AGORA
CENTRAL EUROPE

Na internetu? Bez starostí!

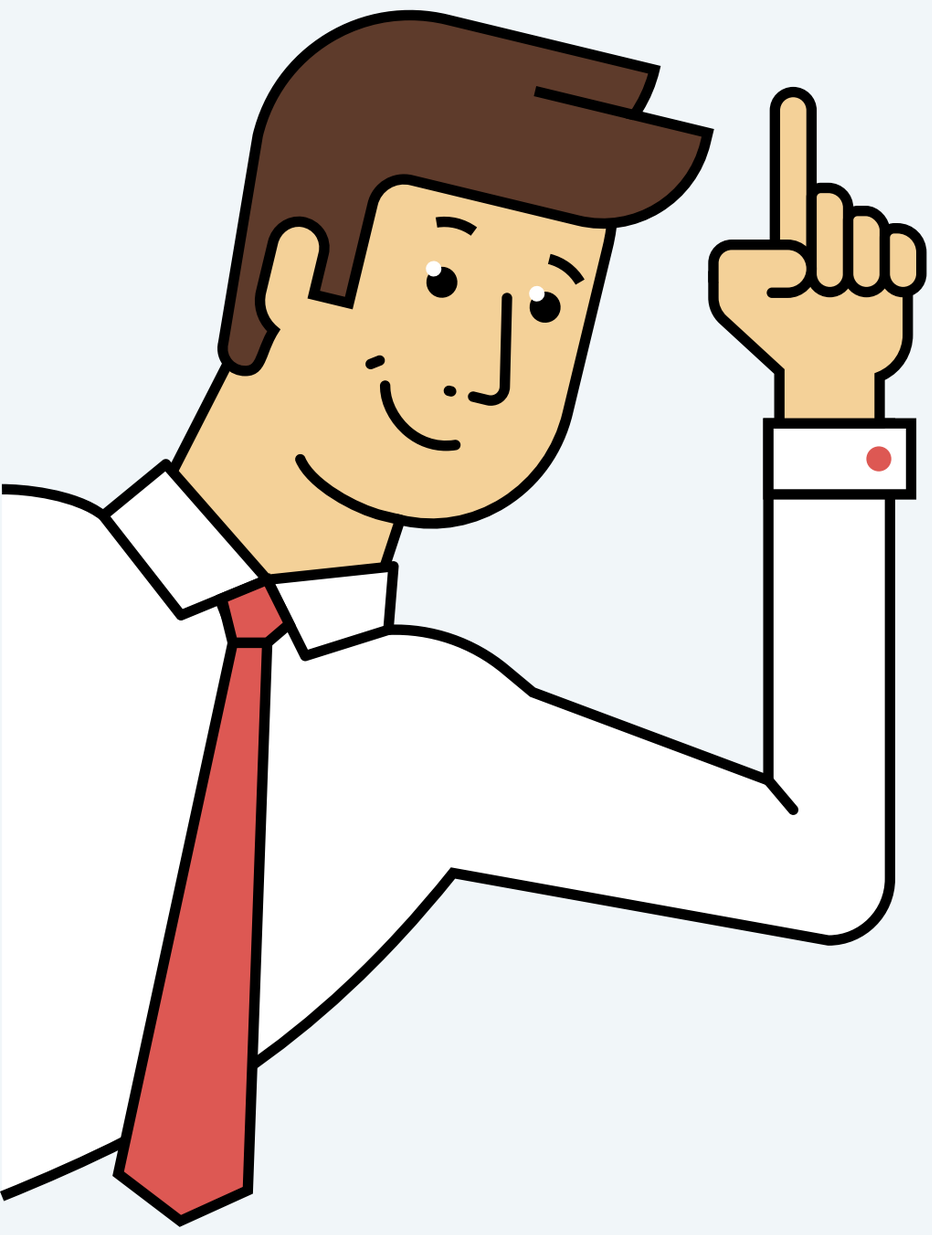
Manuál, jak surfovat po internetu,
a přitom nepřijít o své úspory

AGORA
CENTRAL EUROPE

Na internetu? Bez starostí!

Manuál, jak surfovat po internetu,
a přitom nepřijít o své úspory

Slovo úvodem



Občas si můžeme ze zpráv v médiích všimnout, že internetoví podvodníci vylákali z nějakého důvěřivce tu menší, tu větší finanční částku. Možná proto, že tyto zprávy nejsou v médiích každý den, můžeme nabýt pocitu, že se nás internetové podvody nebudou nikdy týkat a že se nenecháme jen tak napálit. Podvodníci ale používají čím dál sofistikovanější metody a ohroženi můžeme být opravdu všichni. To dokazuje statistika internetových podvodů za 1. pololetí roku 2023, kterou publikovala Česká bankovní asociace spolu s Policií ČR:

- **Internetoví podvodníci vylákali během tohoto období z klientů bank více než 674 milionů korun.**
- **Celkem na ně podnikli 31 233 útoků.**
- **Průměrná škoda na jednoho podvedeného dosáhla 21 522 korun.**
- **Nejčastěji se jednalo o podvodná volání, fiktivní investiční nabídky, inzertní podvody, nigerijské dopisy a podvody s falešnými webovými stránkami.**

Samozřejmě, ze strachu z možného podvodu se můžete vyhýbat internetovým platbám, komunikaci s jinými lidmi, či internet vůbec nepoužívat. To by byla ovšem chyba, protože internet poskytuje řadu možností, jak si zlepšit, zpříjemnit či zjednodušit život. Je to jako s reálným světem – musíme se v něm naučit žít, abychom si jej užívali plnými doušky.

Dominik Voráč

AUTOR PŘÍRUČKY

> ***Tento manuál vám přinese základní poznatky, jak se chovat ve světě internetu (a vlastně i mimo něj), abyste se nezapsali do podobné statistiky, jakou uvádíme výše.***

www.agorace.cz

E-mailová schránka

Využití e-mailové schránky je různé: můžete přes ni komunikovat se svými známými, dostávat (řetězové) e-maily, akční nabídky od různých prodejců, ale také e-maily, které vás mohou pěkně podvést.
Nejčastějšími podvody v e-mailové schránce jsou takzvané phisingové útoky (čtěte fišingové). Podvodníci při těchto útocích často využívají falešné e-maily, které vypadají jako zprávy od legitimních společností nebo institucí. Cílem je přimět uživatele k zadání osobních údajů, jako jsou hesla či čísla kreditních karet. Podvodníci se mohou vydávat například za instituce jako je Česká pošta, Česká správa sociálního zabezpečení či za vaši banku. E-mail ve většině případů obsahuje odkaz, na který musíte kliknout – po kliknutí se dostanete na podvodné stránky, které po vás chtějí například číslo kreditní karty, pin, přihlášení k bankovnímu účtu apod. Někdy vás donutí si stáhnout podvodný program.

Nejdůležitější je na takový odkaz vůbec neklikat. Jak už bylo řečeno, po kliknutí se vám může stáhnout do počítače škodlivý program, který ovládne váš počítač. Útočník pak může spravovat vaše hesla, dostat se do internetové bankovnictví, sledovat vaši komunikaci apod. Otevírejte tedy jen odkazy, které vedou na webové stránky, u nichž jste si jisti, že představují oficiální instituci.

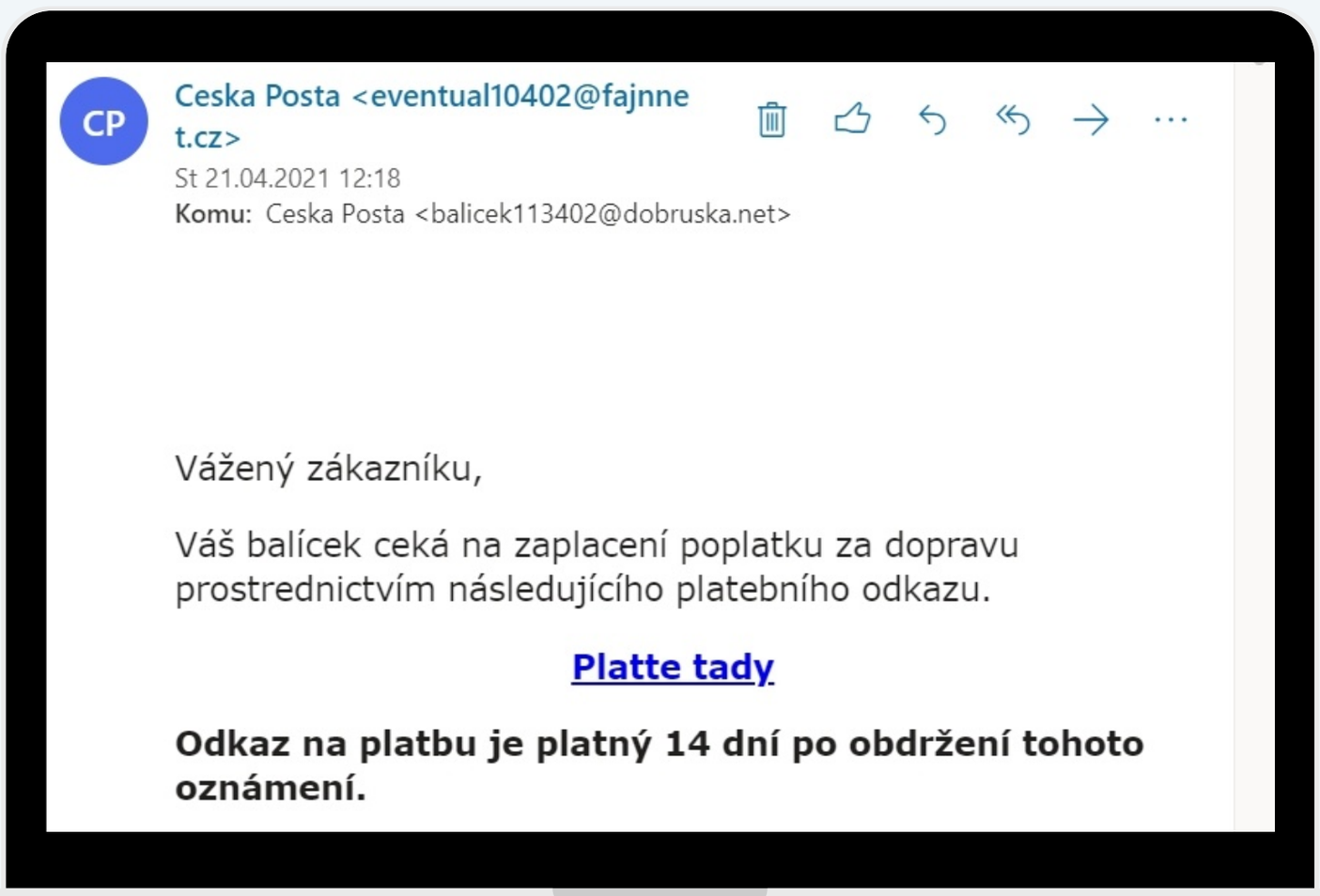
Jak poznat, že se jedná o falešný e-mail od České pošty?

1. Zeptejte se sami sebe, jestli v tomto okamžiku vůbec nějaký balíček očekáváte. Pokud nikoliv, už to by ve vás mělo vzbudit podezření.

2. Mnohé prozradí e-mailová adresa, odkud je e-mail poslán, což poznáte v kolonce „Od:“ (viz obrázek dole). Je zde sice jako jméno uvedeno „ČeskáPošta“ (i to, že nemá jméno mezeru, je podezřelé), ale samotný e-mail je (sup6a06…@icemanuae.com“ opravdu neodpovídá webové adrese oficiální instituce.

3. To, na jakou stránku vás odkaz navede, můžete ověřit pouhým najetím myši na text odkazu, přičemž se vám okamžitě ukáže jeho adresa. Pokud je adresa v tomto případě jiná než ceskaposta.cz, jedná se o podvod. NA DANÝ ODKAZ NEKLIKEJTE! Jaké má daná instituce webové stránky, se můžete vždy dozvědět pomocí vyhledávače (seznam.cz, google apod.).

4. K tomu, že se jedná o podvod, vás může také navést špatné a kostrbaté používání českého jazyka – většina podvodů je tvořena ze zahraničí pomocí strojového překladu, který může obsahovat různé chyby.



Příklad podvodného e-mailu. Je důležité se zaměřit na adresu odesílatele (eventual10402@fajnnet.cz). Může nám také napovědět nepříliš dobrá čeština a také možnost kliknutí na odkaz, který vede na podvodné stránky.
Zdroj obrázku: https://www.denik.cz/krimi/podvod-posta-balicek-email-falesny-20210528.html

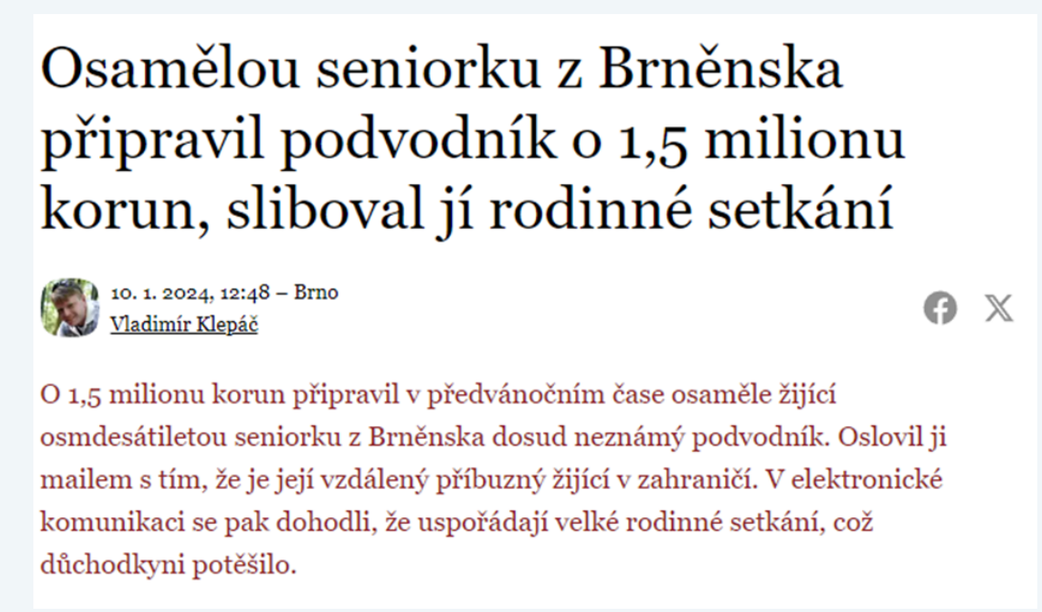
E-mailová schránka

Co dělat, když už jste na odkaz klikli a údaje vyplnili?
V tomto případě ještě nemusí být nic ztraceno, ale musíte rychle jednat. Někdy pomůže sama banka, která podvod rozpozná a kreditní kartu automaticky zablokuje. Na to ale spoléhat nemůžete. Proto raději co nejdříve kontaktujte banku s prosbou o zablokování karty. Tím zabráníte, aby útočníci vaši kartu dále používali. Pokud máte stejné heslo do internetového bankovnictví a jiných služeb, jako jste vyplnili na falešné stránce, okamžitě všechna hesla změňte. Nejdůležitější je ovšem prevence – kromě obezřetnosti si například můžete nastavit maximální výši platby, která může z vaší kreditní karty odejít. Pokud útočník tento limit vyčerpá, další platby už provést nemůže a vy máte alespoň více času na zablokování karty.

Dalším příkladem podvodných e-mailů jsou tzv. **scamy** (čtěte skemy, česky podvody), které jsou rafinovanější a využívají komunikaci útočníka s jeho obětí. Prvním příkladem jsou nigerijské dopisy, které se vyznačují tím, že oběti dostanou e-mail od někoho, kdo tvrdí, že je bohatým cizinzem (původně se v mnoha případech jednalo o osobu z Nigérie), který potřebuje pomoc s přesunem velké sumy peněz. V těchto e-mailech je oběti slíbena odměna.

Obvykle se od oběti vyžaduje, aby poskytla své osobní informace a zaplatila nějaké poplatky nebo daně, aby transakce mohla pokračovat. Tyto poplatky jsou prezentovány jako nezbytnost k pokrytí různých fiktivních nákladů, jako jsou právní poplatky, úplatky pro úředníky nebo bankovní poplatky. Jakmile oběť zaplatí, podvodník buď požádá o další platby z různých důvodů, nebo se již jednoduše neozve.

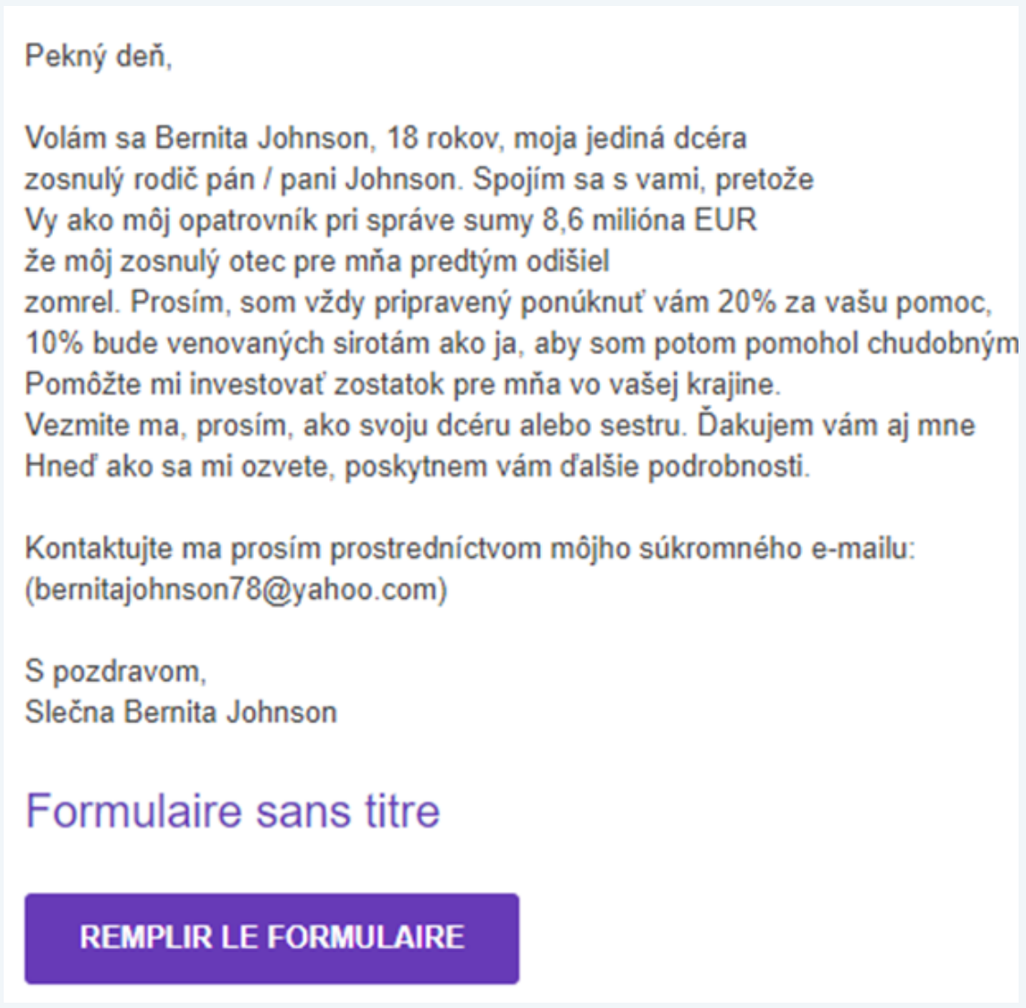
Dalším příkladem podvodu přes e-mail je **romance scam** (romantický scam), V tomto případě vytvoří podvodník falešný profil, přičemž naváže vztah s obětí. Cílem je vytvořit důvěru a citovou připoutanost mezi podvodníkem a obětí. Jakmile se to podaří, pachatel obvykle přistoupí k žádosti o peníze, tvrdíc, že se ocitl v nesnázích nebo má naléhavou situaci, při níž potřebuje peníze. Takové situace mohou zahrnovat sofistikované lži o náhlých zdravotních problémech, potížích s cestováním (například uvíznutí v cizině, potřeba peněz na letenku) a další. Oběti, které jsou přesvědčeny, že s danou osobou mají vztah, chtějí pomoci, a často posílají velké sumy peněz. Po odeslání peněz podvodník buď požaduje více peněz z různých důvodů, nebo jednoduše zmizí. Podvodníci se ovšem mohou vydávat například i za vzdálené příbuzné, čímž mohou opět vylákat z osamělých obětí toužících po rodinném setkání nemalé peníze (viz obrázek vpravo).



Osamělou seniorku z Brněnska připravil podvodník o 1,5 milionu korun, sliboval jí rodinné setkání

10. 1. 2024, 12:48 – Brno
Vladimír Klepáč

O 1,5 milionu korun připravil v předvánočním čase osaměle žijící osmdesátiletou seniorku z Brněnska dosud neznámý podvodník. Oslovil ji mailem s tím, že je její vzdálený příbuzný žijící v zahraničí. V elektronické komunikaci se pak dohodli, že uspořádají velké rodinné setkání, což důchodkyni potěšilo.



Pekný deň,

Volám sa Bernita Johnson, 18 rokov, moja jediná dcéra
zosnulý rodič pán / pani Johnson. Spojím sa s vami, pretože
Vy ako môj opatrovník pri správe sumy 8,6 milióna EUR
že môj zosnulý otec pre mňa predtým odišiel
zomrel. Prosím, som vždy pripravený ponúknuť vám 20% za vašu pomoc,
10% bude venovaných sirotám ako ja, aby som potom pomohol chudobným
Pomôžte mi investovať zostatok pre mňa vo vašej krajine.
Vezmite ma, prosím, ako svoju dcéru alebo sestru. Ďakujem vám aj mne
Hneď ako sa mi ozvete, poskytnem vám ďalšie podrobnosti.

Kontaktujte ma prosím prostredníctvom môjho súkromného e-mailu:
(bernitajohnson78@yahoo.com)

S pozdravom,
Slečna Bernita Johnson

Formulaire sans titre

REMPLIR LE FORMULAIRE

Příklady romantických scamů. Zdroj článku: novinky.cz

Podvodníci se tedy mohou vydávat za kohokoliv – oficiální instituci, kamaráda, příbuzného, či vašeho potenciálního nápadníka. Přistupujte proto k těmto e-mailovým zprávám pozorně a nikdy nikomu neznámému neposílejte citlivé údaje: čísla karet, pin kód či hesla k vašim účtům! Dále důrazně doporučujeme neotvírat žádné přílohy e-mailu, které obsahují koncovku .exe.

Web a sociální sítě

Podobná nebezpečí jako u e-mailové schránky na vás mohou čekat i na webech a sociálních sítích, akorát že místo toho, aby vás podvodníci oslovili přes e-mail, osloví vás přes sociální síť či seznamovací aplikaci. Některé podvody ale můžete najít přece jen více na webech než v e-mailu.

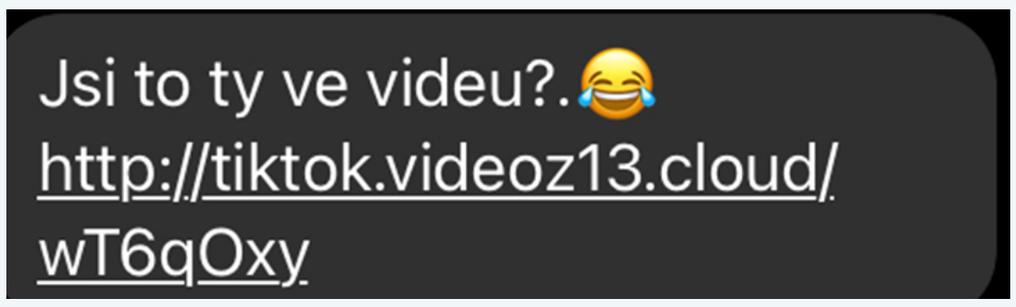
Podvodné weby fungují na stejném principu jako předchozí podvody – podvodník se k vašim penězům může dostat pomocí vašeho vyplnění citlivých údajů na stránkách, popřípadě vám dá pokyn, ať za účelem investice pošlete své peníze na nějaký účet. Nejen u investic, ale u všech finančních transakcí na internetu je důležité, abyste si vyhledali informace o webových stránkách a rovněž prověřili, zdali se jedná o oficiální instituce!

Bazarové podvody

Když prodáváte nějaké zboží na internetu, může se stát, že vás osloví zájemce, který po vás ale z nějakého důvodu bude chtít, abyste mu zaslali své údaje, popřípadě je vyplnili na webových stránkách. Těmito důvody například může být to, aby byla platba rychlejší, popřípadě že je kupující zdaleka, a proto zajistí doručení kurýrem. V tomto případě opět platí, že nikam své údaje neposíláte! Doporučujeme být obezřetní a řídit se zlatým pravidlem – pokud něco prodávám, nikde nevyplňuji údaje o své platební kartě ani ničem jiném. Raději doporučujeme v tomto případě předání z „ruky do ruky“.

Zprávy na komunikačních platformách

Někdy se může stát, že vám váš známý pošle jednoduchou zprávu s odkazem na cizí stránky. V tomto případě buďte obezřetní, protože počítač vašeho známého mohl být napaden a teď odesílá phisingové zprávy s podvodnými odkazy. Radíme se nejdříve podívat na odkaz – pokud je neznámý, neotvírejte jej. A také se raději známého zeptejte, zdali tu zprávu psal on, nebo někdo jiný. Příkladem takové zprávy je obrázek níže.



Dalším příkladem podvodné zprávy může být, když vám kamarád napíše, že potřebuje vaše číslo – a to z toho důvodu, že jej ztratil, nebo že díky tomu získáte něco zdarma. Následně vás poprosí o zaslání ověřovacího kódu. V tomto případě se ale nejedná (s největší pravděpodobností) o známého, ale o podvodníka, který se dostal do jeho účtu. Díky tomu, že mu zašlete ověřovací kód, za něj můžete zaplatit určitou finanční transakci, či se vám také může nabourat do vašeho účtu.

Nabídky investování

Poslední dobou se rozvinuly podvody s webovými stránkami, které lákají na výhodné zisky z investic. Na tyto podvodné stránky lze narazit i pomocí reklam na webech, kdy se podvodníci zaštiťují známými firmami či osobnostmi (viz obrázek). V tomto případě je nutné si něco o dané firmě vyhledat. Na obrázku níže vidíme, že se naprosto neznámá firma firma frogolover invest zaštiťuje prezidentem ČR. Má se jednat údajně o akcie ČEZ, ale firma tomu neodpovídá.

Telefonní hovory

Ještě zákeřnější než internetové podvody jsou podvody spojené s telefonními hovory. Může se vám tak stát, že vezmete hovor od neznámého čísla a někdo po vás bude chtít číslo vaší kreditní karty s pinem či přihlášení do internetového bankovnictví například pod záminkou, že vám byl napaden účet. Nejčastěji se jedná o údajné pracovníky banky, policisty či lékaře. Na hovor jsou navíc dobře připraveni, protože znají vaše jméno či číslo účtu nebo vaši adresu – někdy jdou totiž tyto údaje zjistit z veřejných zdrojů. **Legitimní organizace, jako jsou banky nebo daňové úřady, nikdy nepožadují citlivé informace, jako jsou hesla nebo PIN kódy, přes telefon. V případě pochybností je vždy nejlepší kontaktovat danou instituci přímo pomocí oficiálních kontaktních údajů.**

Podvodníci byli opět úspěšní. Po telefonu od ženy vylákal více než milion korun

29.7.2022

Nikola Čížková
Reportérka
Napište mi

Pardubičtí kriminalisté prověřují další z případů podvodů, ve kterém hraje hlavní roli neznámý pachatel, či spíše pachatelé. V podvodu sehrál roli falešný policista i bitcoinmat. Vše začalo telefonátem, ve kterém se měl ozvat muž, který se vydával za zaměstnance jedné z bank.

Oběti podvodných telefonátů mohou přijít i o miliony. Zdroj článku: denik.cz

1 Pracovník banky

Pan David K. obdrží telefonát od osoby, která se vydává za zaměstnance jeho banky. Tato osoba tvrdí, že došlo k podezřelé aktivitě na jeho účtu a je nutné ověřit jeho údaje pro zabezpečení účtu. David K. je požádán, aby sdělil své přihlašovací údaje do internetového bankovnictví a kód, který mu přijde SMS zprávou. Po telefonátu zjistí, že z jeho účtu byly vyvedeny všechny finanční prostředky.

2 Živnostník

Živnostník dostane telefonát od údajného zaměstnance daňového úřadu, který tvrdí, že má nedoplatek na daních, a pokud nezaplatí okamžitě, bude proti němu zahájeno právní řízení. Útočník žádá okamžitý převod peněz na uvedený účet. Živnostník, pod tlakem a v obavě z právních problémů, posílá požadovanou částku. Později zjišťuje, že nešlo o legitimní požadavek a že peníze byly odeslány na účet podvodníka.

3 Technická zpráva

Žena dostane telefonát od osoby, která se vydává za technika známé softwarové společnosti. Tato osoba tvrdí, že na jejím počítači byl detekován vážný bezpečnostní problém a že je nutné okamžité řešení. Podvodník žádá ženu, aby mu poskytla vzdálený přístup k jejímu počítači a platbu za službu. Po poskytnutí přístupu útočník nainstaluje škodlivý software a získává přístup k citlivým datům. Díky tomu se pak dostane prakticky ke všem penězům, které žena vlastní.

3 Dobročinná pomoc

Pár týdnů po velké přírodní katastrofě obdrží Monika P. telefonát od osoby, která se vydává za zástupce mezinárodní dobročinné organizace. Ta žádá o finanční příspěvek na pomoc postiženým přírodní katastrofou. Předstírá naléhavost situace , přičemž žádá o okamžitý převod peněz na speciální účet. Monika P. posílá peníze. ale později zjišťuje, že organizace, na kterou přispěla, ve skutečnosti neexistuje a že její finanční prostředky byly odeslány přímo podvodníkovi.

Osmero pravidel bezpečnosti nejen na internetu

1. Buďte pozorní

Pokud vás někdo neznámý osloví, ať už s určitou nabídkou, prosbou či důležitým upozorněním týkajících se vašich financí, zpozorněte a spíše danému člověku nevěřte.

2. Pozor na odkazy

Před kliknutím na odkaz stránek, které chcete navštívit, se podívejte, jak vypadají. Podvodné weby používají napodobeniny webů oficiálních institucí: například místo www.zasilkovna.cz může adresa vypadat jako www.zasilkovna.sitecz.cz. Oficiální instituce používají většinou co nejjednodušší webovou adresu.

3. Poznejte webové adresy oficiálních institucí

Pokud chcete mít pocit naprosté bezpečnosti, ale chcete využívat internet naplno, využívejte jen ty webové stránky, které již dobře znáte. U těch, které neznáte, se podívejte na jejich webovou adresu, a v případě, že chcete zadávat své údaje v rámci nějaké neznámé webové stránky, ověřte si pomocí vyhledávače Google, zda není falešná.

4. Pozor na citlivé údaje

Nikdy neposkytujte cizím osobám citlivé údaje typu číslo karty a pin kód ke kartě. Nikdy také nikomu neposkytujte přihlašovací údaje do různých účtů. A už vůbec ne do internetového bankovnictví.

5. Nakupujte přes ověřené e-shopy

Chcete-li platit za zboží přes internet, provádějte tak přes známé e-shopy, které můžete najít na stránce heureka.cz. Tyto e-shopy po vás budou při nákupu požadovat číslo platební karty a takzvaný CVC/CVV kód, který se nachází na zadní straně vaší karty. Většinou pak bude po vás vyžadováno potvrzení platby přes mobilní telefon.

6. Pozor na přílohy e-mailů či stahování zvláštních souborů

Pokud stahujete soubory (například v rámci přílohy e-mailu), dejte si pozor, o jaký typ souboru se jedná. Pokud se jedná o fotky (například s příponou .png či .jpg), jsou bezpečné. Největší nebezpečí skrývají soubory s příponou .exe. Podvodníci navíc jména souborů kamuflují, aby si dotyčný myslel, že vypadají jako obrázky, důležitá je ovšem přípona. Například soubor s názvem *Kopie dokladu o transakci_14_09_2021.exe* je nebezpečný, protože se nejedná o žádný obrázek.

7. Vzdělávejte se

Doporučujeme si vyzkoušet vědomostní test na tuto problematiku na webu kybertest.cz, dále doporučujeme webové stránky https://www.jaknainternet.cz/ či https://saferinternet.cz/. Můžete také sledovat oficiální stránky Policie ČR.

8. Buďte obezřetní, ale nebojte se

Internet je skvělé místo, které nabízí spoustu možnosti pro zpříjemnění a zjednodušení života. Pokud se naučíte základní pravidla bezpečnosti na internetu, nemusíte se bát. Můžete poprosit známé, aby vám pomohli s internetovým bankovnictvím či s koupí zboží na internetu. Ale vždy myslete na to, co je psáno v tomto manuálu.

Pár pojmů na závěr

1. **Phishing** [fišin]

Druh internetového podvodu, kdy útočníci posílají falšované e-maily nebo zprávy, které se tváří jako od legitimních společností nebo známých osob. Cílem je přimět oběti k prozrazení osobních údajů, jako jsou hesla, čísla kreditních karet nebo další citlivé informace. Phishingové zprávy mohou obsahovat odkazy na podvodné webové stránky, které se vzhledem podobají legitimním, nebo přílohy obsahující škodlivý software.

2. **Smishing** [smišin]

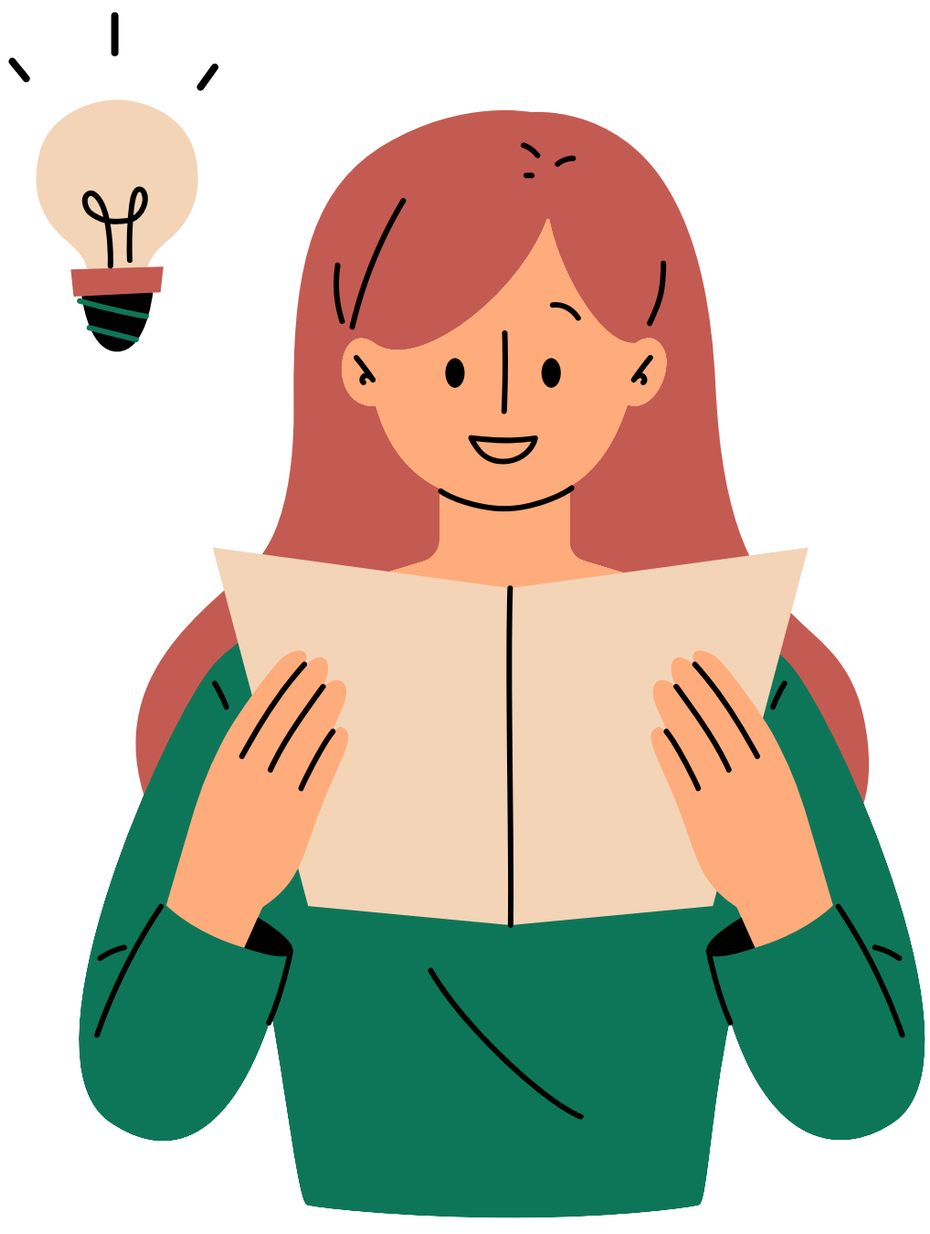
Smishing je forma phishingu, která využívá SMS zprávy jako kanál pro podvod. Útočníci posílají textové zprávy, které se tváří jako od důvěryhodných zdrojů, s cílem přesvědčit oběti k akcím, které mohou vést k odcizení osobních údajů nebo finančních ztrát. Zprávy mohou vyzývat k okamžitému jednání, například k potvrzení údajů účtu nebo k přístupu na odkaz, který vede na podvodnou stránku.

3. **Vishing** [višin]

Vishing je technika podvodu, kdy útočníci používají telefonní hovory k získání citlivých informací od obětí. Útočník se může vydávat za zaměstnance banky, technické podpory nebo jiné důvěryhodné instituce. Útočníci mohou používat přesvědčivé scénáře, aby přiměli oběti prozradit osobní údaje nebo dokonce přímo převést peníze na účty řízené podvodníky.

4. **Malware** [malvér]

Malware či škodlivý software je termín označující jakýkoliv software vytvořený s úmyslem poškodit, narušit nebo neoprávněně získat přístup do počítačového systému. Malware se může šířit prostřednictvím infikovaných e-mailových příloh, škodlivých webových stránek, stahování softwaru z nespolehlivých zdrojů nebo prostřednictvím jiných typů sítových útoků. Jakmile je systém infikován, malware může ukradnout osobní údaje, šifrovat nebo mazat data, monitorovat online aktivitu uživatele, nebo využívat systém k šíření dalšího malware.



Partneři projektu

AGORA CENTRAL EUROPE

Norway grants

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Studijní a vědecká knihovna v Hradci Králové

Bibliothek Liberec
Knihovna Liberec
Library Liberec

Text a grafika: **Dominik Voráč**

Vydavatel: **Agora CE, o. p. s.**

Příručka vznikla za přispění finanční podpory z projektu Fondy EHP/Norské fondy 2014–2021, program Vnitřní věci