září 2026

Zpr@vodaj ČSSZ

Jak se zneužívá jméno ČSSZ, str. 1 • Desatero digitální hygieny, str. 3

ČSSZ upozorňuje: Jak se nenachytat v online světě

Internet nám usnadňuje každodenní život, ale zároveň vytváří prostor pro stále propracovanější podvody. V poslední době ČSSZ opakovaně zaznamenává případy, kdy se podvodníci vydávají za její zaměstnance nebo využívají její jméno v SMS zprávách, e-mailech či telefonátech. Jejich cílem je získat osobní údaje, přístup k účtům nebo peníze.

Neviditelný podvodník

Podvodníci dnes nevystupují jen pod anonymními adresami a neznámými telefonními čísly. Stále častěji se vydávají za důvěryhodné instituce, státní úřady, banky nebo známé společnosti. V posledních týdnech zaznamenala podobné případy také Česká správa sociálního zabezpečení (ČSSZ), která veřejnost upozornila na podvodné SMS zprávy, e-maily i telefonáty zneužívající její jméno

Jak podobné podvody fungují, na co si dát pozor a jak se účinně chránit?

Cílem většiny internetových podvodů je přimět člověka k ukvapenému jednání. Útočníci spoléhají na to, že pod tlakem nebo ve spěchu nebudeme věnovat dostatečnou pozornost detailům.

UPOZORNĚNÍ

ČSSZ občanům neposílá SMS zprávy, zprávy prostřednictvím aplikace WhatsApp ani e-maily s informací o údajném nedoplatku či přeplatku na sociálním pojištění a nevyzývá tímto způsobem k úhradě plateb ani k zadávání osobních či platebních údajů. Pokud takovou zprávu obdržíte, jedná se o podvod.

Nejčastější podvody zneužívající jméno ČSSZ:

Podvodné SMS zprávy

V takzvaných smishingových zprávách se podvodníci často vydávají za státní instituce, dopravce nebo banky. Zpráva může obsahovat informaci o nedoplatku, přeplatku, nevyzvednuté zásilce nebo údajném nároku na finanční prostředky. Právě falešné zprávy o údajném nedoplatku nebo přeplatku patří v současnosti mezi nejčastější podvody zneužívající jméno ČSSZ. Útočníci se snaží vyvolat obavu z dluhu nebo naopak nalákat na neexistující finanční částku, kterou je údajně možné získat po kliknutí na zaslaný odkaz.

Aktuálně se šíří například SMS ve znění:

„Dobrý den, při kontrole evidence sociálního pojištění byl u Vás zjištěn evidovaný nedoplatek. Info zde: eportal-cssz-cz.casa“.

Součástí bývá odkaz, který vede na falešnou internetovou stránku. Ta se často podobá skutečnému webu instituce a snaží se získat od uživatele osobní údaje, přihlašovací údaje nebo údaje k platební kartě. Na takovou zprávu nikdy nereagujte, neklikejte na odkaz a nezadávejte jeho prostřednictvím žádné osobní, přihlašovací ani platební údaje.

pokračování na straně 2...

... pokračování ze strany 1

Informace o sociálním pojištění a službách ČSSZ ověřujte pouze prostřednictvím jejích oficiálních internetových stránek:

- ČSSZ: cssz.gov.cz (v případě Institutu posuzování zdravotního stavu ipzs.gov.cz),
- ePortál ČSSZ: eportal.cssz.cz.

Podvodné e-maily

Na obdobném principu fungují i phishingové e-maily. Ty mohou na první pohled působit důvěryhodně, obsahovat loga institucí nebo profesionálně zpracovanou grafiku.

V prostředí ČSSZ např. zprávu o údajném přepočtu důchodu či výši doplatku a další prvky, které mají vzbudit dojem oficiálního dokumentu.

Typickými znaky bývají:

- výzva k okamžitému jednání,
- upozornění na údajný problém s účtem,
- hrozba ztráty služby nebo nároku,
- odkaz na stránku vyžadující zadání osobních údajů.

Podvodné telefonáty

Stále častěji se objevují také podvodné telefonáty, označované jako vishing, a to i v souvislosti se zmíněným e-mailem.

Volající se může představit jako pracovník úřadu, banky, policie nebo technické podpory. Snaží se vyvolat obavy a přesvědčit volaného, aby mu sdělil citlivé údaje, potvrdil určitou operaci nebo provedl převod peněz.

Pamatujte, že důvěryhodné instituce po občanech běžně nepožadují hesla, bezpečnostní kódy ani přístupy do internetového bankovnictví. Na telefonát ideálně vůbec nereagujte, v žádném případě nesdělujte přihlašovací údaje, hesla apod., neinstalujte žádné aplikace ani neumožňujte vzdálený přístup ke svému zařízení.

POZOR: ČSSZ varovala před

- podvodnými SMS,
- falešnými e-maily,
- podvodnými telefonáty.

Jaké online podvody jsou dnes nejčastější?

Podvodné SMS a e-maily nejsou jediným rizikem. Kyberzločinci neustále hledají nové způsoby, jak své oběti přimět k neuváženému jednání.

Phishing 2.0: podvody, které vypadají jako skutečné

Ještě před několika lety bylo možné řadu podvodných zpráv rozpoznat podle špatné češtiny nebo podezřelého vzhledu. Dnes už to často neplatí. Moderní phishing využívá kvalitní grafiku, loga skutečných institucí, přesvědčivý jazyk i aktuální témata. Falešné stránky mohou být na první pohled téměř nerozeznatelné od originálu.

Proto už nestačí hodnotit pouze vzhled zprávy. Důležité je vždy ověřovat, kdo je skutečným odesílatelem a kam vede odkaz, na který máme kliknout.

Falešné investice a kryptoměny

Dalším častým trikem jsou nabídky mimořádně výhodných investic.

Podvodníci slibují vysoké výnosy, minimální riziko a rychlý zisk. Mohou vystupovat jako investiční poradci nebo zástupci údajných investičních společností. Často zneužívají témata umělé inteligence, kryptoměn nebo známých osobností.

Společným znakem bývá tlak na rychlé rozhodnutí a snaha přimět člověka k zaslání peněz ještě předtím, než si nabídku důkladně prověří.

Podvody na bazarech a v e-shopech

Mnoho lidí se setkalo také s podvody při nakupování nebo prodeji na internetových tržištích.

Typickým scénářem je zaslání odkazu na údajnou platební bránu nebo přepravní službu. Podvodník tvrdí, že je třeba potvrdit přijetí platby nebo vyplnit údaje pro doručení zásilky. Ve skutečnosti se snaží získat citlivé údaje nebo přístup k bankovnímu účtu.

Nová výzva: umělá inteligence v rukou podvodníků

Umělá inteligence přináší řadu užitečných možností, ale stejně jako každou technologii ji lze zneužít.

Přesvědčivější podvodné zprávy

Nástroje využívající umělou inteligenci dokážou během několika vteřin vytvořit profesionálně působící text bez pravopisných chyb. Podvodné e-maily tak mohou působit mnohem důvěryhodněji než dříve.

To znamená, že samotná gramatická nebo vizuální úroveň zprávy už není spolehlivým ukazatelem její důvěryhodnosti.

pokračování na straně 3...

... pokračování ze strany 2

Napodobení hlasu
Umělá inteligence dnes dokáže poměrně věrně napodobit nejen lidský hlas, ale i obličej ve videokonferencích. Podvodníci mohou tuto technologii využít k vytvoření falešných telefonátů či videohovorů, ve kterých se budou vydávat za rodinného příslušníka, kolegu nebo pracovníka instituce.

Pokud po vás kdokoli po telefonu požaduje citlivé údaje nebo okamžitou finanční operaci, je vždy vhodné si jeho totožnost i požadavek nezávisle ověřit.

Nelze se spoléhat ani na zobrazené telefonní číslo, které útočníci dokážou podvrhnout. Chcete-li mít jistotu, že opravdu mluvíte se správnou osobou, hovor ukončete a zavolejte na správné číslo, které máte uložené v telefonu.

Je důležité zdůraznit, že problémem není samotná umělá inteligence, ale její zneužívání ke klamání a manipulaci lidí.

Deset návyků digitální hygieny

Žádná technologie nedokáže zabránit všem podvodům. Nejlepší ochranou zůstává obezřetnost a zdravá nedůvěra.

1. Ověřujte odesílatele
Před otevřením odkazu nebo přílohy si vždy zkontrolujte, kdo vám zprávu skutečně poslal.

2. Nespěchejte
Podvodníci často vytvářejí pocit naléhavosti. Právě tehdy je potřeba zpomalit a vše si ověřit.

3. Neklikejte bez rozmyslu
Pokud si nejste jisti původem zprávy, na odkaz neklikejte ani ho nepřepisujte do adresního řádku. Web navštivte vždy sami zadáním jeho ověřené oficiální adresy, případně využijte uložené záložky.

4. Chraňte svá hesla
Nikomu nesdělujte hesla, autorizační kódy ani neudělujte jednorázová potvrzení. Vždy pozorně čtěte, co potvrzujete.

5. Používejte silná a unikátní hesla
Každá důležitá služba by měla mít vlastní a dostatečně složité heslo. Používejte prověřeného správce hesel (password manager), který vám umožní vytvářet a bezpečně ukládat desítky dostatečně složitých hesel.

6. Zapněte vícefaktorové ověřování
Dodatečné ověření výrazně zvyšuje bezpečnost vašich účtů.

7. Aktualizujte zařízení a aplikace
Pravidelné aktualizace pomáhají odstraňovat bezpečnostní zranitelnosti.

8. Buďte obezřetní u investičních nabídek
Mimořádně vysoký výnos bez rizika neexistuje.

9. Sdílejte jen nezbytné údaje
Čím méně osobních informací zveřejníte, tím méně materiálu mají podvodníci k dispozici.

10. Když si nejste jistí, ověřujte
Raději se jednou zeptejte navíc, než abyste se stali obětí podvodu.

Jak komunikuje ČSSZ

Při komunikaci s občany ČSSZ nikdy:

- nezasílá SMS zprávy, whatsappové zprávy ani e-maily s informací o nedoplatku nebo přeplatku obsahující odkazy na úhradu či vyplnění údajů,
- nepožaduje heslo k Identitě občana,
- nepožaduje přihlašovací údaje do internetového bankovnictví,
- nepožaduje číslo platební karty včetně ověřovacích údajů,
- nevyžaduje sdělení autorizačních SMS kódů,
- nevyžaduje potvrzení bankovních operací na základě nevyžádaného telefonátu nebo e-mailu.

Pokud obdržíte podezřelou zprávu nebo telefonát, které se vydávají za ČSSZ, buďte obezřetní a informace si

raději ověřte prostřednictvím oficiálních komunikačních kanálů.

Dodržování základních pravidel nám dává šanci

Kybernetické podvody jsou stále propracovanější a jejich cílem se může stát kdokoli bez ohledu na věk či zkušenosti. Dobrou zprávou je, že většina útoků spoléhá na stejný princip: snaží se nás přimět jednat rychle a bez ověření informací.

Pokud si osvojíme základní pravidla kybernetické bezpečnosti, zachováme si zdravou míru opatrnosti a budeme ověřovat neobvyklé požadavky, můžeme většině podvodů úspěšně předejít. ■

Všechna reprodukční práva jsou vyhrazena. Jakékoliv šíření a kopírování online Zpr@vodaje ČSSZ bez výslovného svolení ČSSZ není povoleno. Obrátit se můžete na redakce@cssz.gov.cz. Děkujeme za pochopení.