozor?

- **Nevěřte e-mailům**, které se tváří, že jsou od vaší banky. Pokud jste na pochybách, zavolejte do své banky přes číslo, které má banka na oficiálním webu (ne v mailu!).
- Nikomu **neposílejte kód**, který vám banka poslala v textové zprávě.
- Nepište **číslo své platební karty** na nezabezpečené stránky

Banky vám nebudou psát e-mailem ohledně peněz nebo přihlášení na účet.

PRÁCE S INFORMACEMI

Internet je komplikovaný. Snadno proto člověk udělá chybu, které později lituje.

- **Nezveřejňujte** na webu nebo sociálních sítích žádné **soukromé** informace (adresu, datum dovolené, fotku letenky či kreditní karty, rodné číslo apod.)
- **Nepřeposílejte** věci, které nemáte ověřené (řetězové dopisy, návody na zbohatnutí, pyramidové hry)
- **Buďte skeptičtí** k čemukoli, co ve vás vyvolá okamžité a **silné emoce**, může jít o past, propagandu či manipulaci
- **Zálohujte** svá data a mějte kontakt na důvěryhodného člověka, se kterým můžete řešit problémy počítače či mobilu
- Mějte zapnuté **aktualizace systému** a **neinstalujte programy** z neznámých zdrojů. Podvodníci jsou nesmírně vynalézaví a vytrvalí…

A KDYŽ SI NEJSTE JISTÍ, ZEPTEJTE SE!

Tento návod je určený k další úpravě a šíření na základě licence Creative Commons (BY-NC-SA). Autor: Pavel Kasík, pavelkasik.com, 2022 (v3)