



Digital Security
Progress. Protected.

Podvody na internetu:

Jak se chránit před hrozbami





Informace v této brožuře vám pomohou být o krok napřed před kybernetickými zločinci. Nejnovější informace o bezpečnosti digitálních technologií najdete na www.Dvojklik.cz.

Obsah

Úvod

Podvody na internetu

- Příběh I. Phishing
- Jak poznat, že jde o podvod?
- Jak na incident reagovat?

Krádež a zneužití identity

- Jak poznáte, že jste se stali obětí krádeže či zneužití identity?
- Jak se vyhnout krádeži identity?
- Jak ověřit e-mail, jestli pochází od legitimního zdroje?

Falešné obchody a inzeráty – bazarové podvody

- Prodávající v roli oběti
- Příběh II. Podvod na Marketplace
- Kupující v roli oběti

Podvody na e-shopech

- Jak se vyhnout podvodům na e-shopech?

Podvody se vstupenkami

Podvody s kryptoměnami

- Typy investičních podvodů
- Jak se nestát obětí kryptoměnového podvodu?

Úvod

Různé formy podvodů a kybernetických hrozeb se stávají neodmyslitelnou součástí fungování na internetu. Ochrana proti těmto hrozbám vyžaduje nejen technologické znalosti, ale také zvýšenou schopnost rozpoznávání podezřelých situací a rafinovaných triků. V této příručce se podíváme na nejčastější podvody, které na internetu hrozí. Ukážeme si, jak je poznat a jak se jim efektivně bránit či vyhnout.



Podvody na internetu

Častou technikou podvodů na internetu je **tzv. phishing**. Nejčastěji se jedná o falešné e-maily, které vypadají jako oficiální komunikace od bank či vládních institucí. Prostřednictvím těchto e-mailů se však útočníci snaží vylákat z uživatelů citlivé údaje, jako jsou přihlašovací jména, hesla nebo dokonce údaje k vašemu platebnímu účtu nebo platební kartě.

Kyberzločinci k útokům využívají také **sociální sítě**. Vydávají se třeba za Facebook a tvrdí,

že se někdo mohl přihlásit k vašemu účtu, že bylo resetováno vaše heslo nebo cokoli jiného, co vyvolá pocit naléhavosti. Připojí také odkaz, na kterém se můžete k účtu přihlásit, heslo obnovit a účet zachránit. Odkaz vás však přesměruje na falešnou přihlašovací stránku Facebooku, skrze kterou se v dobré víře přihlásíte ke svému účtu. Svě heslo tímto způsobem předáte rovnou do rukou útočníků. Pokud používáte stejné heslo i do dalších služeb, ohrozíte tím i je.

Příběh I. Phishing

Podvodníci posílali z čísla 778 507 689 SMS s informací o neuhrazeném dluhu a odkazem na falešný web, který se vydával za oficiální registr exekucí www.exekuceinfo.cz, kde jste měli stav své exekuce zkontrolovat.

Ukázka falešné aplikace

 EXEKUCEINFO.CZ

O služběKontaktPřihlásit

OKAMŽITÉ OVĚŘENÍ INFORMACÍ Z REGISTRU EXEKUCÍ!

 **Identita občana**

Přihlaste se pomocí identifikace BankID a zjistíte své dluhy. Určeno pro právnické a fyzické osoby. Výpis s informacemi o dluzích, které jsou vymáhány v podobě exekuce, je k dispozici ihned online.

☐ Souhlasím s obchodními podmínkami

PRIHLASIT SE

Výpisy exekucí jsou z **oficiální exekuční databáze** vedené a spravované **Exekutorskou komorou ČR**. Veškeré dotazy do této exekuční databáze jsou **zpoplatněny na základě vyhlášky vydané Ministerstvem spravedlnosti č. 329/2008 Sb.**

Přivodce a další informace:  Milostivé léto 2023 | Registr exekucí | Registr dlužníků | Výpis exekuce | Centrální evidence exekucí | Exekuční rejstřík | Registr dlužníků - Oficiální registr
Copyright 2004-2023, GetData s.r.o., Roháčova 145/14, 130 00 Praha 3, Česká republika | IČO: 27102343 | Městský soud v Praze, oddíl C, vložka 96380 | [Obchodní podmínky](#)



Přihlášení do falešného internetového bankovníctví

Přihlášení do domnělé aplikace fungovalo pouze pomocí tzv. BankID, tedy přihlášením do internetového bankovníctví, které bylo také falešné.

← → ↻ 🔒 https://exekuceinfoccz.pro/moneta ☆ — | 100% | + 🔍 Search ⬇️ 🌐 S 🔄 📄

MONETA MONEY BANK 📞 224 443 636 🗣️ English version

POZOR, Vaše přihlašovací údaje mohou být v nebezpečí, proto od 1. dubna zrušíme možnost přihlášení přes SMS

Přihlaďte se přes mobilní aplikaci Smart Banka, díky které budou Vaše přihlašovací údaje v bezpečí před phishingovými útoky, protože kombinace ID, hesla a kódu z SMS představuje za určitých okolností bezpečnostní riziko.

- 🔑 Bezpečnější přihlášení přes Smart Banku
- 🔒 Ochrana před viry a malware
- 👤 Přihlašování a placení biometrikou
- 🛡️ Dvojitá ochrana díky PINu
- 🛡️ Maximální chrání před phishingovými útoky

[Více informací o připravovaných změnách](#)

Přihlášení

ID

Heslo

Přihlásit

[Nápověda pro přihlášení](#)
[Problémy s předvyplňováním údajů?](#)

Útočníci se tímto způsobem chtěli dostat k bankovnímu účtu oběti. Další možnosti přihlášení do Identity občana (přes datovou schránku nebo mojeID) nebyly vůbec k dispozici.

POKUD NEJSOU K DISPOZICI VŠECHNY OBVYKLÉ FUNKCIONALITY WEBU, NAPŘ. ZPŮSOBY PŘIHLÁŠENÍ, ZPOZORNĚTE. MŮŽE JÍT O VAROVNÉ ZNAKY, ŽE S WEBOVOU STRÁNKOU NENÍ NĚCO V POŘÁDKU.

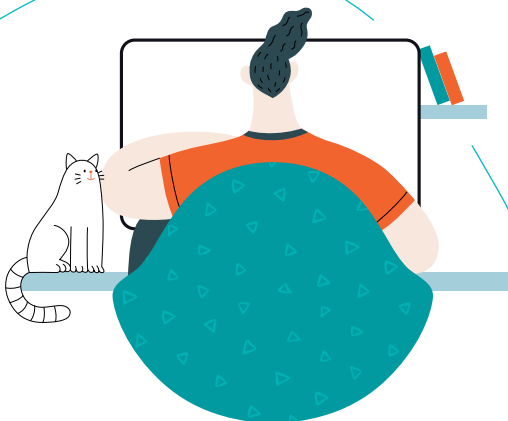
Tlačítko pro přihlášení navíc obsahuje překlep. Jedná se o malý detail, který vás ale může na podvod včas upozornit a varovat ještě před tím, než někam zadáte svoje přihlašovací údaje. Po podrobnějším zkoumání stránky zjistíte, že odkazy v zápatí jsou také nefunkční.

Jak poznat, že jde o podvod?

- 1 Může vás upozornit samotná SMS zpráva. Textové zprávy nejsou oficiálním informačním kanálem státních institucí.
- 2 Zprávu zpravidla obdržíte neočekávaně a nevyžádaně.
- 3 Upozornit vás může také přílišná naléhavost zprávy – máte ihned něco zkontrolovat nebo provést nějakou akci.
- 4 Webové stránky, na které vede proklik z SMS zprávy nebo e-mailu, obsahují chyby, některé části nemusí být přeložené vůbec a URL adresa neodpovídá té oficiální.

Jak na incident reagovat?

- 1 Na podobné odkazy v ideálním případě vůbec neklikajte. Na weby úřadů bychom neměli přistupovat z odkazů v SMS zprávách nebo z e-mailů.
- 2 Pokud si chcete zkontrolovat výši exekuce, oficiální adresu exekuční databáze zadejte přímo do adresního řádku prohlížeče.
- 3 Pokud jste již zadali na falešný web své přihlašovací nebo bankovní údaje a zjistili jste, že jste se stali obětí podvodu, je třeba informovat o podvodu samotnou instituci, svoji banku, a v případě vzniklých škod i Policii ČR.
- 4 Změňte si všechna hesla tam, kde používáte stejnou kombinaci přihlašovacích údajů, které jste útočníkům poskytli.



Krádež a zneužití identity

Krádež identity je v digitálním světě závažným problémem. Vedle tradičních forem podvodů (např. phishing) jsme stále častěji svědky sofistikovanějších technik, jako je catfishing, romance scamy nebo grooming.



Catfishing spočívá ve vytvoření falešné identity (zpravidla na sociálních sítích) za účelem kompromitování, kyberšikany nebo krádeže osobních údajů či finančních prostředků oběti.

Romance scam je podvodná praktika, při které se pachatel vydává za potencionálního partnera. Ve chvíli, kdy útočníci získají důvěru, žádají své oběti o peníze nebo osobní informace pod záminkou nouze, zdravotních problémů nebo jiných falešných příběhů.

Grooming je manipulativní taktika, při které se pachatelé snaží navázat důvěrný vztah s dětmi nebo mladistvými. Cílem jsou často psychické manipulace, sexuální zneužívání nebo jiné formy vykořisťování.

Sextorze je forma kybernetického vydírání, při které útočník využívá intimních fotografií nebo

videí oběti k vydírání nebo manipulaci. Útočník hrozí zveřejněním či sdílením těchto materiálů, pokud oběť nesplní jeho požadavky, které často zahrnují peněžní platby nebo další činnosti.

Dalšími terčí útoků se mohou stát vaše **zdravotní údaje či investice**. Útočníci vás mohou nalákat na falešné charitativní kampaně nebo nejrůznější žádosti o pomoc, aby získali peníze od soucitných lidí. Stranou nezůstávají ani **falešné pracovní nabídky**.

Když útočník nasbírá dostatečné množství citlivých dat, může se pokusit napodobovat identitu oběti pro různé aktivity – žádost o půjčku, nákup zboží na internetu, výběr peněz z bankomatu a podobně. Takové podvodné jednání potom označujeme jako **krádež identity (identity theft)**.

**DŮVĚRYHODNÉ ORGANIZACE NIKDY NEBUDOU ŽÁDAT O CITLIVÉ INFORMACE PROSTŘEDNICTVÍM E-MAILU NEBO NEZABEZPEČENÉHO KANÁLU.
BUĎTE OBEZŘETNÍ VŮČI OSOBÁM, S NIMIŽ INTERAGUJETE POUZE ONLINE.**

Jak poznáte, že jste se stali obětí krádeže či zneužití identity?

1

Neobvyklé finanční transakce

Pokud zjistíte náhlé a neobvyklé transakce na svých bankovních účtech, platebních kartách nebo jiných účtech, které jste neautorizovali, může to být indikace, že někdo používá vaše údaje.

2

Upomínky na dluhy nebo účty

Pokud dostáváte upomínky na dluhy, faktury nebo účty za služby, které jste nevyužívali, je možné, že někdo vytvořil účet na vaše jméno.

3

Nedostupnost důležité pošty

Pokud přestane přicházet důležitá pošta, jako jsou bankovní výpisy, platby nebo úřední dokumenty, mohlo by to znamenat, že vám někdo změnil adresu.

4

Nedostupnost vašich účtů

Pokud najednou zjistíte, že se nemůžete přihlásit do svých online účtů, je to zřejmě důsledkem zneužití.

5

Neobvyklé zprávy a volání

Nedůvěryhodné e-maily, zprávy nebo telefonáty, které žádají o vaše citlivé informace nebo o zaslání peněz, mohou být známkou podvodníků snažících se získat vaše údaje.

6

Zprávy o otevření nových účtů

Pokud obdržíte zprávu o otevření účtu nebo půjčky, o které jste nepožádali, mohlo by to být varování před zneužitím identity.



Naše doporučení

Buďte obezřetní a pravidelně kontrolujte své účty. Pokud narazíte na některý z výše uvedených znaků, měli byste co nejdříve jednat a prověřit možnou krádež identity. Mějte také na paměti, že prevence a správné digitální návyky mohou výrazně snížit riziko krádeže identity.



Jak se vyhnout krádeži identity?

- 1** Používejte **silná, unikátní hesla** pro každý účet. Heslo může být fráze nebo kombinace symbolů. Nemělo by být založeno na žádných informacích, které veřejně sdílíte, jako je datum narození, jméno, adresa apod. Heslo by mělo být dostatečně dlouhé (alespoň 8 znaků) a mělo by obsahovat alespoň jedno velké písmeno, speciální symbol (například @, \$, #, &, /, >, !) a několik číslic. Dobře se pamatují např. heslové fráze typu POUživ4m_Ese+ nebo používejte [generátor hesel](#), který vám pomůže vytvořit komplexní heslo. [Správce hesel](#) zase umožní hesla ukládat v zašifrované podobě. Přihlašujete se jedním hlavním heslem a program pak hesla automaticky vypisuje do přihlašovacích oken.
- 2** Pokud je to možné, povolte pro své online účty **vícefázové ověření**. Toto opatření znamená, že kromě hesla budete muset použít ještě další ověření při přihlášení (může to být např. kód z SMS nebo potvrzení v ověřovací aplikaci).
- 3** Buďte opatrní, jaké osobní údaje sdílíte online. **Vyhňte se sdílení citlivých informací** na veřejných fórech a sociálních sítích.
- 4** Mějte zapnuté **výstrahy na přihlášení k vašemu účtu**. Upozornění obdržíte vždy, když se k němu někdo pokusí přihlásit z nového zařízení nebo neobvyklé lokality. Pokud jste to nebyli vy, můžete dle pokynů v e-mailu obnovit heslo a svůj účet zabezpečit.
- 5** **Aktualizujte pravidelně operační systémy**, používané aplikace a [antivirový software](#) na svých zařízeních, abyste minimalizovali riziko kybernetických útoků.
- 6** Před kliknutím na odkaz v e-mailu si ověřte, zda je **e-mail skutečně od legitimního zdroje**.
- 7** Používejte **zabezpečené sítě Wi-Fi** a vyhněte se připojení k veřejným nezabezpečeným sítím, které mohou být snadným cílem pro útočníky.





Jak ověřit, jestli e-mail pochází od legitimního zdroje?

- 1 Začněte tím, že si důkladně přečtete obsah e-mailu. Zaměřte se na gramatické chyby a neobvyklé formulace. Chyby v textu, často i drobné nesrovnalosti, mohou naznačovat podvod.
- 2 Zkontrolujte e-mailovou adresu odesílatele. Někdy se může podvodná adresa velice podobat té pravé, například jako „support@paypal-security.com“ místo skutečné „paypal.com“. I malá odchylka může být znakem podvodu.
- 3 Zkontrolujte adresu odkazu. Pokud se v e-mailu nachází odkaz, neklikajte na něj. Místo toho přejeďte kurzorem myši nad odkaz, abyste získali náhled na jeho skutečnou adresu. Porovnejte ji s oficiální webovou stránkou, ke které by měl odkaz směřovat. Pokud se adresa liší nebo působí podezřele, neklikajte na odkaz.
- 4 Pokud dostanete e-mail, který se tváří jako důležitá komunikace od banky nebo jiné instituce, raději si zjistěte kontakt na tuto instituci sami z oficiálních zdrojů (např. oficiální webové stránky, kontaktní telefonní číslo atd.) a ověřte, zda jsou zprávy skutečné.
- 5 Používejte funkci [zabezpečeného prohlížeče](#), která umí podezřelé weby blokovat.

Falešné obchody a inzeráty

V posledních letech stoupá počet útoků, které nazýváme bazarové podvody či podvody na internetových tržištích, jako je Bazoš, Vinted, Sbazar nebo Marketplace na Facebooku. Stále častěji se do role obětí dostává paradoxně prodávající, takové podvody označujeme jako reverzní inzertní podvody.



PRODÁVAJÍCÍ V ROLI OBĚTI

Jak fungují podvody na internetových bazarech?

Útok často začíná oslovením na platformě online tržiště, ze které se útočníci snaží přesunout konverzaci do chatovací aplikace (nejčastěji WhatsApp, Viber, Messenger) nebo do SMS. Děje se to proto, že internetová tržiště se snaží čím dál více posilovat svoji obranu proti podvodům a mohou účty podvodníků zachytit a blokovat, nebo oběť včas upozornit.

Útočníci se tváří jako zájemci o koupi zboží a nabízejí prodejci, aby si ho předali přes přepravce, jako je například DPD, GLS nebo Zásilkovna. Prodejci (oběti) zašlou odkaz na platební bránu, přes kterou má obdržet platbu za prodávané zboží. Brána často vyžaduje osobní údaje a údaje o platební kartě. Jakmile prodejce v svoje údaje vyplní, začne jej útočník okrádat o peníze z karty.

Dalším scénářem může být, že útočníci požadují zaplacení jistiny pro případ, že by mu prodávající nic neodeslal nebo balíček přišel poškozený. Falešnou platební bránu potom vydávají za úschovnu peněz, kterou má ve správě daný online bazar.

Útočníci si své oběti pečlivě vybírají a zpravidla cílí na oběti, které nabízejí zboží v hodnotě do 5 000 Kč nebo mají na kartě k dispozici alespoň 7 000 Kč.

I přes rozmach nástrojů umělé inteligence, pracují některé útočné skupiny stále zcela manuálně. Generativní umělou inteligenci ale mohou používat ke zlepšování jazykové kvality podvodného obsahu, a tím i ke zvýšení důvěryhodnosti svého sdělení. Umělá inteligence jim také dokáže urychlit přípravu podvodných stránek, které mohou obsahovat i funkci AI chatbota.

Pokud útočníci pracují manuálně, vedou si o obětech přesnou evidenci. Vědí tedy, kde naposledy konverzace skončila a o čem už s obětí komunikovali. Útočníci na zprávy nereagují okamžitě, aby věrohodně napodobili chování běžného člověka, který nemá telefon vždy při sobě nebo neodpovídá na zprávy v pracovní době. Zpravidla mezi zprávami nechávají 8hodinové okno, které má představovat spánek. Bezpečnostní experti se domnívají, že se snaží přizpůsobit časovému pásmu obětí.

Při vyhledávání si oběti filtrují a kontaktují jen ty, které splňují několik základních parametrů. V případě, že se během konverzace objeví ze strany oběti jen drobný náznak pochybností, celou konverzaci zahodí a raději se zaměří na jinou oběť, kterých je na internetových tržištích dostatek.

Útočníci dělí svoje oběti do několika skupin. Nejčastěji cílí na nováčky, tedy uživatele, kteří mají čerstvě vytvořený účet a málo nabídek, a na běžné uživatele, kteří už v minulosti něco málo prodali a ještě mají pár aktivních inzerátů. Zároveň se ale vyhýbají uživatelům, kteří dokončili obchod v posledních dnech, a tudíž si dobře pamatují, jak daná platforma funguje.

Podle bezpečnostních expertů právě souhra těchto faktorů pravděpodobně vede k tomu, že se úspěšnost podvodů těchto skupin napříč všemi regiony pohybuje okolo 20 %.

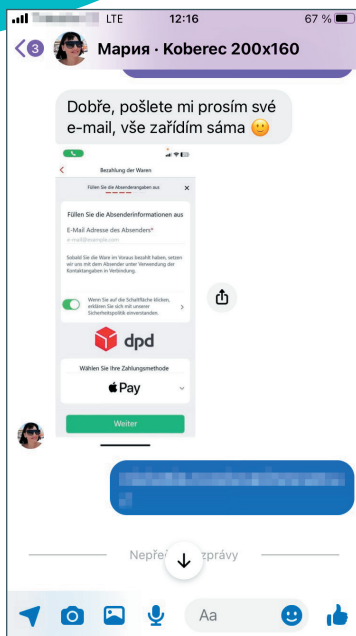
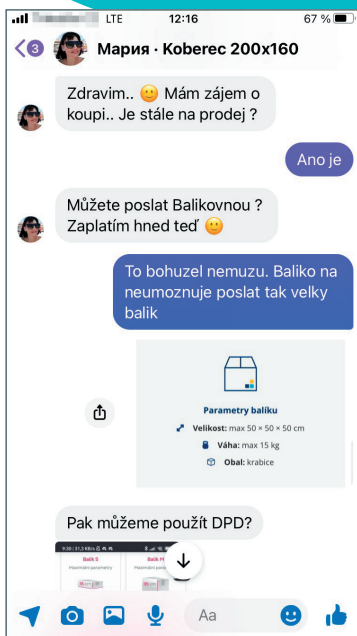


Příběh II. Podvod na Marketplace

- 1 Podvodník vytvoří falešný profil kupujícího na Marketplace. Tento profil obsahuje zdánlivě pravdivé informace, ale ve skutečnosti jsou falešné nebo ukradené.

Podvodník si vybere produkt na aukční platformě, v tomto případě koberec a kontaktuje prodávajícího.

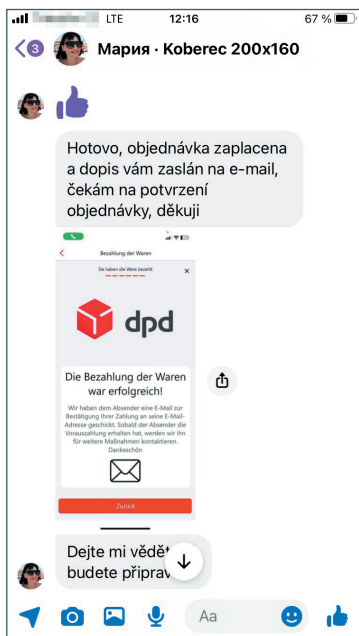
- 2 Komunikace se zdá nápadně strojově přeložená, zájemce o zboží neskloňuje a má špatný slovosled. Mějte na paměti, že opravdový kupující cizí národnosti by vás spíše kontaktoval anglicky.



- 3 Kupující se snaží obchod nápadně rychle vyřídít. Trvá na předání zboží přes dopravce a posílá odkaz na platební bránu. Opakovaně se ptá, zda jste už vyplnili údaje nebo potvrdili platbu

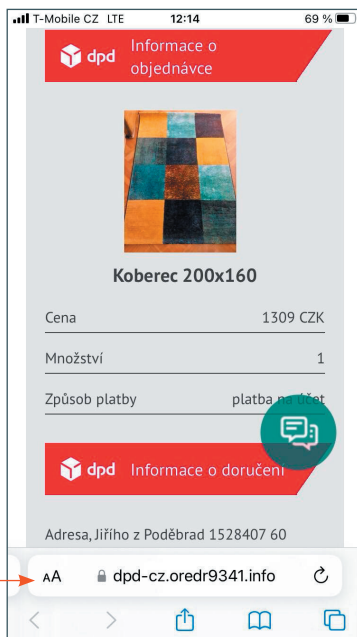
- 4 V takovém okamžiku zpomalte a pořádně si komunikaci znovu pročtěte.

Podvodník může také poslat falešný potvrzovací e-mail o platbě nebo dokonce falešný potvrzovací doklad o platbě.



5

Postup platby u českých dopravců tímto způsobem, tedy přes prodávajícího, zpravidla neprobíhá. Částka navíc odpovídá ceně prodávaného zboží, a ne ceně za dopravu.



Všimněte si falešné URL adresy.



Naše doporučení

- Ptejte se na jiné obvyklé způsoby platby nebo na možnost osobního předání apod. Podvodníci se z toho většinou snaží vycouvat nebo se nápadně vymlouvají. Může se stát, že konverzaci sami ukončí.
- Pokud se vám cokoli na komunikaci nezdá, raději ji ukončete. V tomto případě se rozhodně vyplatí opatrnost nad ziskem.



KUPUJÍCÍ V ROLI OBĚTI

Scénář probíhá tak, že scammer (podvodník) zveřejní na internetovém bazaru inzerát o prodeji zboží a čeká, až se mu někdo ozve. Poté podvodník oběti zašle SMS zprávu nebo e-mail s odkazem na falešnou webovou stránku, kde má oběť provést platbu za zboží. Po vyplnění údajů útočníci okradou oběť o domnělou platbu za zboží. Případně se útočník pokusí od oběti zjistit údaj o zůstatku na jejím bankovním účtu a následně se pokusí ukrást právě tuto částku.

Jak se vyhnout podvodnému prodeji na internetu?

- 1 Zkuste najít další zdroje**
Pokud vidíte inzerát na nějakém webu nebo sociální síti, zkuste najít tentýž produkt nebo službu na jiných důvěryhodných zdrojích. To vám umožní srovnat informace a zjistit, zda je inzerát pravdivý.
- 2 Ověřte identitu inzerenta**
Pokud je to možné, ověřte identitu inzerenta. Například pokud se jedná o prodej zboží od jednotlivce, můžete si ověřit jeho jméno, kontaktní údaje a historii prodejů.
- 3 Dejte pozor na příliš dobré nabídky**
Buďte obezřetní vůči inzerátům, které nabízejí produkty nebo služby za velmi nízké ceny. Může to být znak podvodu.
- 4 Ověřte fotografie**
Pokud jsou k inzerátu připojeny fotografie produktu, zkuste prověřit, zda tyto fotografie nejsou jen stažené z jiných zdrojů na internetu.
- 5 Komunikujte s inzerentem**
Pokud máte nějaké pochybnosti ohledně inzerátu, můžete kontaktovat inzerenta a klást otázky ohledně produktu, služby nebo podmínek prodeje. Způsob komunikace a odpovědi vám poskytnou lepší představu o důvěryhodnosti inzerenta.
- 6 Používejte zabezpečený prohlížeč**
Některé produkty digitální ochrany obsahují také funkci zabezpečeného prohlížeče, která dokáže upozorňovat na podvodné stránky.



Naše doporučení

Pamatujte, že prevence je klíčová. Důkladné ověřování e-shopu a inzerátu vám pomůže minimalizovat rizika spojená s nákupy a online transakcemi.

Podvody na e-shopech

Falešné internetové obchody na první pohled nemusí vyvolávat podezření. Pracují s vkusnou grafikou a používají správně češtinu. Ke zvýšení důvěryhodnosti stránek používají útočníci i falešné recenze uživatelů z celé republiky. Neférové nebo podvodné e-shopy ale neuvádějí obchodní podmínky, ani žádný konkrétní kontakt na provozovatele. To by mělo u uživatelů vyvolat podezření.

KAŽDÝ E-SHOP MUSÍ PODLE ZÁKONA UVÁDĚT SVÉ IČO, KONTAKTNÍ ÚDAJE A OBCHODNÍ PODMÍNKY.

Pokud na těchto e-shopech zákazník vyplní osobní údaje, například jméno, telefon a adresu, a objedná si produkt, odešle své údaje rovnou podvodníkům. K objednávce ale nikdy nedojde a poptávané zboží zákazník neobdrží.

Phishingový je také kontaktní formulář, i ten pouze shromažďuje údaje uživatelů. Webové stránky navíc nejsou nijak šifrované, data z nich proto mohou zachytit i další útočníci na internetu.



Digitální bezpečnost výrazně ohrožujete, pokud používáte jedno heslo pro více účtů. V případě, že kyberútočníci získají přístup k jednomu z vašich účtů, ať už proto, že heslo jednoduše prolomí nebo ho získají z databáze uniklých přihlašovacích údajů, otevírají se jim dveře k dalším online účtům, které mohou být zneužity k neoprávněným transakcím nebo mohou odhalit vaše osobní či platební údaje.

Podvody na e-shopech v číslech

¼ Čechů se při svých online nákupech setkala s podvodem.

42 % z nich podvod nijak neřeší.

Pouze ¼ lidí používá v e-shopech unikátní hesla.

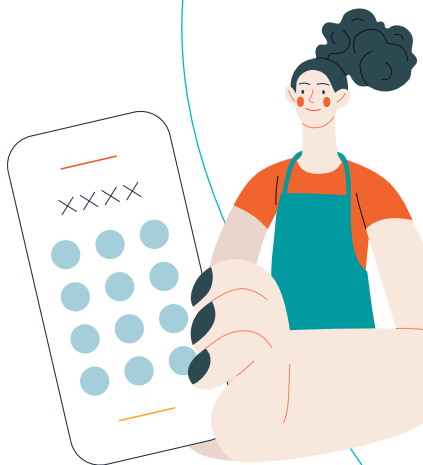
Zdroj: Průzkum ESETu, Median, 12/2024

Nejčastěji nakupujeme pomocí notebooku, přibližně polovina z nás však využívá také chytrý mobilní telefon. Především mezi nejmladší „nakupující“ generací se jedná o nejoblíbenější zařízení. Používání [kybernetické ochrany](#) na chytrých telefonech je stále podceňované. Přitom v nich dnes uchováváme celou řadu osobních a citlivých informací.



Jak zabezpečit telefon?

- 1 Používejte zámek obrazovky**
Ideálně ověření pomocí biometrických údajů, tedy rozpoznáním obličeje nebo otiskem prstu.
- 2 Pozor na nedůvěryhodné zdroje**
Aplikace stahujte pouze z oficiálních obchodů Google Play či App Store.
- 3 Nezapomeňte na kvalitní antivir**
Ani u chytrého telefonu nezapomínejte na kvalitní bezpečnostní program, který ho ochrání před viry, malwary, trojskými koni, škodlivými aplikacemi či podvodnými webovými stránkami.



Jak se vyhnout podvodům na e-shopech?

- 1** Zkontrolujte legitimitu e-shopu, na každém e-shopu byste měli najít:
 - IČO, kontaktní údaje a adresu provozovatele či prodejce,
 - obchodní podmínky,
 - recenze, především ty negativní (podvodníci je zpravidla neuvádějí),
 - SSL certifikování (na začátku URL adresy jsou znaky HTTPS).
- 2** Na falešný internetový obchod vás může upozornit podivně znějící doména, na které je e-shop provozován. Pravost stránky si můžete ověřit například na [CZ.NIC](#) nebo na dalších mezinárodních platformách.
- 3** Informace na webu se také mohou jevit jako strojově přeložené, případně všechny texty nejsou přeloženy do češtiny. Text může mít také nekonzistentní formátování napříč webem.
- 4** Pokud obchod nabízí produkty či služby za podezřele nízké ceny, vždy zbystřete. Stejně tak pokud je nabídka chaotická a nabízí zboží napříč různými kategoriemi.



- 5** Důvěryhodné e-shopy nabízí více možností platby – například na dobírku nebo přes výdejové místo. Podvodné e-shopy požadují zpravidla pouze platbu předem.
- 6** Při online platbě používejte bezpečné připojení a vyhýbejte se veřejným bezplatným Wi-Fi sítím.
- 7** Pokud se v e-shopu registrujete, vytvořte si ke svému účtu jedinečné heslo, které není snadno uhodnutelné. Pokud využíváme jedno heslo pro více služeb, výrazně tím ohrožujete svou digitální bezpečnost. Útočníci mohou heslo prolomit prostřednictvím útoků hrubou silou nebo ho získat z databáze uniklých hesel.

Limity pro platby nebrání kyberútočnickům v tom, aby se dostali k vašim finančním prostředkům, pouze snižují škody v případě úspěšného útoku. Oproti tomu **vicefázové ověření může rovnou zabránit neoprávněné transakci nebo neoprávněnému přístupu k vašemu online účtu.**

- 8** Experti také nedoporučují ukládat si v daném účtu platební kartu. Můžete využívat jednorázových virtuálních platebních karet nebo mít zvláštní účet na platby v e-shopech, kam si převedete jen částku na konkrétní platbu.
- 9** Česká obchodní inspekce (ČOI) vede také seznam všech rizikových webů, které najdete na adrese www.rizikove.cz.
- 10** V případě používání [antivirového řešení společnosti ESET](#) jste již automaticky i před těmito rizikovými e-shopy chráněni.
- 11** Udržujte všechna svá zařízení vždy aktuální. Aktualizace operačního systému a bezpečnostních programů či aplikací instalujte co nejdříve, obsahují opravy chyb z předešlých verzí.



Policie ČR doporučuje

Nastalou situaci je důležité řešit bezprostředně, při rychlém jednání a spolupráci s Policií ČR lze docílit i zastavení finančních prostředků, které jste za zboží zaplatili. Online platbu může zadržet i banka, kterou nakupující může kontaktovat ihned, pakliže má u konkrétní platby jakoukoliv pochybnost.

Podvody se vstupenkami

Kybernetičtí podvodníci často zneužívají velké kulturní a sportovní události k podvodným prodejům vstupenek a phishingu. Pokud nakupující neseženou vstupenky na oficiálních distribučních místech, uchylují se na různá internetová fóra (či Facebook a jiné sociální sítě a bazary jako je Sbazar nebo Bazoš). A právě tam se mohou stát obětí podvodu.



V komunikaci s případným prodejcem si vždy všimněte celého znění e-mailu nebo zprávy v chatu a tónu komunikace – je moc formální nebo naopak příliš uvolněný? Obsahuje text nějaké gramatické chyby? I přes možnosti nástrojů, jako je například ChatGPT nebo různé automatické překladače, zůstává čeština pro podvodníky z cizích zemí stále tvrdým oříškem.

Pokud vás kontaktuje někdo pod záštitou známého prodejce, zkontrolujte, zda adresa odesílatele sedí s oficiální adresou e-shopu. Pokud zpráva obsahuje nějakou přílohu nebo odkaz, buďte obzvlášť opatrní. Obecně platí, že byste neměli otevírat přílohy a klikat na odkazy z nevyžádaných e-mailů, pokud se nejedná o prokazatelně oficiální komunikaci nějaké známé autority.

Je důležité připomenout, že útočníci v Česku dlouhodobě šíří nebezpečné e-maily, jejichž přílohy obsahují [spyware](#). Taková příloha může mít příponu .exe. Pokud si nejste jisti, že se jedná o oficiální a bezpečnou komunikaci, není nic špatného na tom si zprávu obratem ověřit na oficiální zákaznické podpoře.



Podvody s kryptoměnami

Kolísající kurzy kryptoměn ovlivnily také online hrozby. Zločinci se místo těžby kryptoměn zaměřili na jejich krádeže, jak je vidět na globálním nárůstu phishingových útoků s tematikou kryptoměn a rostoucím počtu cryptostealerů.

Phishingové útoky se mohou skrývat za tváře známých osobností jako je například Elon Musk pomocí ukradených účtů na Twitteru, Discordu nebo Facebooku. Často se tak může jednat o falešné giveaways, jejichž cílem je z oběti vylákat menší množství kryptoměny s vidinou získání násobného počtu dané kryptoměny.

V poslední době jsou zaznamenány také masivní nárůsty pokusů o podvodné vylákání kryptoměn na diskuzních platformách typu Discord nebo Telegram, kde se útočníci vydávají za správce, oficiální zástupce kryptoburz nebo support team. Typicky se jedná o falešný support, který vám nabízí pomoc s řešením vašeho problému, kterým může být nepřipsaní kryptoměny do peněženky nebo nedoručená platba, přitom z vás ale útočník vyláká další krypto nebo peníze.

Dalším známým typem podvodu je, že útočníci zveřejní přístupové údaje ke kryptopeněžence, která již obsahuje nějaké coins. Pokud se tam pokusíte poslat měnu uvedeného blockchainu (nejčastěji ETH), abyste mohli obsah peněženky prodat nebo převést, je váš vklad okamžitě odcizen. Phishingové útoky, při kterých se podvodníci snaží získat přístupové údaje ke kryptopeněženkám nebo k jednotlivým účtům u známých kryptosměnárů, nejčastěji cílí na Binance, Coinbase, Coinomi a MetaMask.

Typy investičních podvodů

1 Ponziovo schéma (také Letadlo nebo Pyramida)

Tato podvodná machinace dostala jméno po Charlesu Ponzim, který k podvodům využil mezinárodního chaosu po 1. světové válce. Oběti jsou lákány k tomu, aby investovaly do neexistujících společností za účelem rychlého zbohatnutí. Výnosy jsou ale v tomto případě vypláceny z peněz dalších nešťastníků, kteří na podvod naletěli. A kryptoměny, jako dosud neprobádaná oblast, jsou pro tento účel ideální.

2 Podvod Pump & Dump

Podvodníci na základě nepravdivých informací vybízejí investory k nákupu akcií málo známých kryptoměnových společností. Cena akcií následně vzroste a podvodník své vlastní akcie rychle prodá. Akcie obětí zůstanou bezcenné.

3 Falešná doporučení od celebrit

Podvodníci se také zmocňují účtů celebrit na sociálních sítích nebo vytvářejí falešné účty a vybízejí jejich příznivce, aby investovali na základě výše uvedených taktik. V jednom případě si přišli na přibližně 2 miliony dolarů, přičemž zneužili jméno Elona Muska, aby tato lest působila důvěryhodněji.



Podvodníci zneužili jméno Elona Muska pomocí falešného účtu na platformě X.



Podobný typ podvodu je známý také v českém prostředí, např. deepfake video s prezidentem Petrem Pavlem a moderátorem Michalem Půrem, kteří ve videu doporučovali speciální investiční aplikaci. Než bylo video ze sítě staženo, získalo přes 400 tisíc zhlédnutí.

V minulosti zasáhla Česko také vlna podvodů s falešnými investičními stránkami, kdy podvodníci využívali například jméno Petra Kellnera, Jaromíra Jágra nebo Petra Čecha. Útočníci šířili podvodné sdělení formou reklamy, a to jak prostřednictvím legitimní inzerce na internetu, tak phishingovými e-mailovými kampaněmi. Tyto podvody jsou přitom stále aktuální. Pokud uživatel na takovou reklamu klikne, je přesměrován na podvodnou webovou stránku.



Podvodné video s Petrem Pavlem

iglkkeyword=CrypteBoom&subid=b447757b2c55f49mgvazb

VAROVÁNÍ: Z důvodu extrémně vysoké popularity medií zavřene registrací 08/27/2020 - POSPĚŠTE SÍŤ 23-58:6

CRYPTO BOOM Exkluzivní nabídky pro obchody v Česku Alice C. právě vyvolala/a 350 USD

Bitcoin dělá z lidí boháče
A vy se můžete stát dalším milionářem...

zobrazit

BITCOIN: IS IT THE FUTURE OF MONEY? **LIVE** **CNN**
LAWMAKERS ► SECURITY WILL BE TIGHT- ELITE TROOPS, SNIPERS, CNN.com

ZMĚNTE VÁŠ ŽIVOT JEŠTĚ DNES!

Křestní jméno
Příjmení
E-mail

DALŠÍ

Nabídka 11,379.485 USD
Požadávka 11,379.485 USD

BitGo **Norton** **secure//trading** **McAfee**

Ukázka podvodné webové stránky

4

Neexistující burzy

Podvodníci posílají e-maily nebo zveřejňují zprávy na sociálních sítích, kde slibují přístup k virtuální hotovosti uložené na kryptoměnových burzách. Uživatel musí obvykle nejprve zaplatit malý poplatek. Burzy samozřejmě v tomto případě neexistují a oběť nemá v podstatě žádnou šanci získat vložený poplatek zpět.

5

Podvodné aplikace

Kyberzločinci falšují legitimní aplikace pro kryptoměny a nahrávají je do obchodů s aplikacemi. Pokud si takovou aplikaci nainstalujete, můžete přijít o své osobní a finanční údaje nebo do svého zařízení stáhnout škodlivý kód (dropper). Prostřednictvím falešných aplikací mohou podvodníci uživatele přimět také zaplatit za neexistující služby, nebo se pokusit ukrást jeho přihlašovací údaje do kryptoměnové peněženky.

Co je to dropper?

Dropper je typ škodlivého kódu (malware), který si nainstalujeme společně s jinou aplikací. Na tu můžeme narazit v neoficiálních obchodech s aplikacemi, na diskuzních fórech nebo internetových úložištích. Po infikování zařízení dropper spouští další škodlivý kód (například trojské koně, ransomware, spyware či adware) nebo provádí další akce, které mohou vést k odcizení dat a poškození systému.



Chcete být chráněni před droppery?

Chraňte se kvalitním [bezpečnostním softwarem](#).



Jak se nestát obětí kryptoměnového podvodu?

Prevence kryptoměnových podvodů je klíčová pro bezpečné fungování v kryptoměnovém prostředí. Zde je několik opatření, která vám mohou pomoci vyhnout se podvodům:

- **Vzdělávejte se**

Seznamte se důkladně s principy fungování kryptoměn a technologií blockchain. Osvojení základních znalostí vám pomůže lépe porozumět potenciálním rizikům.

- **Používejte ověřené platformy**

Vyhněte se pochybným nebo neznámým platformám a burzám. Používejte pouze osvědčené a důvěryhodné služby pro nákup, prodej a výměnu kryptoměn.

- **Chraňte si soukromí**

Dbejte na své soukromí a nikdy neposkytujte citlivé informace, (jako jsou hesla) na neověřených webových stránkách nebo přes nezabezpečené kanály.

- **Chraňte se před phishingem**

Buďte obezřetní při klikání na odkazy ve zprávách, e-mailech nebo sociálních sítích. Phishingové útoky jsou častým způsobem, jak podvodníci získávají přístup k účtům.

- **Používejte vícefázové ověření (2FA)**

Aktivujte ho na všech svých kryptoměnových účtech. Toto dodatečné zabezpečení znesnadňuje hackerům přístup k vašemu účtu i v případě, že by se podařilo získat vaše heslo.

- **Ukládejte kryptoměny bezpečně**

Používejte bezpečné peněženky (např. hardwarová) pro dlouhodobé ukládání kryptoměn. Těmito způsoby lze minimalizovat riziko úniku prostřednictvím online útoků.

- **Aktualizujte software a antivirovou ochranu**

Pravidelně aktualizujte software na svých zařízeních a používejte spolehlivý antivirový program. To může pomoci odhalit a blokovat škodlivý software.

- **Mějte nadhled**

Buďte skeptičtí vůči slibům rychlého zbohatnutí a neotestovaným investičním schémátům. Investujte pouze tolik, kolik si můžete dovolit ztratit, a vyhýbejte se nejistým projektům.

- **Pozor na podvodné ICO**

Buďte opatrní při účasti na Initial Coin Offerings (ICO). Mnoho podvodných projektů slibuje vysoké zisky a poté zmizí s penězi investorů.

- **Zapojte se do komunity**

Sledujte komunity a diskuse kolem kryptoměn. Informujte se o aktuálních hrozbách a varováních od ostatních uživatelů.

ESET HOME Security

PROZKOUMEJTE FUNKCE BEZPEČNOSTNÍHO ŘEŠENÍ ESET PRO DOMÁCNOSTI

Blokujte podezřelé webové stránky a e-maily

Díky funkci **anti-phishing** zablokujete stránky, které se snaží odcizit vaše osobní údaje, zabráníte tak krádeži identity a zneužití vašich osobních údajů.

Braňte se proti škodlivému kódu

Proaktivní antivirus vás ochrání před viry, trojskými koni, červy a spywarem. Umělá inteligence zabudovaná do naší ochrany detekuje pokročilý, dosud neviděný malware a zároveň má minimální dopad na výkon zařízení.

Ochrana proti ransomware blokuje škodlivý software, který se vás pokouší odpojit od vašich dat a požaduje výkupné.

Nakupujte, vyhledávejte a komunikujte online bez obav

Zabezpečený režim prohlížeče nabízí automatickou ochranu online bankovníctví a přístupu k webovým kryptopeněženkám. Díky šifrované komunikaci mezi klávesnicí a prohlížečem si zajistíte bezpečnější transakce a ochranu před keyloggery, malwarem a dalšími typy digitálních hrozeb.

Mobilní ochrana je rozšířena o anti-phishing (SMS phishing), který skenuje příchozí SMS zprávy a upozorňuje na nebezpečné odkazy.

Rodičovská kontrola umožňuje blokovat nežádoucí webový obsah podle kategorií nebo jednotlivých webových stránek, aby byly na internetu v bezpečí i vaše děti.

Brána firewall zajišťuje bezpečnost používání veřejné sítě Wi-Fi tím, že udržuje vaše zařízení mimo dosah ostatních uživatelů a potenciálně infikovaných zařízení. Tuto funkci využijete především během cestování a při práci na dálku.

Strážce sítě blokuje hrozby z vaší sítě Wi-Fi tím, že chrání domácí router a ukazuje, kdo je k němu připojen.



Digital Security
Progress. Protected.

BEZPEČNÝ DIGITÁLNÍ SVĚT PRO KAŽDÉHO

Zvolte si úroveň ochrany podle svých potřeb.
Zabezpečte svá zařízení antivirem, blokováním
podvodů a šifrováním dat.

www.eset.cz



O SPOLEČNOSTI ESET

Společnost ESET® již více než 30 let vyvíjí špičkový software a služby v oblasti IT bezpečnosti, které chrání firmy, kritickou infrastrukturu a spotřebitele po celém světě před stále sofistikovanějšími digitálními hrozbami. Od zabezpečení koncových bodů a mobilních zařízení až po detekci a reakci koncových bodů, stejně jako šifrování a vícefázová autentizace, vysoce výkonná a snadno použitelná řešení ESET nenápadně chrání a monitorují 24/7. Aktualizují obranu v reálném čase, aby uživatelé byli v bezpečí a firmy fungovaly bez přerušení. Vyvíjející se hrozby vyžadují vyvíjející se společnost zaměřenou na kybernetickou bezpečnost, která zajišťuje bezpečné používání digitálních technologií. Za tím stojí výzkumná a vývojová centra společnosti ESET po celém světě, která pracují na naší společné budoucnosti. Pro více informací navštivte www.eset.com nebo nás sledujte na [LinkedIn](#), [Facebook](#), a [Twitter](#).

© 1992 - 2024 ESET, spol. s r.o. - Všechna práva vyhrazena.

Ochranné známky použité v tomto dokumentu jsou ochranné známky nebo registrované ochranné známky společnosti ESET, spol. s r.o. nebo ESET North America. Všechny ostatní názvy a značky jsou registrovanými ochrannými známkami příslušných společností.



Digital Security
Progress. Protected.