

WORKSHOP PRO ŽIVNOSTNÍKY A MALÉ FIRMY

Phishing. Jak nenaletět.

Jak vás chtějí podvést? Jak to poznat?
A co dělat, když už jste „klikli“.

ING. DOMINIK MALČÍK, PH.D. · REDAMP.IO · ŘÍJEN 2026

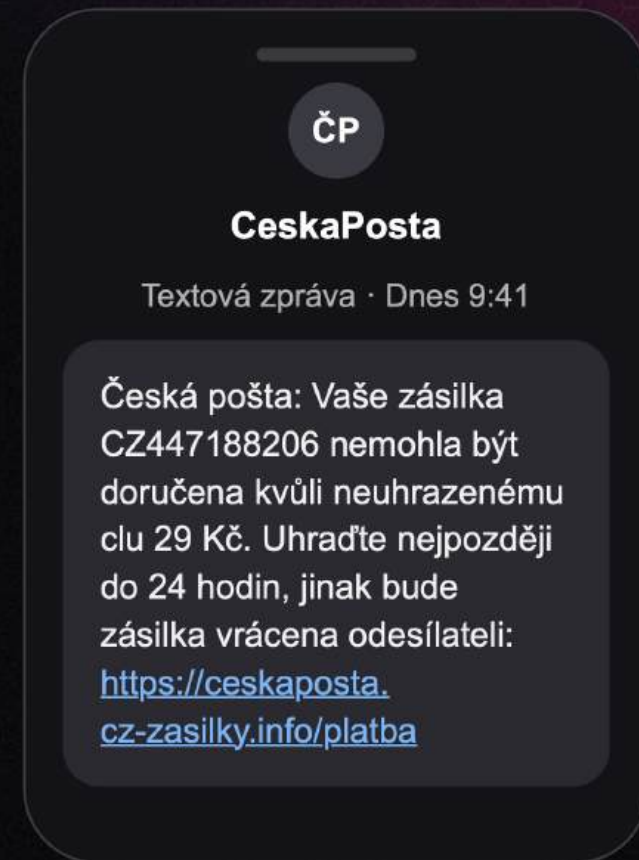


pro podnikavé



ZAČNĚME OTÁZKOU

Znáte tuhle SMS zprávu?



PLÁN NA 30 MINUT

Dnes čtyři otázky.

01

**Co je
phishing?**

02

**Jak poznat
phishing?**

03

Jak se bránit?

04

**Co když už
jste „klikli“?**

Ke každé otázce konkrétní příklady z Česka. A jedna věc, kterou si odnesete.

Phishing je „rybaření“.
Návnadou je zpráva.
Kdo je ryba?

Jedna past. Čtyři cesty.



Phishing

E-MAIL

„Ověřte prosím
svůj účet.“



Smishing

SMS, WHATSAPP

„Doplaťte 29 Kč
za balík.“



Vishing

TELEFONÁT

„Volám z
bezpečnostního
oddělení banky.“



Quishing

QR KÓD

„Naskenujte QR kód
a zaplaťte parkovné.“

Chtějí jediné. Abyste něco udělali.



Klikněte

na odkaz, který vede na falešnou stránku.



Otevřete

přílohu, která pustí do počítače škodlivý program.



Vyplňte

heslo, číslo karty nebo kód z SMS.



Zaplatte

na jejich účet. Fakturu, pokutu, „clo“.

Emoce a spěch.

Pokaždé stejný recept.

VÝHRA

„Gratulujeme! Vyhráli jste iPhone. Stačí uhradit poštovné 1 Kč. Zaplaťte hned kartou.“

STRACH

„Váš účet bude do 24 hodin zablokován. Ověřte svou totožnost.“

ZTRÁTA

„Na váš účet se přihlásilo neznámé zařízení. Volejte ihned na číslo +420 800“

POKUTA

„Evidujeme neuhrazenou pokutu 1 500 Kč. Zaplaťte do zítřka, jinak přejde do správního řízení.“

NEJČASTĚJŠÍ MÝTUS

**„Jsme moc malí.
Nás si nikdo nevšimne.“**



**Útoky dnes posílají stroje.
Zkoušejí všechny.**

21 137

trestných činů v kyberprostoru za
rok 2025.

Každý osmý trestný čin v Česku se odehrál online.

Dříve ho prozradily chyby.
Dnes píše bez chyb.

Dříve lámaná čeština.

Dnes vás oslovují jménem.

DŘÍVE

Vážený zákazníku, Váš účet byl pozastaven kvůli bezpečnostní problém. Prosím klikněte zde pro ověření Vašeho účtu.

Chyby a obecné oslovení. Poznáte na první pohled.

DNES · PŘÍLOHA

Dobrý den, pane Dvořáku, viděla jsem na Instagramu vaši novou provozovnu, gratuluji! Posílám nabídku na polepy výloh, ceník je v příloze. Hezký den, Klára

 Cenik_polepy_2026.zip

Příloha je škodlivý program. Osobní zprávu otevřete bez váhání.

DNES · ODKAZ

Dobrý den, pane Dvořáku, k provozovně Kadeřnictví Dvořák přibyla na Googlu nová recenze s 1 hvězdičkou. Odpovědět na ni můžete zde:

[Odpovědět na recenzi](#)

Odkaz vede na falešné přihlášení ke Googlu. Chtějí vaše heslo.

Nejdřív si vás najdou.

Zpráva pak sedí jako ulitá.



Sociální sítě

Co prodáváte a kde jste zrovna na dovolené.



Firemní web

Jména, e-maily, dodavatelé.



Veřejné rejstříky

ARES, obchodní a živnostenský rejstřík.



Uniklá data

E-maily a hesla z úniků e-shopů a služeb.

SPEAR PHISHING

Díky umělé inteligenci (AI) je dnes tzv. spear phishing naprosto běžný. Zprávy jsou personalizované, a proto jim ve spěchu snadno uvěříte.

PODVOD SE ZMĚNOU ÚČTU

Dodavatel má nový účet. Opravdu?

Změnu účtu vždy ověřte telefonem.

Na tel. číslo, které už znáte. Nikdy ne na číslo z e-mailu.



Mlýn Podlesí

fakturace@[mlyn-podlesi.cz](mailto:fakturace@mlyn-podlesi.cz)

Změna bankovního spojení

Dobrý den, od 1. listopadu přecházíme k nové bance. Fakturu č. 2026/1147 na 48 600 Kč prosím uhradte už na nový účet 2601••••48/2010. Původní účet rušíme. Děkuji, Petra Malá, Mlýn Podlesí s.r.o.

PRAVÁ

[mlyn-podlesi.cz](mailto:fakturace@mlyn-podlesi.cz)

FALEŠNÁ

[mlyn-podIesi.cz](mailto:fakturace@mlyn-podIesi.cz)

Vypadá vizuálně stejně, ale je to úplně jiná adresa: místo malého l (el) je tam velké l (i). Stejně se zneužívá i číslice 1.

Jméno odesílatele je jen popisek. Rozhoduje adresa.



Finanční správa

podatelna@financni-sprava.[cz-vraceni.top](mailto:podatelna@financni-sprava.cz-vraceni.top)

Předmět: Přeplatek na dani 4 860 Kč čeká na vyplacení



Jméno, logo a podpis

Kdokoli zkopíruje za minutu.



Adresa za zavináčem

Tam se dívejte vždy. A čtěte ji od konce.
Pozor i na záměnu znaků.

Z čeho se skládá adresa odkazu.

Rozhoduje doména s koncovkou.



Dávejte pozor na adresu odkazu.

Poznejte, kam odkaz opravdu míří.

ADRESA V ODKAZU	KAM ODKAZ OPRAVDU MÍŘÍ	VERDIKT
https://ceskaposta.cz/sledovani	ceskaposta.cz	✓ Pravá
https://ceskaposta.cz-zasilky.info/platba	cz-zasilky.info	✗ Falešná
https://gov.cz.platba-pokuty.eu/prihlaseni	platba-pokuty.eu	✗ Falešná
https://datovaschranka.cz-gov.cc	cz-gov.cc	✗ Falešná

MASKOVANÝ ODKAZ

Text odkazu může lhát. Podívejte se, kam vede.



Počítač: najed'te myší a počkejte. Neklikejte.



Mobil: odkaz neotevírejte. Aplikaci nebo web si otevřete sami.



Microsoft 365

no-reply@sharepoint-docs.net

Petra Malá vám nasdílela dokument

Faktura_2026-1147.pdf

Dokument je chráněný. Pro zobrazení se přihlaste svým firemním účtem.

Otevřít dokument ve OneDrive

<https://onedrive-share.cz-dokument.top/login>

Tohle uvidíte až po najetí myší na tlačítko.

Tři otázky.

Před každým kliknutím.

01

Je to nečekané?

Balík, který nečekáte. Faktura, kterou neznáte. Výhra, o kterou jste nesoutěžili.

02

Tlačí na mě?

Spěch, strach, výhra nebo prosba, ať to nikomu neříkáte.

03

Chce to klik, údaje nebo peníze?

Odkaz, příloha, heslo, karta, kód z SMS, platba.

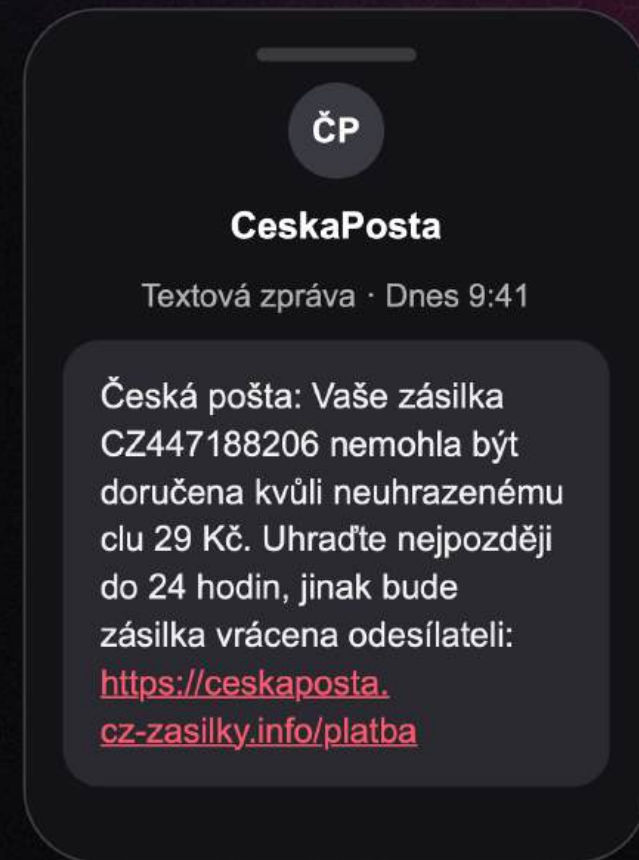
Aspoň jedno ano? Zastavte se a ověřte to jinou cestou.

Ta SMS ze začátku. Ted' ji prokouknete.

- 1 Nečekali jste žádné clo.
- 2 Tlačí na čas: do 24 hodin.
- 3 Odkaz míří na cz-zasilky.info.

Stav zásilky ověřujte v legitimní aplikaci dopravce nebo na webu, který si sami do prohlížeče napíšete.

Obejdete tak zmanipulovaný odkaz.



Pokuta přes SMS?

Takhle úřady nepracují.

Pravá adresa státu končí na gov.cz. Nic za tím.

Pro podnikatele navíc

Nabídky „zápisu do registru“ za poplatek chodí i do datové schránky.

Datová schránka je bezpečná, ale poslat do ní zprávu může kdokoli.



FALEŠNÝ BANKÉŘ

Volá banka.
Jenže to není banka.

744 000 Kč

průměrná škoda u telefonního podvodu v Česku.



PRAVIDLO 3Z OD POLICIE ČR

Zastav. Zavěs. Zkontroluj.

BANKA ANI POLICIE PO VÁS NIKDY NECHTĚJÍ



Převést peníze na
„bezpečný účet“.



Nainstalovat aplikaci pro
vzdálený přístup.



Sdělit kód z SMS, PIN
nebo heslo.

QR kód je jen odkaz. Jen ho nevidíte.

-  Po naskenování si nejdřív přečtěte adresu. Teprve pak otevírejte.
-  U QR platby z faktury zkontrolujte v bance účet a příjemce.



Co vidíte a slyšíte, se dá podvrhnout.

Ověřte si informace vlastní cestou.

	 E-mail	 SMS	 Telefon	 Web
LZE SNADNO PODVRHNOUT	Jméno odesílatele, logo, podpis i text odkazu. U nechráněné domény i samotnou adresu.	Jméno odesílatele. Zpráva se vám může zařadit i mezi „pravé“ SMS.	Číslo i jméno na displeji. AI umí napodobit i hlas.	Vzhled, logo i zámek https. Podvodný odkaz se může skrývat i v QR kódu.
OVĚŘTE	Doménu odesílatele a kam odkaz v e-mailu opravdu míří. Při pochybnostech se odesílatele zeptejte jinou cestou.	Informace obsažené v SMS zprávě si ověřte v aplikaci nebo na webu, který otevřete sami (nikoliv přes odkaz ve zprávě).	Zastavte se, zavěste a volejte na číslo, které si sami dohledáte nebo které už máte ověřené.	Než na stránce cokoli zadáte, zkontrolujte v adresním řádku doménu s koncovkou. Známý vzhled webu ani zámek u https nestačí.

Ochrana není věda.
Stačí pár nastavení.

Jedno heslo všude.

Jeden klíč od všeho.

Když uniknou hesla z jednoho e-shopu, útočník je pomocí robota zkusí na váš e-mail i do banky. Tento typ útoku trvá typicky jenom pár vteřin.

Řešení: správce hesel



Pamatujete si jen jedno silné heslo a správce hesel ideálně odemykáte otiskem prstu nebo obličejem. Ostatní hesla vymyslí a uloží on. Na falešné stránce je navíc sám nevyplní.

Heslo nestačí.

Zapněte druhý zámek.

DOBŘE

Kód z SMS

Lepší než nic. Dá se ale vylákat.

LEPŠÍ

Ověřovací aplikace

Dobrá volba pro většinu služeb.

NEJLEPŠÍ

Přístupový klíč (passkey)

Otisk prstu nebo obličej. Na falešné stránce nefunguje.

Začněte e-mailem a bankou. Přes e-mail se obnovují všechna ostatní hesla.

AKTUALIZACE

Neodkládejte je. Zavírají známé díry.

Telefon, počítač, prohlížeč, aplikace i router.
Nejlépe automaticky. A co nejdříve.



Aktualizace softwaru

Systém · právě teď

Je připravena nová verze systému. Obsahuje důležité bezpečnostní opravy.

Připomenout zítra

Instalovat v noci

Telefon.

Pět minut nastavení.



Android

- ✓ **Podporovaný telefon***, automatické aktualizace.
- ✓ Play Protect zapnutý.
- ✓ Aplikace jen z Google Play. Instalaci odjinud nepovolujte.
- ✓ V Chrome zapnutá rozšířená ochrana.



iPhone

- ✓ Podporovaný telefon, automatické aktualizace.
- ✓ Aplikace jen z App Store.
- ✓ Nikdy neklikejte na „Stáhnout profil“.
- ✓ V Safari upozornění na podvodné weby.

* Mnoho výrobců vydává aktualizace nedostatečně. Telefon s neaktualizovaným operačním systémem je brzy po koupi zranitelný. Dlouhodobou podporu pravidelných aktualizací poskytují například Samsung a Google Pixel.

Počítač.

Windows i Mac.



Windows

- ✓ Windows 11, automatické aktualizace.
- ✓ Běžný účet, ne správce.
- ✓ Defender a SmartScreen zapnuté.
- ✓ Žádné příkazy z webu do Win + R, Terminálu ani PowerShellu.



Mac

- ✓ Podporovaný macOS, automatické aktualizace.
- ✓ Heslo zadávejte, jen když jste sami něco spustili.
- ✓ Aplikace jen z App Store nebo od ověřených vývojářů.
- ✓ Žádné příkazy z webu do Terminálu.

Pojistka pro nejhorší den.

Když přesto něco projde.



Limity v bance

Denní limit na kartu a na platby na internetu.
Upozornění na každou platbu do mobilu. Útočník pak nevybere všechno.



Zálohy*

Kopie dat mimo počítač, kterou útočník nesmaže.
A jednou za čas si vyzkoušejte, že obnova opravdu funguje.

* DOPORUČENÍ PRO ZÁLOHY: PRAVIDLO 3-2-1 NEBO 3-2-1-1

3 kopie dat: originál a dvě zálohy

2 různá úložiště, třeba disk a cloud

1 kopie mimo firmu, pro případ požáru nebo krádeže HW

1 kopie offline nebo neměnná. Tu útočník nesmaže.

Co zvládnete sami.

S čím pomůže odborník.

SAMI, JEŠTĚ DNES

- ✓ Správce hesel
- ✓ Dvoufázové ověření u e-mailu a banky
- ✓ Automatické aktualizace všude + neodkládat!
- ✓ Limity a upozornění v bance
- ✓ Ochrana telefonu (viz slajd 29)
- ✓ Běžný účet v počítači (viz slajd 30)

SE SPECIALISTOU

- ✓ Zabezpečení firemního e-mailu a domény
- ✓ Filtrování škodlivých odkazů
- ✓ Správa zařízení a oprávnění
- ✓ Zálohy s vyzkoušenou obnovou
- ✓ Školení a cvičný phishing pro tým
- ✓ Zabezpečení firemních sítí

Klikli jste?

Ted' rozhoduje rychlost.

Samotné kliknutí ještě neznamená napadení.

Co se stalo potom?

Podle toho jednejte.

01 Jen se otevřela stránka s přihlášením

Zavřete ji. Nic nezasílatejte, nic nestahujte a nic neinstalujte. S aktualizovaným zařízením se pravděpodobně nic nestalo.

02 Zadali jste heslo

Hned ho změňte přes skutečný web, ne přes odkaz od útočníka. Pokud to služba umožňuje, odhlaste ostatní zařízení. V e-mailu zkontrolujte nastavení přeposílání zpráv. Měli jste stejné heslo jinde? Změňte ho i tam na jiné.

03 Zadali jste údaje z karty

Nebo jste potvrdili platbu? Hned volejte banku na číslo z karty nebo z aplikace. Kartu zablokujte a požádejte o zastavení nebo reklamaci platby. Rozhoduje každá minuta.

04 Nainstalovali jste aplikaci

Nebo jste někomu povolili vzdálený přístup? Zařízení hned odpojte od internetu nebo vypněte. Banku kontaktujte z nenapadeného zařízení a napadené nechte zkontrolovat odborníkem.

Nestyďte se. Zavolejte hned.



Banka

Číslo z karty nebo z bankovní aplikace. Kartu zablokujete i sami v aplikaci.



Policie ČR

Linka 158. Při ztrátě peněz podejte oznámení.



Váš IT technik

Kontrola zařízení, e-mailu a účtů.

A řekněte to kolegům i rodině. Stejná zpráva přijde i jim.

JEDNA VĚC NA ZÁVĚR

Než kliknete, zastavte se.
Ověřte legitimitu jinou cestou.



Děkuji. Ptejte se.

Ing. Dominik Malčík, Ph.D.

Zakladatel a CEO, Redamp.io

dominik.malcik@redamp.io • +420 724 844 313



Nové podvody z Česka

kb.redamp.io/cs/blog →