



Oddělení kybernetické bezpečnosti • FORENZNÍ LABORATOŘ

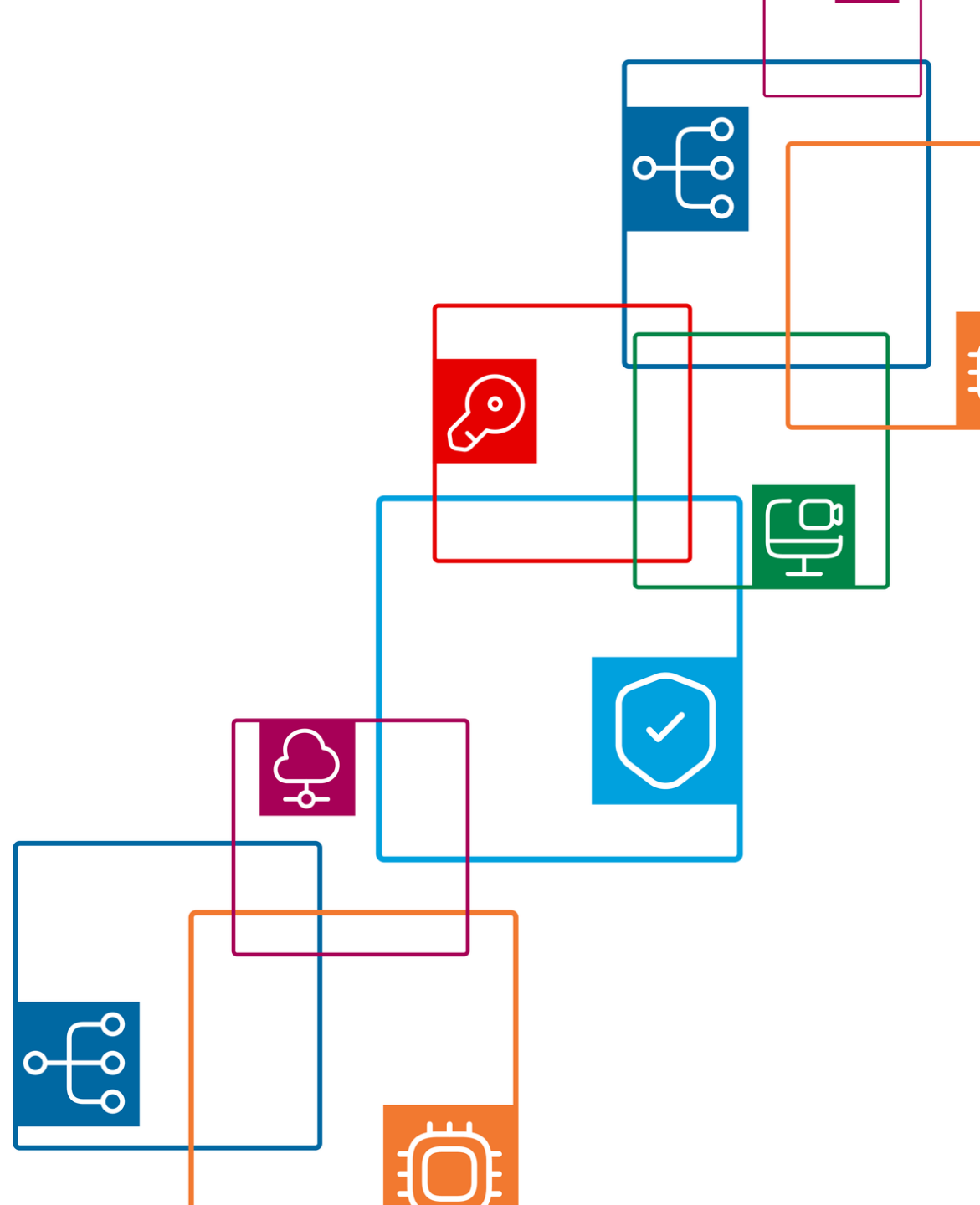
Trendy v phishingu a sociálním inženýrství

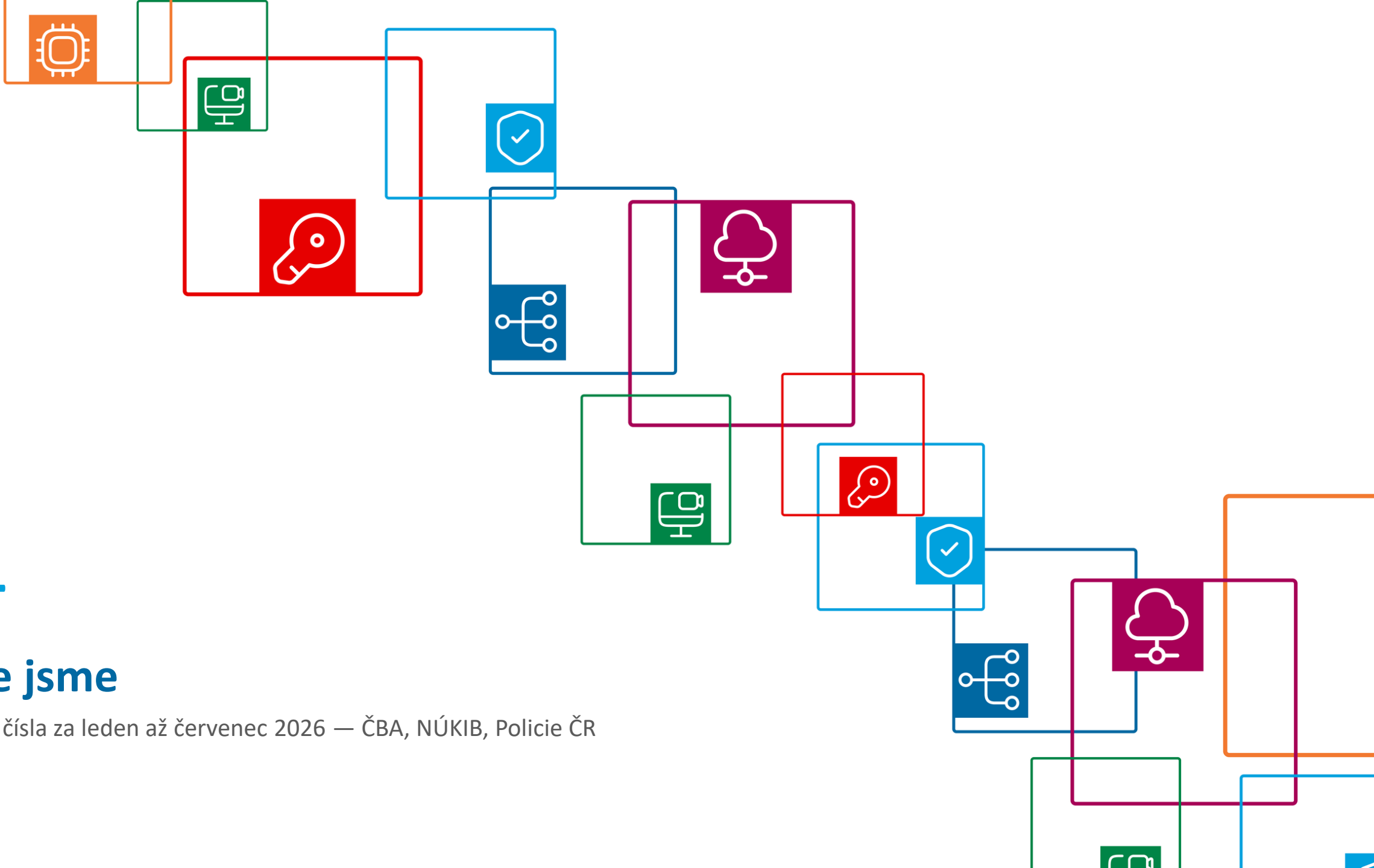
aneb proč jsou naše varování často k ničemu

Radomír Orkáč

Forenzí laboratoř • Oddělení kybernetické bezpečnosti
CESNET, zájmové sdružení právnických osob

Phishingator Workshop 2026 • Konference CESNET ke 30 letům
1. října 2026 • Telehouse • 10:45–11:20





01

Kde jsme

Česká čísla za leden až červenec 2026 — ČBA, NÚKIB, Policie ČR

Škody rostou čtyřikrát rychleji než počet útoků

10 mld Kč

se podvodníci pokusili získat

1,9 mld Kč

skutečná škoda

8,1 mld Kč

banky ubránily — 81 %

62 705

případů, meziročně +20 %

+79 %

meziroční nárůst škod

30 335 Kč

průměrná škoda na jednu oběť

Případů přibýlo o pětinu, ale škody o 79 procent. Kyberkriminalita dnes tvoří 13,6 % veškeré kriminality v ČR.

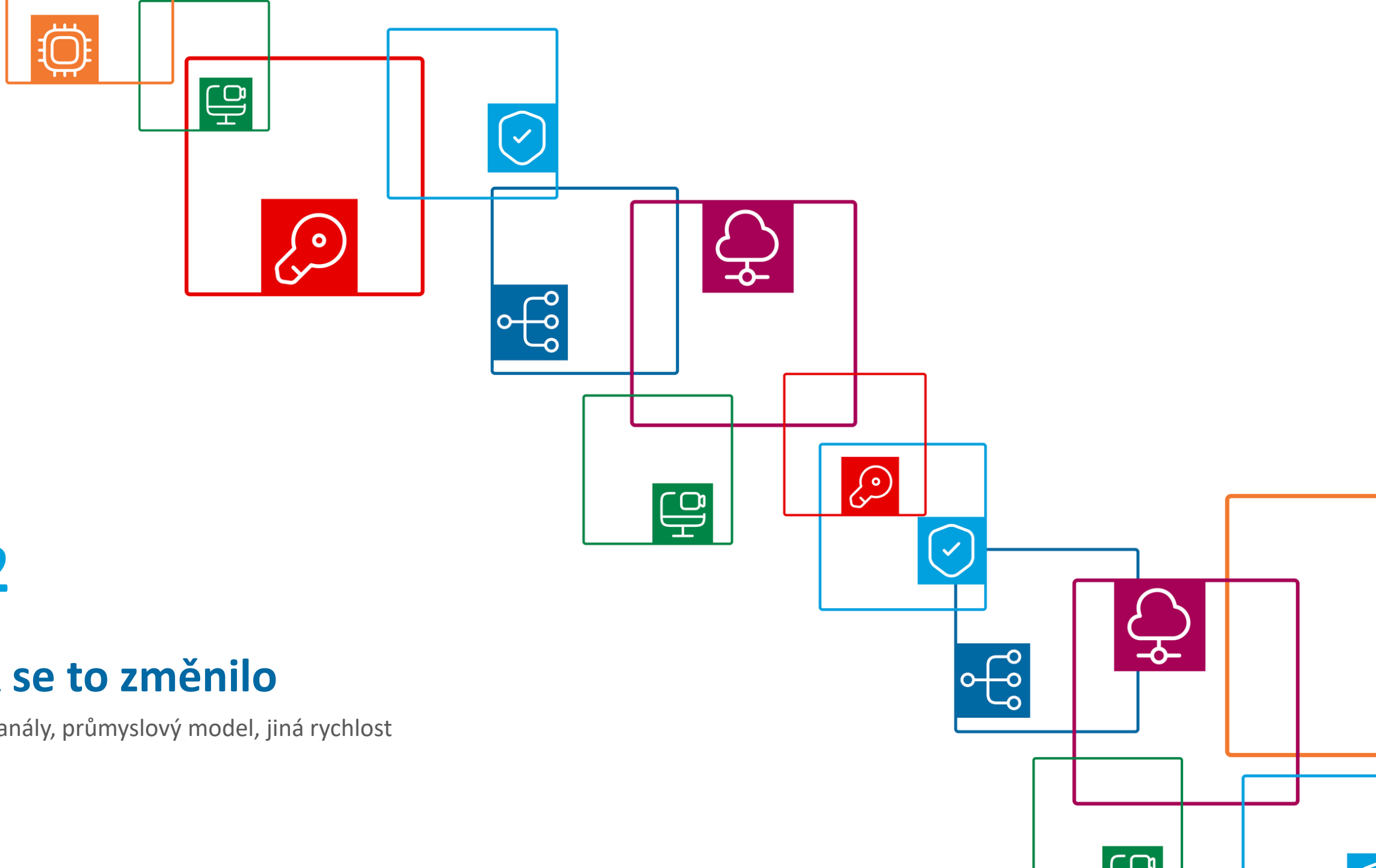


Pointa: Obrana, která funguje, se přesunula na konec řetězce — platbu zachytí banka, ne my. Těch zbylých 19 % je 1,9 miliardy.

02

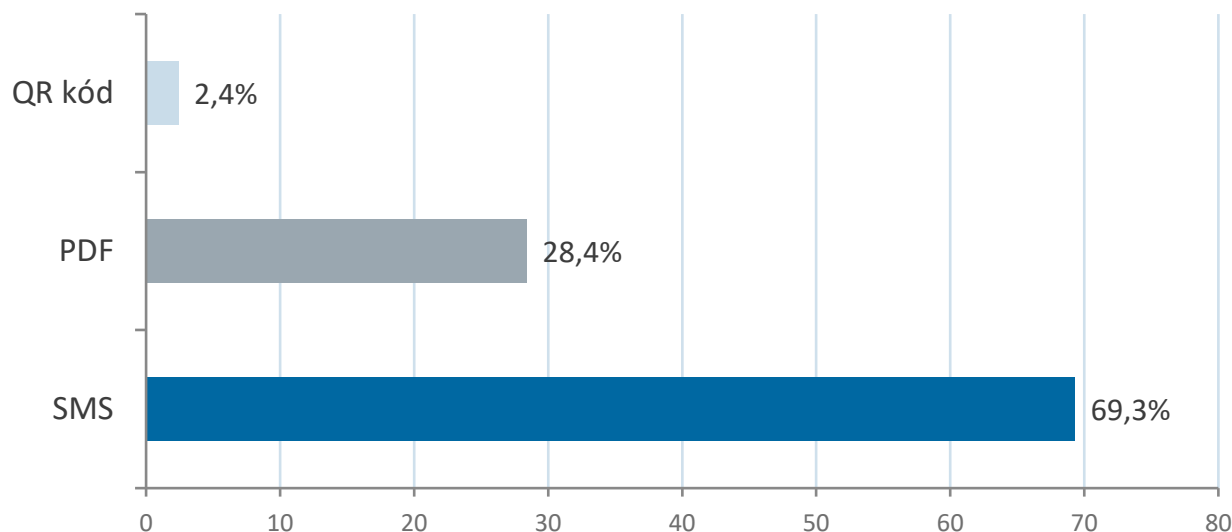
Jak se to změnilo

Jiné kanály, průmyslový model, jiná rychlost



V mobilu dorazí phishing nejčastěji esemeskou

Jakou cestou přichází phishing do mobilu (podíl v %)



o 40 % častěji lidé kliknou
na mobilu než v e-mailu — medián, Verizon DBIR 2026

15,4 % → 17,3 %
podíl SMS a sociálních sítí na veškerém phishingu, mezikvartálně
— APWG Q4 2025



Pointa: Školíme lidi na e-mail, jenže sedm z deseti phishingových zpráv dorazí do mobilu esemeskou. A na telefonu člověk nemá čas ani nástroj, jak si odesílatele ověřit.

Jakmile obrana začne fungovat, útok se přesune jinam

CO V ČESKU ZABRALO

- Operátoři blokují přes milion podvodných SMS měsíčně
- Podvržená telefonní čísla (spoofing) má ČTÚ podle vlastního vyjádření pod kontrolou
- Od 7/2025 si operátoři smějí bez souhlasu uživatele předávat provozní údaje a na vyžádání i informace o rizikových hovorech bankám
- Podezřelou SMS lze zdarma přeposlat operátorovi na číslo 7726 — na klávesnici slovo SPAM

CO SE STALO PAK

- Útočníci odešli na WhatsApp, iMessage a RCS — nástupce SMS, který zprávy posílá přes internet
- Operátor vidí jen to, že telefon komunikoval s WhatsAppem — ne s kým a už vůbec ne o čem
- Zprávy jsou šifrované od odesílatele k příjemci — nevidí do nich ani platforma
- Filtr na úrovni sítě je proti tomu z principu slepý



Pointa: Když jeden kanál zavřeme, útočník přejde na další. Zablokovaných SMS přitom přibývá dál a vypadá to jako úspěch — jenže tím měříme kanál, ze kterého už odešel. Kolik podvodů protéklo přes WhatsApp, nevíme.

Falešná SMS o dluhu u VZP vás může i zadlužit

„Dobrý den, evidujeme u Vás neuhrazený poplatek.
Prosíme o jeho uhrazení co nejdříve.“

<https://vzp-govcz-e-vzp.casa>

- Doména jen skládá známé zkratky — vzp, gov, cz. Skutečná adresa je vzp.cz
- Stránka nechce číslo karty — chce přihlášení přes bankovní identitu
- Podle VZP se podvod masivně šířil v druhé polovině září 2026

PROČ JE TO HORŠÍ NEŽ KRÁDEŽ

S bankovní identitou útočník nevybere jen účet.
Může si vaším jménem sjednat půjčku.

Škoda proto nemusí skončit tím, co na účtu máte.

*„VZP nikdy nerozesílá podobné SMS zprávy s výzvou k okamžité platbě prostřednictvím přiložených odkazů.“
— Jan Svoboda, ředitel Odboru bezpečnosti VZP*



Pointa: U VZP je pojištěno kolem šesti milionů lidí, tedy víc než polovina republiky — a komukoli z nich tahle zpráva dává smysl.

SMS blaster pošle zprávu úplně mimo operátora

SMS blaster je falešná základnová stanice, obvykle v autě nebo v batohu. Přesvědčí okolní telefony, aby se přihlásily k ní místo k síti operátora, přepne je na staré 2G — kde se síť telefonu nijak neproказuje — a pošle jim SMS jen přes rádio. Zpráva tedy vůbec neputuje sítí: skončí rovnou v telefonech, které má anténa zrovna v dosahu.

desítky tisíc

připojených telefonů k jedinému autu

13 000 000

výpadků připojení k síti za pět měsíců

911

po dobu výpadku omezená tísňová linka

Toronto, listopad 2025 až březen 2026 — první doložený případ v Kanadě.

Nemíří na telefonní čísla

Zprávu dostane každý telefon v dosahu antény.
Útočník nemusí znát jediné číslo.

Končí u dosahu antény

Dál se nikam nepředává — proto s ní
pachatelé jezdili po městě.

Nejde zachytit ani nahlásit

Operátor ji nikdy neviděl: nemá ji na čem
zablokovat ani jak dohledat na 7726.



Pointa: Podvod o peníze se dá zvrátit. Nedovolaná tísňová linka ne — a tohle je vrstva, na kterou žádné naše opatření nedosáhne.

Phishing se dnes prodává jako předplatné

Darcula (nástroj)

884 000 karet

Hotová sada na výrobu podvodných stránek, pronajímá se jako předplatné. Od roku 2025 si stránky nechá vygenerovat umělou inteligencí.

Lucid (nástroj)

169 zneužitých značek

Rozesílá zprávy přes iMessage a RCS, aby obešla filtry na SMS. Zneužila značky 169 firem a úřadů v 88 zemích.

Smishing Triad (sít skupin)

194 000 domén

Volná síť skupin kolem těchto nástrojů. Vydává se za poštu, celní správu nebo výběrčí mytného.

Na druhé straně není jeden člověk, ale dodavatelský řetězec. Ten, kdo vám tu zprávu poslal, často neumí naprogramovat vůbec nic — jen si předplatil hotovou sadu. Někdo jiný ji napsal, další provozuje servery, další prodává telefonní čísla a poslední pere peníze.



Pointa: Rada „všímejte si pravopisných chyb“ je mrtvá. Generativní AI odstranila jazykovou bariéru — kdo ji má ve školicích materiálech, učí lidi znak, který zmizel.

Od kliknutí ke zpeněžení uběhne 22 sekund

Útočník, který se dostane dovnitř, přístup zpravidla prodá další skupině, která z něj udělá peníze. Tohle je medián doby, za jakou to stihne:

2022

přes 8 hodin

obránce měl čas do rána



2025

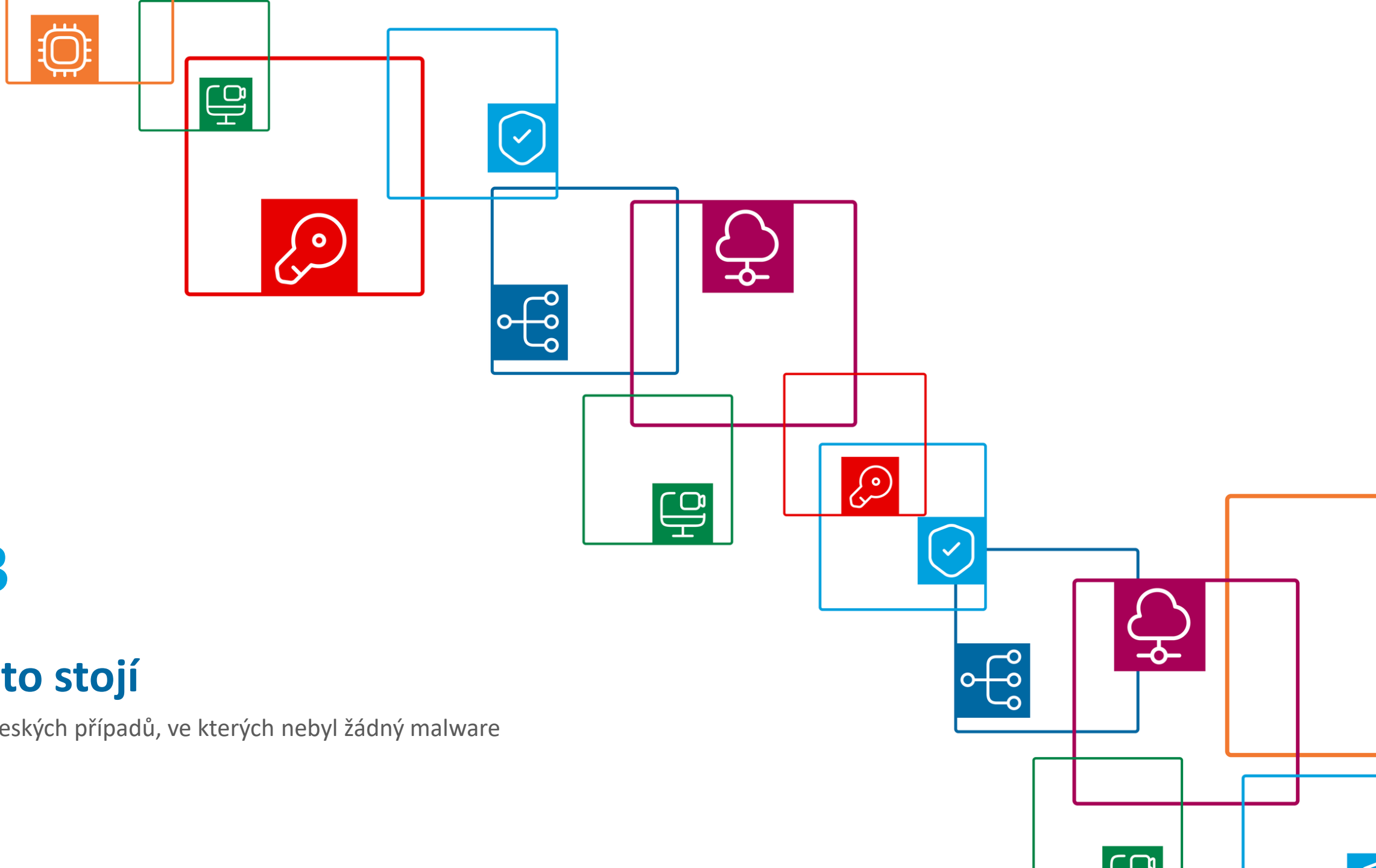
22 sekund

obránce nemá čas na nic

Není to tím, že by útočníci psali rychleji. Nástroje pro druhou fázi mají připravené předem, takže předání je okamžité.



Pointa: Jakákoli obrana postavená na tom, že si toho někdo do rána všimne, je vyřízená. Reakce se dnes měří v minutách, ne ve směnách.



03

Co to stojí

Šest českých případů, ve kterých nebyl žádný malware

Žádný hacker, jen špatné číslo účtu...

KDY A KDE	CO SE STALO	ŠKODA
Karviná, 2025	Účetní poslala platby na jiný účet, protože podvodník použil téměř identickou e-mailovou adresu – zaměnil jen dvě písmena.	1,3 mil. Kč
Českolipsko, 2024	Účetní reagovala na falešný e-mail „od ředitele“ s pokynem k platbě.	1,2 mil. Kč
Uherské Hradiště, 2025	Podvržená změna účtu: 43 000 € odešlo podvodníkům místo dodavateli.	≈ 1 mil. Kč
Česká pošta, 2018	Finanční ředitel České pošty naletěl podvodnému e-mailu a dal pokyn účetní k převodu peněz na zahraniční účet.	≈ 1 mil. Kč
Zlínsko, 2025	Šedesátiletá žena zodpovědná za finance převedla peníze podle pokynů „ředitele“. E-mail přišel z nestandardní adresy.	779 tis. Kč
Olomoucko, 2023	Účetní uhradila fakturu od pravidelného dodavatele – číslo účtu bylo podvržené.	260 tis. Kč



Pointa: V žádném z těch případů nepřišel virus ani odkaz ke kliknutí — přišel obyčejný e-mail se špatným číslem účtu. Žádná technika nemá co zachytit. Zastaví to jedině postup: změnu účtu ověřit telefonicky a platby nad limit nechat schválit dvěma lidmi.

Co mají všechny ty případy společné

1

Žádná technika

Nikde malware, nikde zneužitá zranitelnost. Jen e-mail a trpělivost.

2

Útočník o vás něco věděl dřív, než napsal

Že čekáte fakturu, že máte rezervaci v hotelu, u které jste pojišťovny. Nemusel číst poštu, stačí, co se dá zjistit.

3

Naletěli lidé, kteří tu práci umějí

Zkušené účetní, finanční ředitel, jednatel. Žádní nováčci, žádná nedbalost.

4

Peníze se nevrátily

Ani v jednom z uvedených případů se je nepodařilo získat zpět.



Pointa: Tohle nejsou chyby nepozorných lidí. Je to popis toho, jak vypadá dobře odvedená příprava útočníka proti vzdálenému uživateli.

WHATSAPP · 19. 9. 2026 · JMÉNEM HOTELU DIPLOMAT

Hello Radomír Orkáč,

We're contacting you on behalf of Hotel Diplomat.
During our standard pre-arrival review, we noticed
a detail that needs to be updated before your stay
from 29.09.2026 to 01.10.2026.

You can finish the review here:
<https://travel.guest-arrival-stay.com/1350506...>

If this isn't completed within the next 12 hours,
the arrangement may be released.

PROČ TO SEDĚLO

- Skutečný hotel a skutečný termín pobytu
- Odkaz nevede na hotel, ale na cizí doménu
- Dvanáct hodin, jinak „rezervace propadne“
- Odesílatel: britské číslo +44 7529 289484, ne české +420
- Únik byl na straně hotelu, ne CESNETu

19. 9. · 16:58

Zpráva dorazí na WhatsApp z
britského čísla.

19. 9. · 19:44

Skoro po třech hodinách je
nahlášená.

19. 9. · 20:00

CESNET varuje účastníky. Šestnáct
minut od nahlášení.

22. 9. · 12:35

Varuje i hotel, z neznámé domény
gomystay.com.



Pointa: Varování odešlo za šestnáct minut, rychleji to neumíme. Jenže podvod přišel WhatsAppem a varování e-mailem — kdo zareagoval hned na telefonu, žádné naše varování v tu chvíli neviděl.

VÝHRŮŽKA UČITELŮM, KRÁTCE PO 6:00

„Dneska v 8:00 do školy přijdu se semiautomatickou AR-15, nožem a granáty, zabiju každého, koho uvidím.“

Zpráva učitelům pražské Akademie řemesel, krátce po 6:00 — odeslaná z účtu žáka přes Bakaláře, systém, který používají tisíce českých škol.

- Škola vyklizena, na místě ozbrojené policejní hlídky
- Provozovatel: „nešlo o chybu na straně systému“ — neoprávněný přístup skrz konkrétního uživatele
- Nejpravděpodobněji phishing, smishing, keylogger nebo odemčené zařízení
- Podle policie šlo o druhý útok tohoto typu během jednoho týdne



Pointa: „Nešlo o chybu systému“ — systém fungoval správně, protože účet byl legitimní a přihlášení bylo platné. Odpovědnost přechází z dodavatele/správce na uživatele.

Revolut vydal data klientů na falešnou žádost

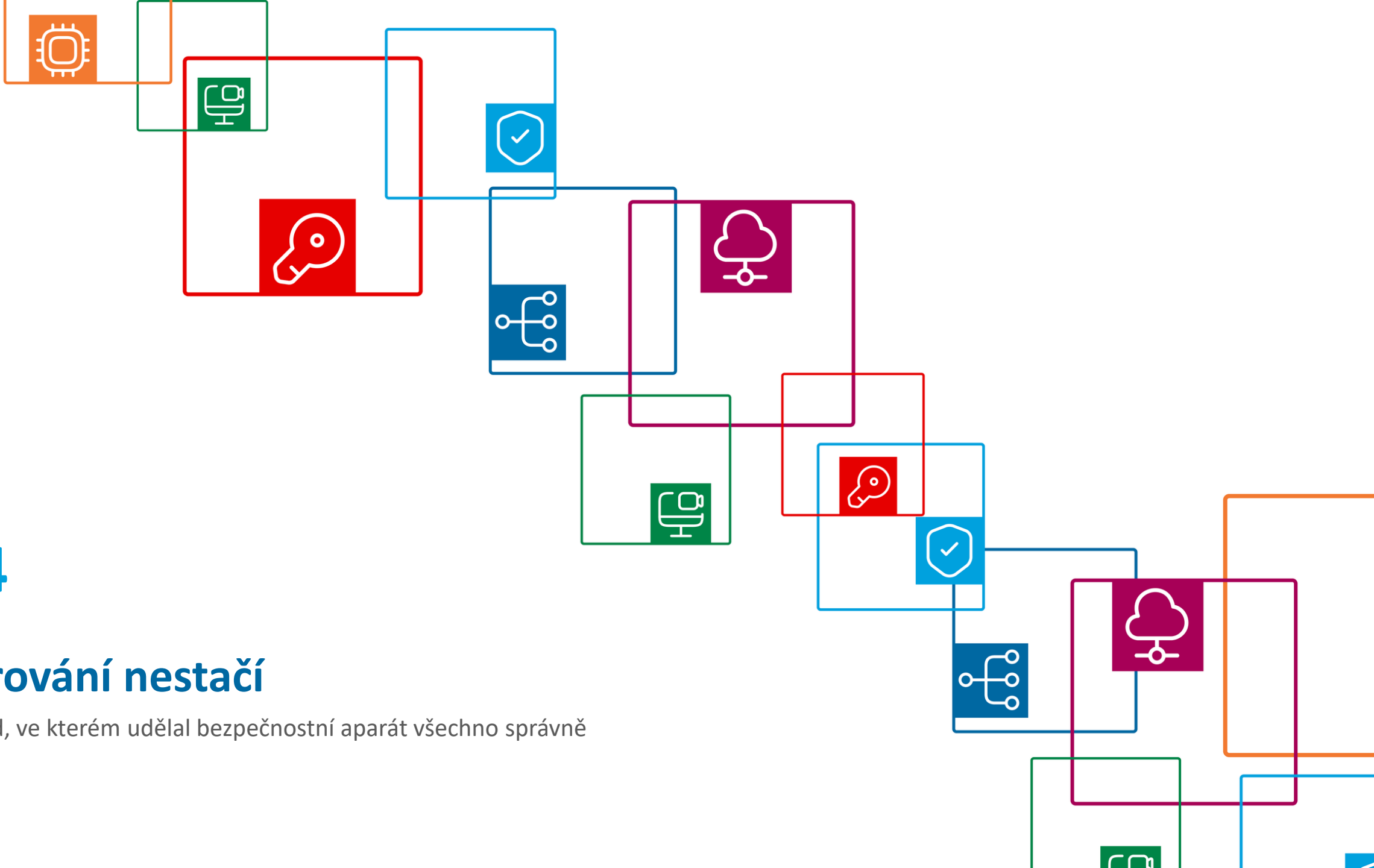
- Září 2026: neoprávněná třetí strana poslala Revolutu žádosti o informace z e-mailu na legitimní doméně vládní agentury
- Revolut jim vyhověl. Zasažen „omezený počet“ klientů — konkrétní číslo firma neuvedla
- Jde o takzvaný fake emergency data request: žádost o data kvůli „bezprostřednímu ohrožení života“, u které se nečeká na soud
- FBI před tímto postupem varovala už v roce 2024. Přístup do policejních schránek se prodává za 1 000 až 3 000 dolarů za žádost

CO ÚNIKLO

Jméno, datum narození, adresa, telefon, e-mail. Kopie dokladů totožnosti. Ověřovací selfie. Výpisy z účtu, IBAN a kompletní historie transakcí včetně bitcoinových operací.



Pointa: Tady nenaletěl nepozorný člověk, ale proces, který byl přesně na tohle postavený. Žádné školení uživatelů by to nezachytilo — ta žádost byla po technické stránce pravá.



04

Varování nestačí

Případ, ve kterém udělal bezpečnostní aparát všechno správně

Varování přišlo včas. A bylo k ničemu.

Správa nemovitostí Hradec Králové, červenec 2026 — podvodníci se vydávali za policisty a pracovníky ČNB a přesvědčili úřednici, že jsou účty v ohrožení.

PO 13. 7. 2026

Odchází první platba.

PO 13. 7. 2026 • 16:00

Ministr vnitra rozesílá všem starostům a primátorům čtyřstránkový dopis s popisem přesně tohoto scénáře.

ÚT 14. 7. 2026

Odchází druhá platba. Celkem 46 milionů korun — historicky největší škoda u tohoto typu podvodu v ČR.

ST 15. 7. 2026

Primátorka si dopis přečetla. Úřednice ho nedostala vůbec.

Proč se varování zastavilo: „*Než si to někdo další otevře a předá někomu kompetentnímu, trvá to.*“ — mluvčí radnice



Pointa: Varování je informace — útok je situace pod tlakem, a mezi tím je propast, kterou oběžník s informacemi nepřeklene.

05

Když není co postřehnout

MirrorFace vs. Jagello 2000 — srpen 2024, Ostrava



Cíl, který zdánlivě nedává smysl

- Cíl: Spolek Jagello 2000 — pořadateli Dnů NATO v Ostravě
- Útočník: MirrorFace (Earth Kasha), čínsky orientovaná APT skupina, podle ESETu podskupina APT10
- Do té doby cílila prakticky výhradně na Japonsko — tohle byl její první známý cíl v Evropě
- Návnada: Expo 2025 Ósaka, navazující na skutečnou dřívější korespondenci spolku

CO V NĚM VIDÍ FIRMA

Spolek, který nemá co ukrást

CO V NĚM VIDÍ ROZVĚDKA

- Kontakty na vojenské atašé
- Seznamy delegací
- Plány návštěv
- Korespondenci se zahraničními partnery



Pointa: Cíl nemusí dávat smysl vám. Stačí, že dává smysl útočníkovi — a nezisková organizace kolem NATO agendy ho dává dokonale.

Na prvním mailu nebylo co zachytit

MAIL Č. 1 · 26. 8. 2024 · bez přílohy, bez odkazu

Od: ██████████ <andryfrewas@gmail.com>
Předmět: Greeting from Tokyo

Dear █████-san,

I hope this email finds you well.
I have some references about the EXPO
Exhibition in Japan in 2025, if you are
interested please reply to this email
and I will send it to you.

Best,

██████████

MAIL Č. 2 · až poté, co oběť odpověděla

Od: ██████████ <andryfrewas@gmail.com>
Předmět: Re: Greeting from Tokyo

[odkaz] The EXPO Exhibition in Japan in 2025
→ OneDrive → ZIP → .docx.lnk

Dear █████-san,

I'm sending you the information about
the EXPO Exhibition in Japan in 2025.
I wish you all the best.

██████████



Pointa: Obyčejný Gmail, žádná podvržená doména — SPF, DKIM ani DMARC tu nemají co dělat. A druhý mail je „Re:“ ve vlákně, kde si oběť ten soubor sama vyžádala.

Za šest dní měl útočník ukradená data venku

KDY · 2024	CO ÚTOČNÍK UDĚLAL
27. 8.	Předseda nemá Windows, přeposílá dvěma kolegům. Oba otevrou .docx.lnk. Nasazen backdoor ANEL.
28. 8.	PuTTY, Visual Studio Code, backdoor HiddenFace
29.–30. 8.	AsyncRAT, Rubeus (Kerberos), csvde (Active Directory), frp
2. 9.	Export dat z Chromu — kontakty a uložené platební karty

14 dní

trvá v průměru, než si oběť útočníka všimne

122 dní

totéž u kyberšpionáže — tedy čtyři měsíce

Na předsedově stroji útok nefungoval. Skončil přesto na dvou dalších počítačích — přeposlal ho tam sám, v dobré víře.



Pointa: Útočník byl hotov za šest dní. Oběti špionáže si ho obvykle všimnou až po čtyřech měsících. Jeho hodiny běží úplně jinou rychlostí než naše — a on nečeká, až ho doženeme.

Naletěl i autor Have I Been Pwned

- Březen 2025. Troy Hunt provozuje službu, kde si půl světa ověřuje, jestli mu unikly přihlašovací údaje
- Phishing se tvářil jako problém s doručením jeho newsletteru. Doména mailchimp-sso.com
- Zadal heslo i jednorázový kód. Útočník ho v reálném čase přeposlal do pravého Mailchimu
- Seznam 16 000 odběratelů byl exportován během okamžiku, z IP adresy v New Yorku
- 1Password mu heslo nenabídl — a on šel i tak dál

JEHO VLASTNÍ SLOVA (PŘEKLAD)

*„Zásadní roli hrála únava.
Nebyl jsem dost pozorný.“*

O jednorázových kódech:

„Proti automatizovanému phishingu jsou naprosto k ničemu — útočník ten kód přepošle dál hned, jak ho zadáte.“

A takhle se takový seznam použije: Letos v září uniklo 347 000 adres zákazníků Trezoru, českého výrobce peněženek na kryptoměny. Phishing pak přišel z jeho vlastní odesílací adresy, takže prošel všemi kontrolami pravosti odesílatele. Kliklo 2 500 lidí.



Pointa: Informovanost nebyla ta chybějící proměnná. A jednorázový kód phishing nezastaví — zastaví ho až passkey nebo hardwarový klíč.

Varování je informace. Útok je situace pod tlakem.

Mezi tím je propast, kterou oběžník nepřeklene. Překlene ji jedině to, co si člověk nacvičil — ne co si přečetl, ale čím si prošel.

CO NEFUNGUJE

- Rozeslat oběžník a jednou ročně školení
- Rada „všimněte si chyb v textu“
- Jednorázový kód proti cílenému phishingu
- Čekat, že to někdo nahlásí do rána

CO FUNGUJE

- Změnu čísla účtu ověřit telefonem
- Platby nad limit schvalují dva lidé
- Passkey nebo hardwarový klíč
- Pravidelné cvičné phishingy

CO NEZAJISTÍ NIKDO

- Že se to nestane
- Že na útoku bude vždy něco k postřehnutí
- Že budete vždy odpočatí
- Že jsme udělali maximum



Pravidelné cvičení nezaručí, že se to nestane. Zaručí jedinou věc — že až to přijde, nebude to poprvé, co to ten člověk vidí.

Zdroje v pořadí, jak případy v přednášce zazněly.

Česká čísla 2026 (ČBA, NÚKIB, Policie ČR)

investujeme.cz/kratke-zpravy/e-smejdi-letos-zautocili-na-10-miliard-korun/

Statistiky smishingu (Zimperium, APWG, DBIR)

deepstrike.io/blog/smishing-statistics

Opatření ČTÚ proti spoofingu

ctu.gov.cz — „Opatření Úřadu proti spoofingu fungují“

Falešné SMS o dluhu u VZP, září 2026

novinky.cz — „Máte dluh u VZP“, 17. 9. 2026

SMS blastery, Toronto 2026

therecord.media/canada-sms-blasters-cybercriminals

Darcula a AI upgrade

netcraft.com/blog/ai-enabled-darcula-suite-makes-phishing-kits-more-accessible-easier-to-deploy

Lucid PhaaS přes iMessage a RCS

thehackernews.com/2025/04/lucid-phaas-hits-169-targets-in-88.html

Mandiant M-Trends 2026 (dwell time, 22 s)

cloud.google.com/blog/topics/threat-intelligence/m-trends-2026

Šest českých BEC případů

safetest.cz/pribeh

Podvod jménem hotelu Diplomat, 19. 9. 2026

podvodná zpráva a varování CESNETu účastníkům konference

Výhrůžka přes Bakaláře, září 2026

magazin.aktualne.cz — „Výhrůžka smrti přišla přes aplikaci...“

Revolut a falešná žádost úřadu

techcrunch.com/2026/09/12/revolut-confirms-customer-data-breach-through-fake-government-requests/

Mechanismus fake emergency data request

krebsonsecurity.com/2024/11/fbi-spike-in-hacked-police-emails-fake-subpoenas/

Hradec Králové, 46 milionů

novinky.cz — „Úřednice posílala miliony podvodníkům...“, 24. 7. 2026

MirrorFace — Operation AkaiRyū

welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/

Troy Hunt — jak se nechal phishnout

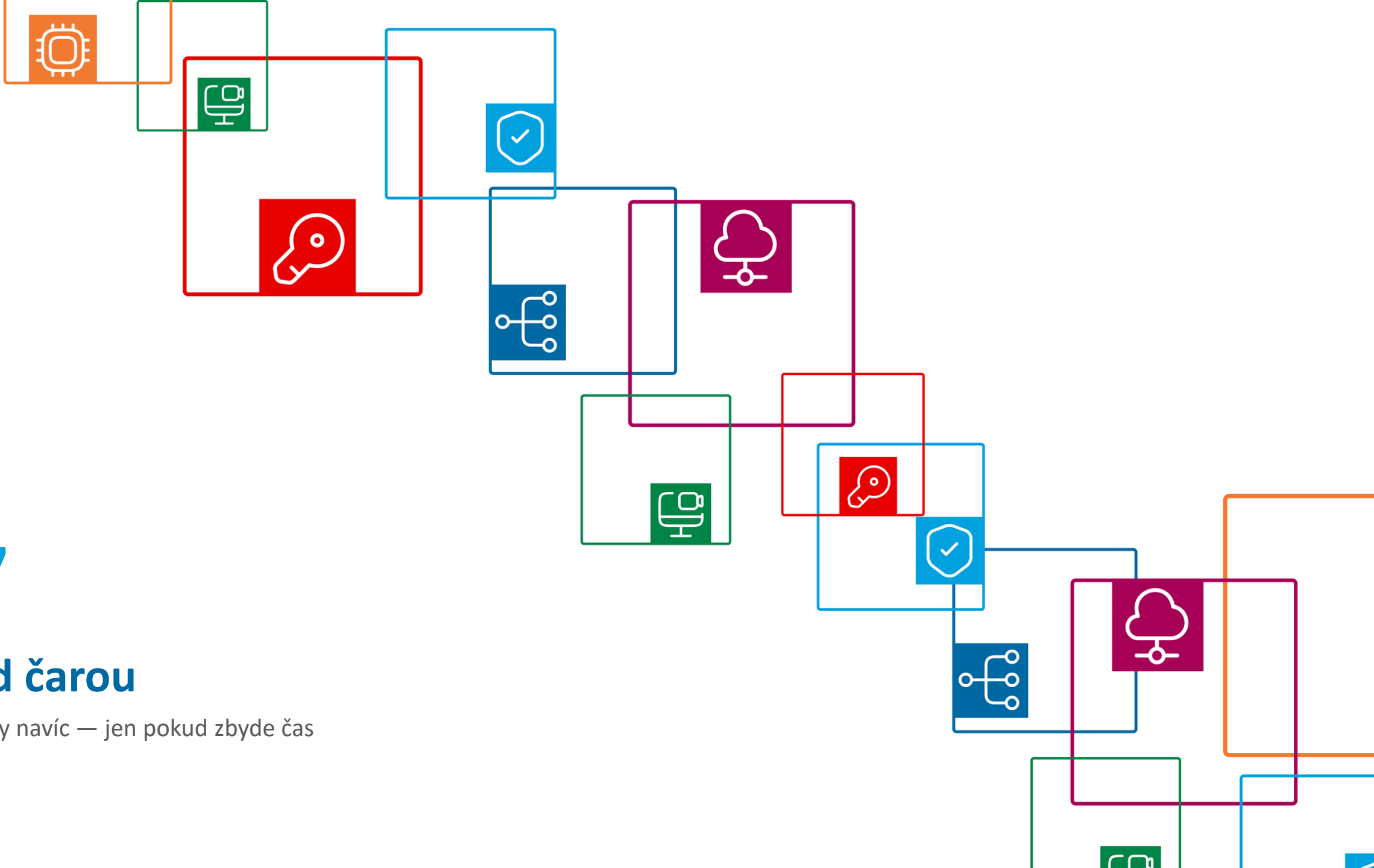
troyhunt.com/a-sneaky-phish-just-grabbed-my-mailchimp-mailing-list/

Rozhovor se Zbyňkem Pavlačíkem (Jagello)

novinky.cz — „Povodně přišly v nejhorší okamžik“, 18. 12. 2024

Trezor a Brevo, 347 000 adres

lupa.cz — „Trezor varuje před phishingovými e-maily“, 11. 9. 2026



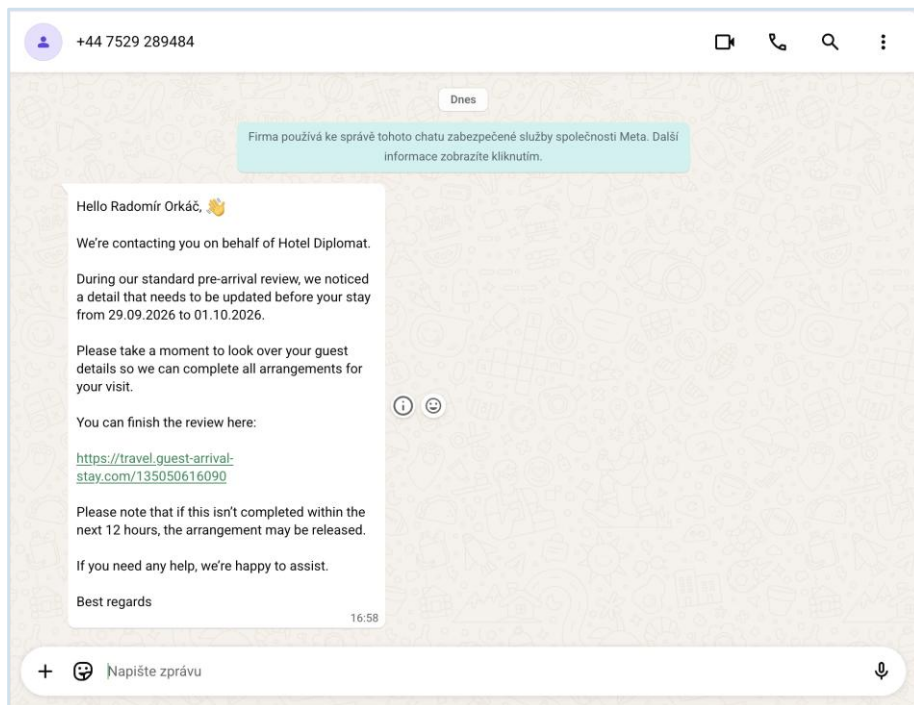
07

Pod čarou

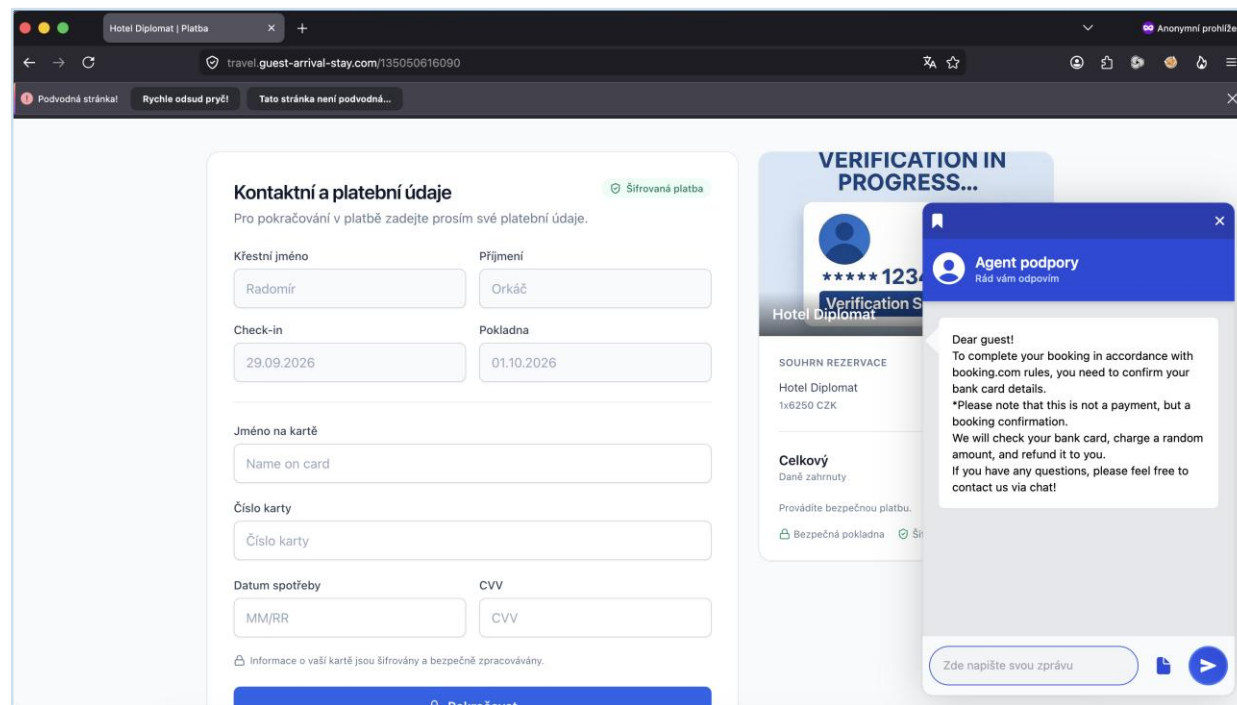
Ukázky navíc — jen pokud zbyde čas

Jak ten podvod na konferenci vypadal

Vlevo zpráva, jak dorazila. Vpravo stránka, na kterou vedl odkaz — s předvyplněným jménem, termínem pobytu i cenou.

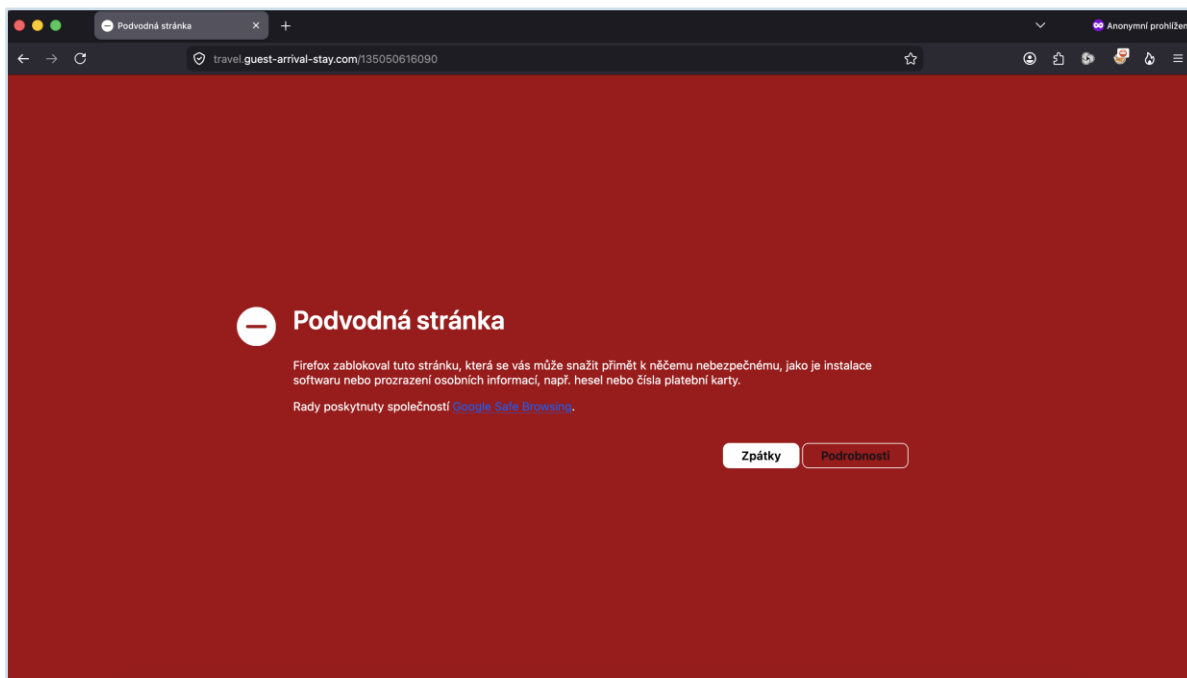


WhatsApp, 19. 9. 2026 v 16:58 — odesílatel +44 7529 289484

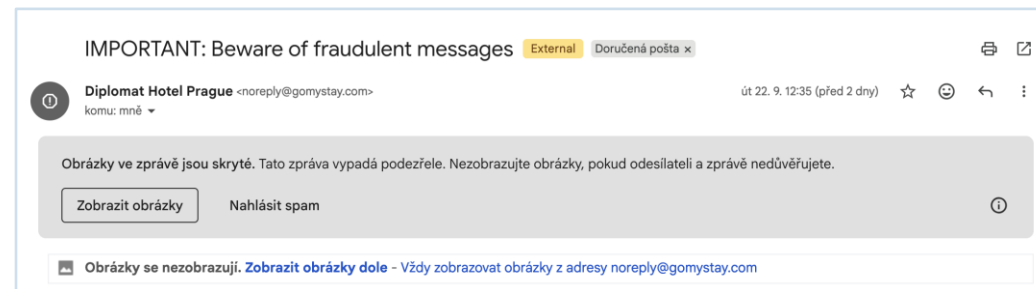


Jméno, check-in 29. 9., odjezd 1. 10. i částka 6 250 Kč — všechno předvyplněné. Chat vedle vysvětluje, že karta se jen „ověří“.

Obě ochrany se ozvaly. Jedna se spletla.



Prohlížeč podvodnou stránku zablokoval — ale až ve chvíli, kdy na odkaz někdo klikl.



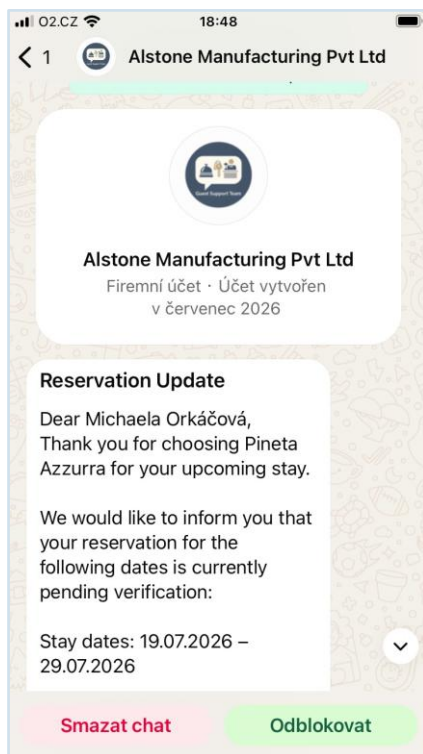
Pravé varování hotelu, 22. 9. ve 12:35.

A TEĎ TA IRONIE

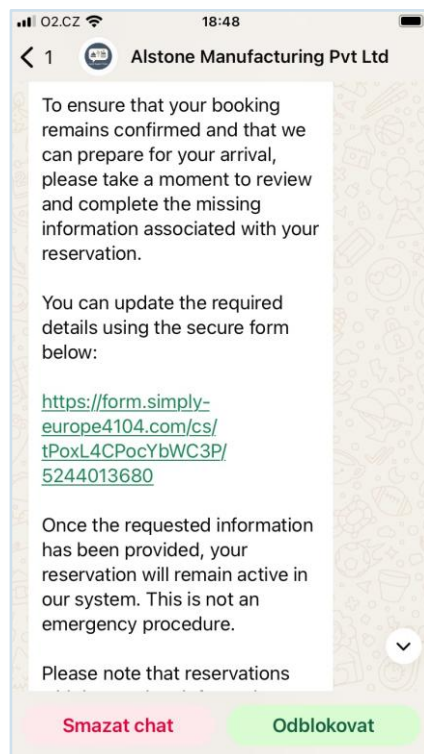
Gmail označil za podezřelé to pravé varování — cizí odesílatel, neznámá doména, skryté obrázky. Podvodná zpráva na WhatsAppu žádnou takovou nálepku nedostala.

Poznáte, co je pravé a co podvrh?

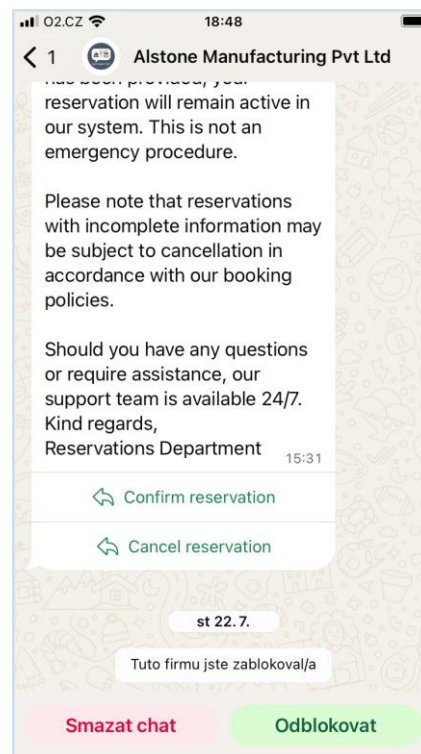
Rezervace v hotelu Pineta Azzurra na 19.–29. 7. 2026 byla skutečná. Tahle zpráva dorazila přes WhatsApp krátce před pobytem.



Firemní účet, založený v červenci 2026



Odkaz na form.simply-europe4104.com



Tlačítka Confirm / Cancel reservation

CO MĚLO ZARAZIT

- Odesílatel je Alstone Manufacturing Pvt Ltd — výrobní firma, ne hotel
- Účet na WhatsAppu vznikl pár dní před pobytem
- Formulář běží na doméně, která s hotelem nesouvisí
- Hrozba zrušením rezervace, když údaje nedoplníte

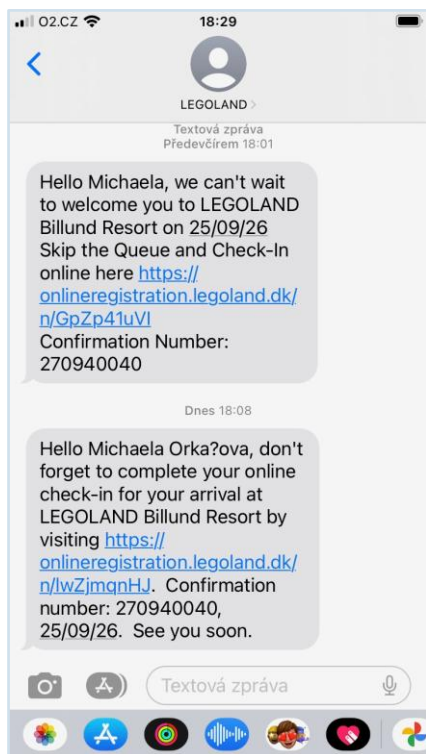
Sedělo přitom jméno, hotel i přesný termín pobytu.

ODKUD TO VĚDÍ

V dubnu 2026 přiznal Booking.com neoprávněný přístup k údajům o rezervacích.

A co tohle? Tentýž telefon, jiný pobyt

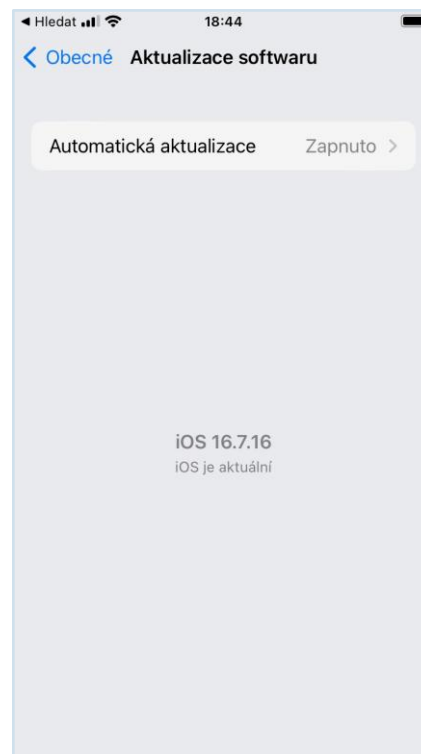
Rezervace v LEGOLAND Billund na 25. 9. 2026 byla taky skutečná. Tyhle zprávy dorazily esemeskou, rovněž před pobytem.



SMS od odesílatele LEGOLAND s číslem rezervace



Prohlížeč u toho odkazu varuje před certifikátem



Telefon hlásí, že systém je aktuální

CO JE NA TOM ZAJÍMAVÉ

- Odkaz míří na legoland.dk — doménu skutečného resortu
- Přesto prohlížeč hlásí, že připojení není soukromé
- Druhá zpráva komolí jméno na „Michaela Orka?ova“
- Proč certifikát neprošel, nevíme — může být chyba na obou stranách

Ta pravděpodobně pravá zpráva vypadá podezřeleji než ten podvrh vedle.