



Phishingator v roce 2026

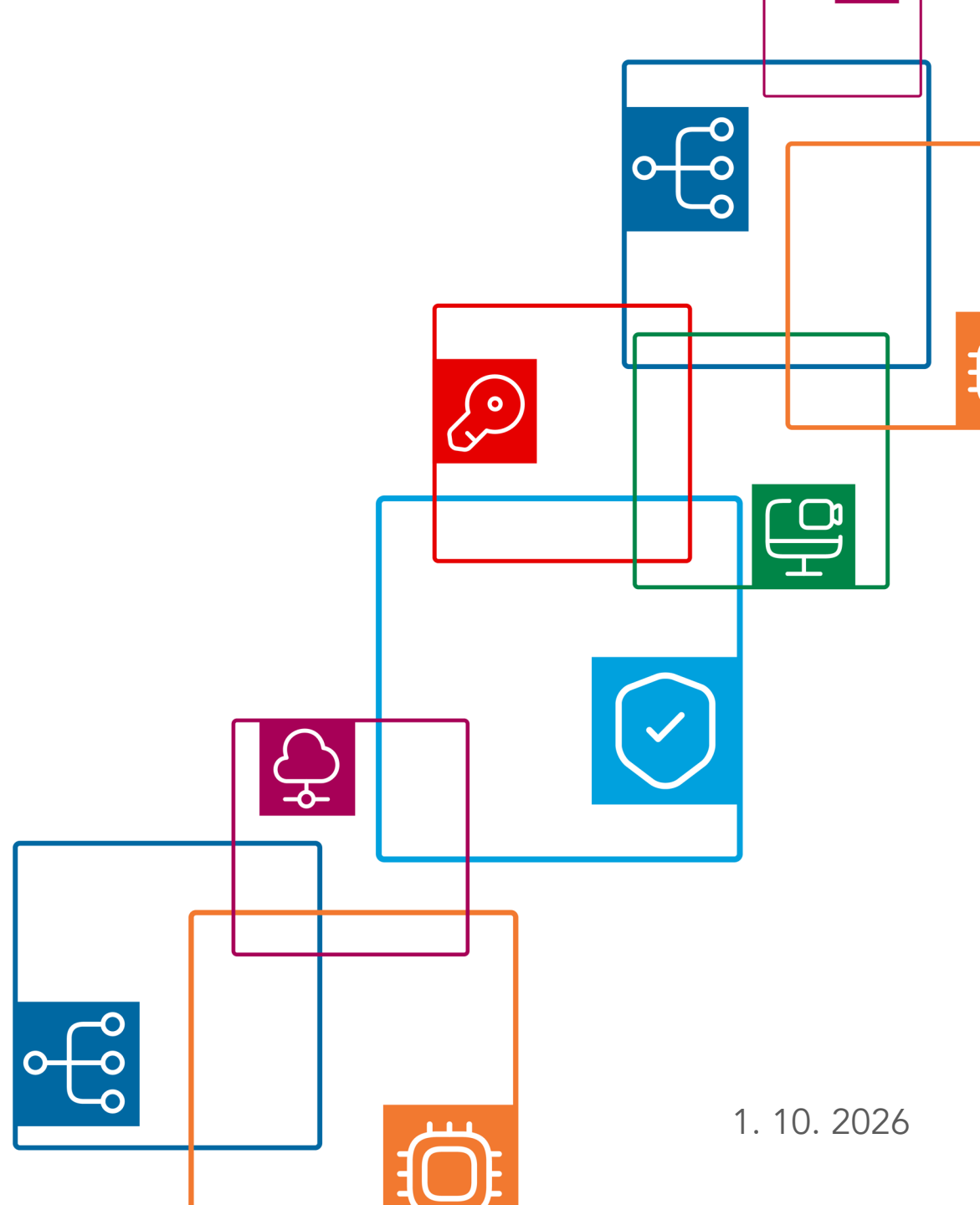
Zkušenosti z provozu, novinky a další plány

Martin Šebela

CESNET FLAB

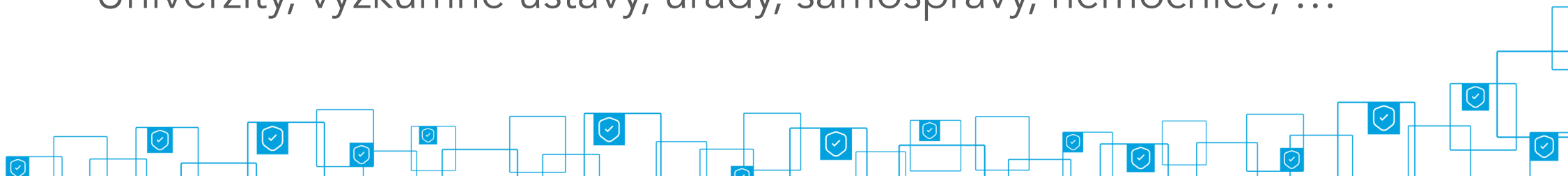
Oddělení kybernetické bezpečnosti

Konference e-infrastruktury CESNET 2026
Phishingator Workshop 2026



1. 10. 2026

- **Nástroj pro simulované phishingové kampaně**
 - Příprava podvodného e-mailu a přihlašovací stránky
 - Výběr příjemců a sledování reakcí
- **Vzdělávání uživatelů vlastní zkušeností**
 - Phishing nanečisto v bezpečném prostředí
 - Vzdělávací stránka s vysvětlením varovných signálů
 - Podpora vzdělávání podle ZKB
- **Phishingator napříč organizacemi**
 - Univerzity, výzkumné ústavy, úřady, samosprávy, nemocnice, ...



Díky Vám Phishingator roste



Správa informačních
technologií **Plzeň**



Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice



Univerzita Palackého
v Olomouci



26

Zákaznických instancí v provozu

Samostatné i sdílené instance pro více zákazníků



Phishingator jako služba

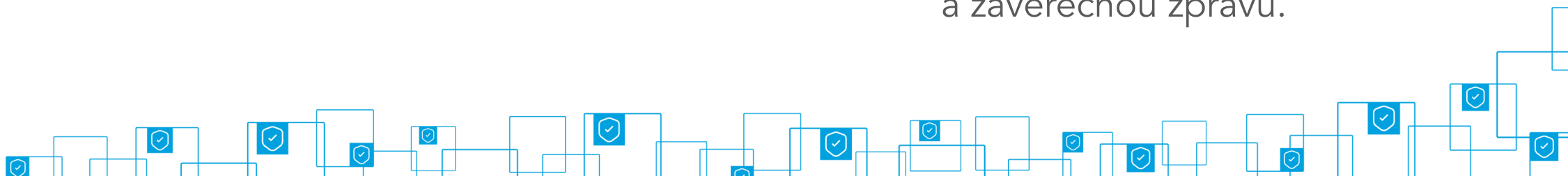
Nasazení přizpůsobíme
vaším potřebám.
Postaráme se o provoz.
Kampaně máte ve svých
rukou.

Kampaně s naší pomocí

Phishingator už používáte.
Pomůžeme s přípravou
a realizací kampaně.

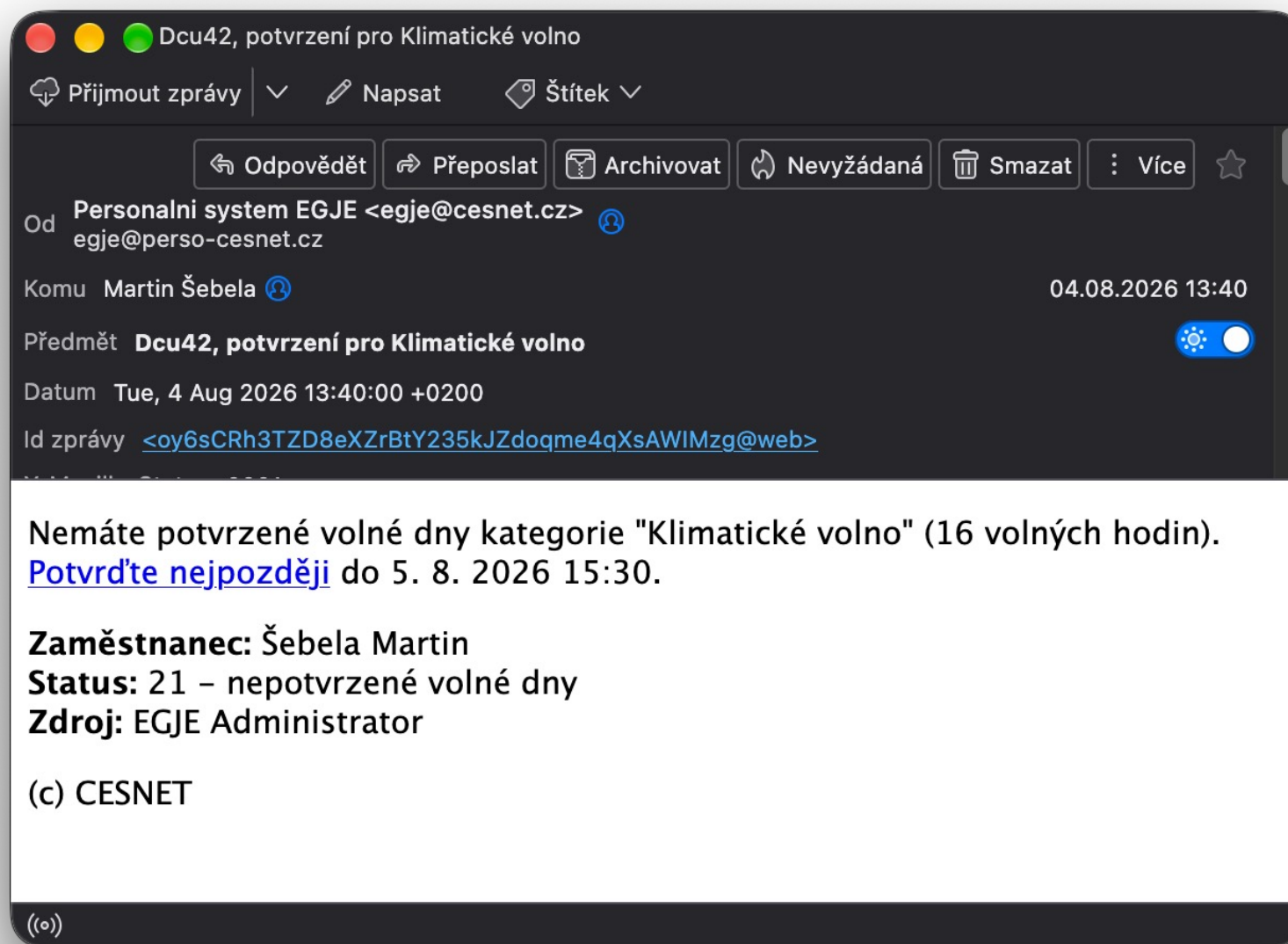
Phishingové testy na klíč

Kampaň připravíme
a provedeme.
Uspořádáme školení
uživatelů.
Dodáme výsledky
a závěrečnou zprávu.



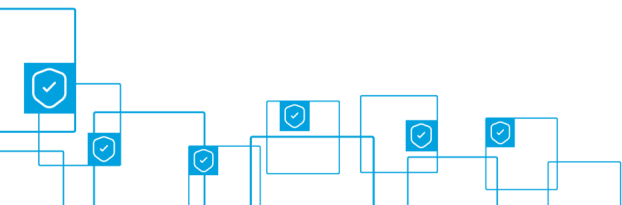
Phishingator v praxi

Zkušenosti z kampaní a reakce uživatelů



- Nešetříme ani zaměstnance CESNETu
- Cvičné phishingové e-maily
 - Pro všechny zaměstnance
 - Pro dobrovolníky
- Spear phishing
 - 13:40 – rozeslání e-mailů
 - 13:40 – první **získané heslo**
 - 13:41 – druhé a třetí **získané heslo**

17			návštěva stránky ohlášeno	4. 8. 2026 13:50:05
16			zadání neplatných údajů	4. 8. 2026 13:47:05
15			návštěva stránky	4. 8. 2026 13:46:39
14			zadání neplatných údajů ohlášeno	4. 8. 2026 13:45:44
13			návštěva stránky	4. 8. 2026 13:45:30
12			návštěva stránky	4. 8. 2026 13:45:15
11			návštěva stránky	4. 8. 2026 13:42:38
10			zadání platných údajů	4. 8. 2026 13:41:46
9			návštěva stránky	4. 8. 2026 13:41:37
8			návštěva stránky ohlášeno	4. 8. 2026 13:41:18
7			zadání platných údajů	4. 8. 2026 13:41:11
6			návštěva stránky ohlášeno	4. 8. 2026 13:41:02
5			návštěva stránky	4. 8. 2026 13:41:00
4			návštěva stránky	4. 8. 2026 13:40:53
3			návštěva stránky	4. 8. 2026 13:40:52
2			zadání platných údajů	4. 8. 2026 13:40:46
1			návštěva stránky	4. 8. 2026 13:40:39



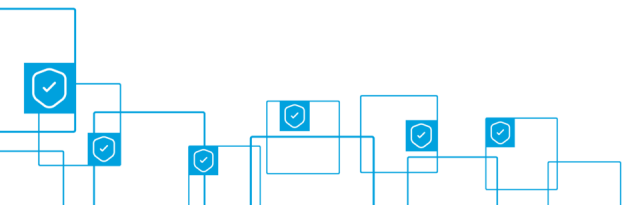
■ Univerzity

- Každoroční kampaně pro první ročníky
- Pravidelné školení zaměstnanců



■ Další organizace

- Průběžné kampaně po menších skupinách
- Jednorázové kampaně pro všechny zaměstnance



Rok 2025

≈ 75 000

unikátních uživatelů oslovených
cvičným phishingem

Získání platného hesla

≈ 10 %

průměrná úspěšnost kampaní

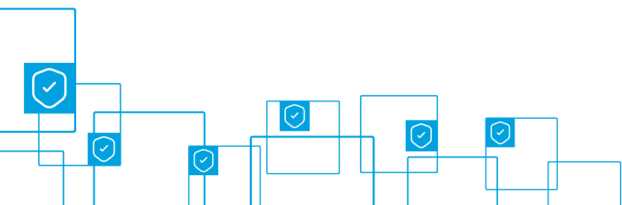
≈ 13 000

zachycených platných hesel

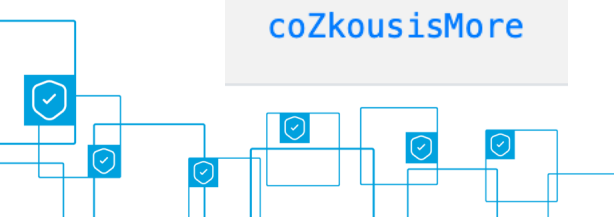
i 20 % a více

u HTML phishingu

Záleží na obtížnosti scénáře, skupině příjemců (např. studenti vs. zaměstnanci).



- Ohlášení phishingu
- Reakce na zjištěné cvičení – pozitivní, negativní
- Několik úrovní
 - Vzkazy do formuláře na podvodné stránce
 - Přímé odpovědi na podvodný e-mail
 - Kontaktování autorů kampaně – IT oddělení, CSIRT týmu
 - Kontaktování CESNET Phishingator týmu



```
' OR 1=1 -- -
```

```
admin
```

```
Dobrý pokus :-) Zdravím ajťáky z kyberbezpečnosti...
```

```
haNiceTryBuddyAle...
```

```
coZkousisMore
```

```
Je toto rybaření?
```

```
"Admin';--"
```

```
nenachytamse
```

```
Dobrý pokus :-)
```

Dobrý den,

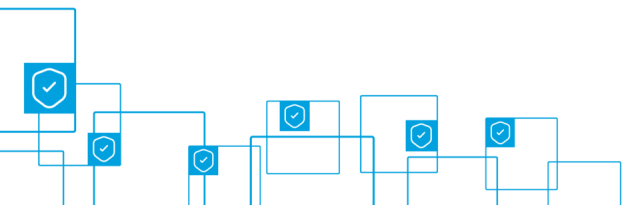
dnes jsem kliknul na odkaz v mailu dole. To mě vedl na stránku phishingator, který mě upozornil, že právě jsem propadl ve zkoušce na phishing a nabídl mi službu Phisingator, který by mě pravidelně zkoušel z phishingu. To bych chtěl, dokonce potřeboval. Chtěl bych si ujistit, [REDACTED] opravdu nabízí tuto službu. Vyhledal jsem to na [REDACTED] a nenašel. Mohli byste mi poslat odkaz? Díky.

Dobrý den
Haha, moc pěkný! O projektu phishingator čtu prvně.

Dobrý den,

to jste mne teda dostali. Na odesilatele se normalne divam, zejména, kdyz se ode mne zada delat neco s bankovnictvim apod. Tentokrat jsem se odesilatele fakt nevsihl. Ale je fajn, ze to takhle delate 😊

To je super,
využil jsem to rovnou do výuky :D

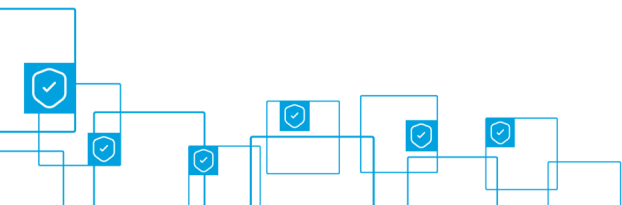


- Ne každý uživatel přijme kampaň pozitivně

Vážený pořadateli cvičných phishingů,

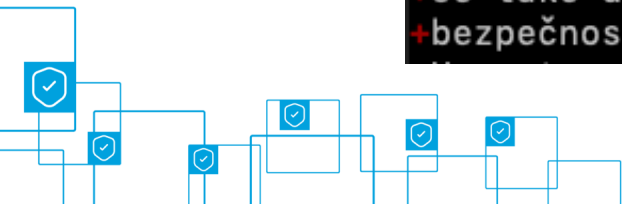
chytili jste mě a nemám z toho radost. Jeden díl viny je můj: dělal jsem to
+rozespalý, a nekontroloval si adresu odesílatele a webu. A víte proč jsem je
+nekontroloval? Protože mě [redacted] změnou hesla otravuje pravidelně. To je Váš díl
+viny.

- I negativní reakce jsou příležitostí vysvětlit smysl kampaně



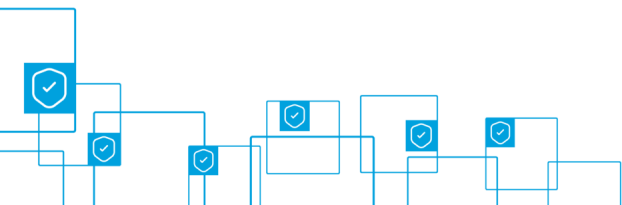
- Uživatel rozpoznal časový nátlak a podezřelý jazyk

```
Vážený Zmena hesla,  
Váš e-mail je napsán velmi zvláštním způsobem:  
Dáváte mi ultimátum na pouhé dva dny bez možnosti dalšího řešení  
Používáte značení pro ručení omezené  
Vyhrazujete si neznámá práva  
Předmět vašeho e-mailu obsahuje další vzkaz, který zní jako vyhrožování  
Vaše časové údaje postrádají přesnost  
Moje heslo na e-mail je automaticky vytvořené pro můj [REDACTED] účet  
Změnu hesla vyřizuje [REDACTED], které má na starosti komunikaci se studenty  
Odkaz na změnu hesla se neshoduje se stránkou pro změnu hesla na [REDACTED]  
+(https://[REDACTED])  
[REDACTED] nemá poštovní centrum nebo o něm nevím  
  
Na základě všech těchto údajů se domnívám, že Vaše žádost o změnu hesla je pokus o  
+napadení mého účtu. Vzhledem k tomu, že Váš odkaz směřuje na jinou stránku školy  
+se také domnívám, že jste zaměstnancem školy pověřeným testováním internetové  
+bezpečnosti studentů. Budu očekávat Vaši odpověď <poslední varování>. [REDACTED]
```



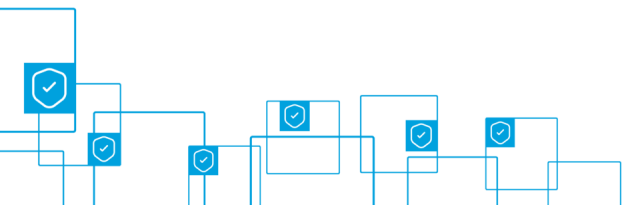
- Uživatel hledal původ zprávy v hlavičkách a certifikátech

```
Tento e-mail pochází ze serveru phishingator.cesnet.cz (IP 78.128.246.81) a  
+obsahuje hlavičku X-CESNET-Phishingator.  
Jde tedy o odeslání z nástroje Phishingator provozovaného CESNETem, zaslané přes  
+interní MTA [redacted].  
Doména v odkazech byla [redacted], která má v  
+minulosti a opakovaně platné certifikáty (Let's Encrypt / DigiCert), viz níže.  
Z mé analýzy to tedy vypadá na autorizovaný test / cvičný phishing, nikoli na  
+externí neautorizovaný útok.
```

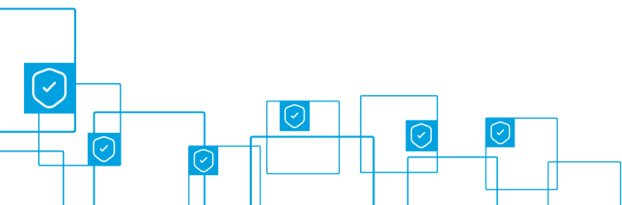


- Prověřování domény
 - Uživatel dohledal registrační údaje a poslal vlastní „varování“
- Návštěva nedorazila

```
contact: [redacted]  
name: [redacted]  
address: [redacted]  
address: [redacted]  
address: [redacted]  
address: CZ  
registrar: [redacted]  
created: [redacted]  
  
očekávejte návštěvu
```



- Zachycené zprávy
 - Odpovědi uživatelů i automatické zprávy o nepřítomnosti
 - Příjem zpráv pro všechny adresy v dané doméně
 - Doména slouží i jako malý honeypot pro sběr skutečného phishingu
- Překlepy v doméně příjemce e-mailu
 - Zpráva může dorazit na doménu registrovanou pro Phishingator
 - Záměna sousedních písmen na klávesnici, vynechání pomlčky, ...
- Zachycené odpovědi vám po kampani můžeme předat



Jak na phishingátorové kampaně

Co doporučujeme a co nedělat

- Začít jednodušším scénářem
 - Snazší e-mail a podvodná stránka
 - Dát uživatelům šanci podvod rozpoznat
 - Počítat s kritickými reakcemi
- Ukázat konkrétní indicie
 - Označené indicie v e-mailu
 - Chybné kódování stránky
- Postupně zvyšovat obtížnost
 - Vycházet ze skutečných phishingových e-mailů

ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Jednotné přihlášení
ke službám ZČU

???? ? ?????? Orion

Heslo

PŘIHLÁSIT

Zapomenuté heslo / Nápověda

CS EN

Službu jednotného přihlášení provozuje CIV.

Ocenit správnou reakci

Poděkovat za hlášení a povzbudit k zasílání dalších vzorků.

Kapacita týmu

Počítat s objemem hlášení. Zaměstnanci a studenti mohou reagovat odlišně.

Evidence hlášení

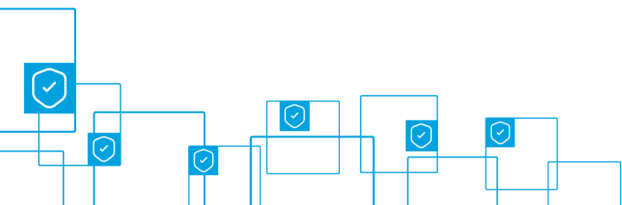
Záznam ve Phishingatoru nebo ticketovacím systému. Využít časovou osu kampaně.

Kam incident hlásit

Kontakt na vzdělávací stránce. Uživatel ví, co dělat při skutečném útoku.

	700	zadání neplatných údajů ohlášeno	4. 8. 2026 16:54:41			Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0
	700	návštěva stránky	4. 8. 2026 16:53:28			Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:153.0) Gecko/20100101 Firefox/153.0
	705	zadání platných údajů	4. 8. 2026 16:20:06			Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:153.0) Gecko/20100101 Firefox/153.0
	705	návštěva stránky	4. 8. 2026 16:19:33			Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:153.0) Gecko/20100101 Firefox/153.0
	713	návštěva stránky	4. 8. 2026 15:52:46			Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
	909	návštěva stránky ohlášeno	4. 8. 2026 15:36:17			Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr

- AI pro obsah i vzhled e-mailu
 - Například zpráva údajně od MKB organizace
 - Použití AI vysvětlit v indiciích
- Kampaně pravidelně opakovat
 - 2–4× ročně podle potřeb organizace
- Alternativa ke kurzu o phishingu v Moodle
 - Cvičný phishing jej může doplnit i nahradit
- NZKB: Povinnost školit uživatele
 - Phishing jako jedno z témat



Novinky ve Phishingatoru

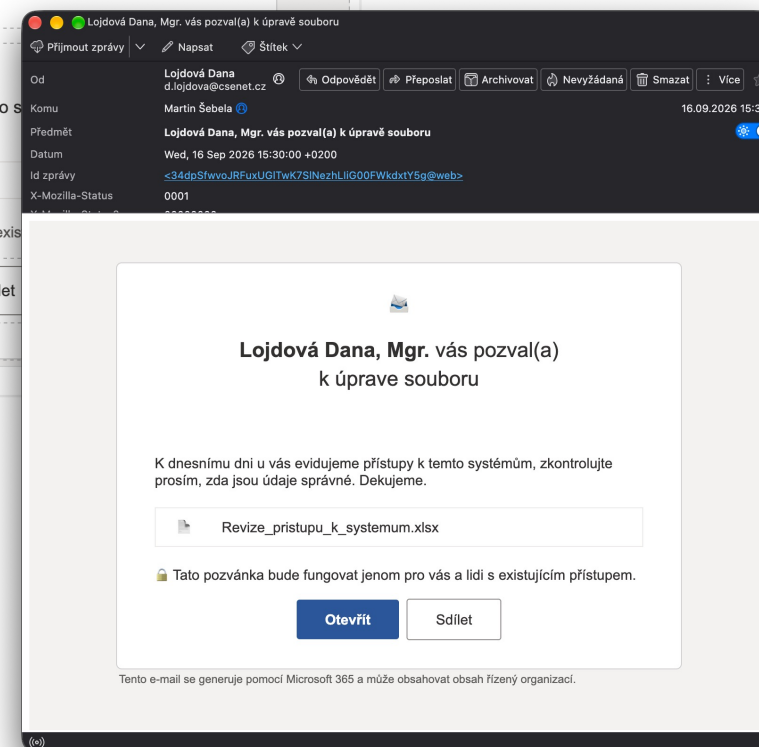
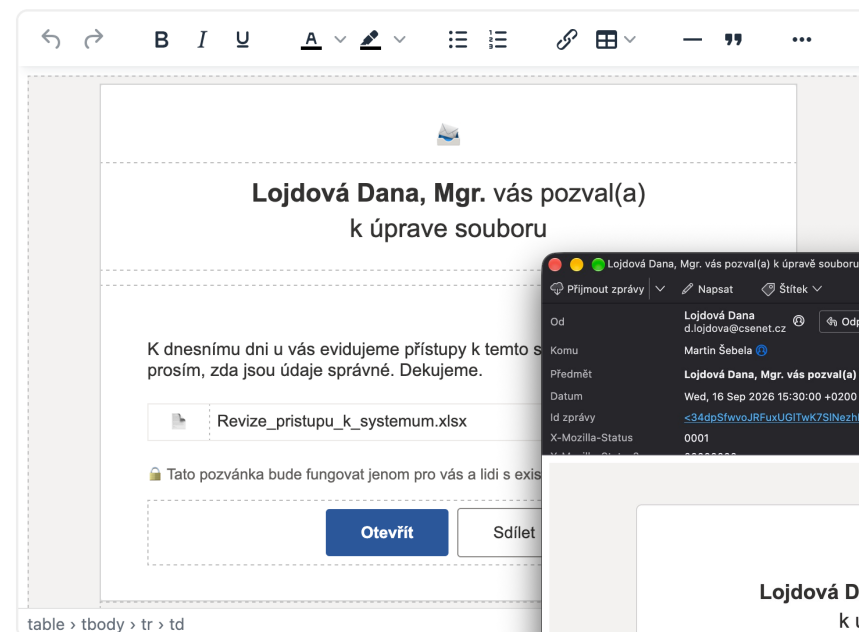
Nové funkcionality, vylepšení a opravy

- Editor TinyMCE
 - Vizuální úpravy i HTML kód
 - HTML, CSS, emoji
 - Našeptávání a zvýrazňování proměnných
- Původní HTML e-maily
 - Převedeny do editoru

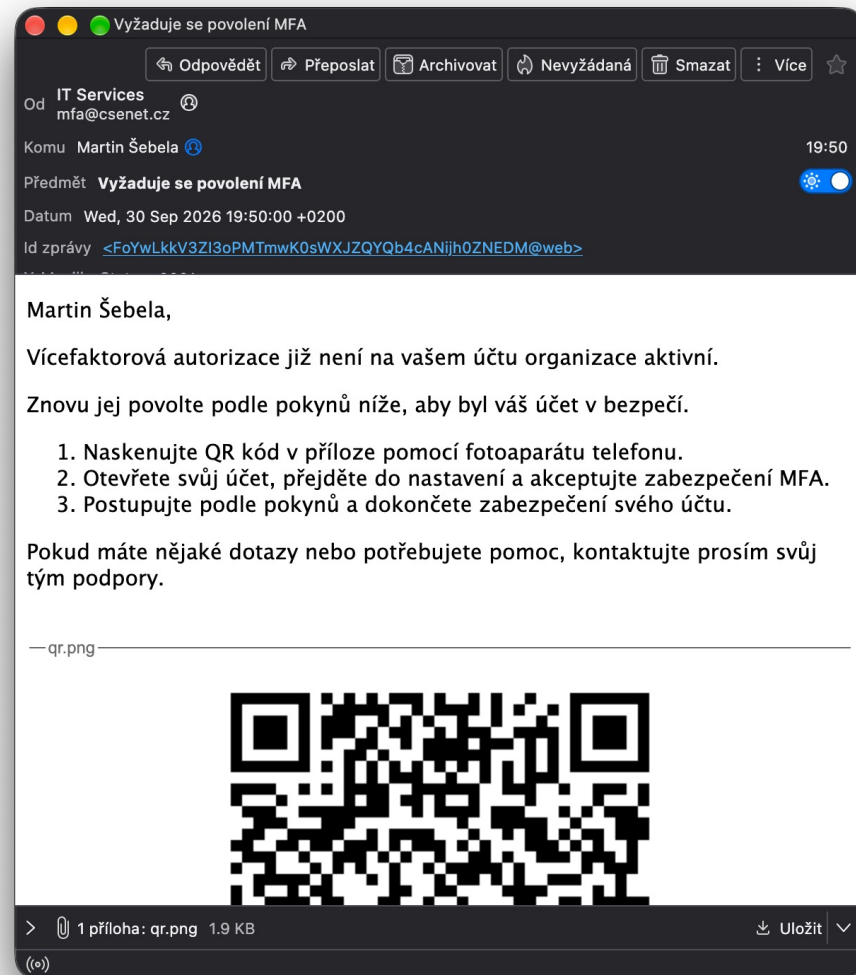
Předmět

Lojďová Dana, Mgr. vás pozval(a) k úpravě souboru

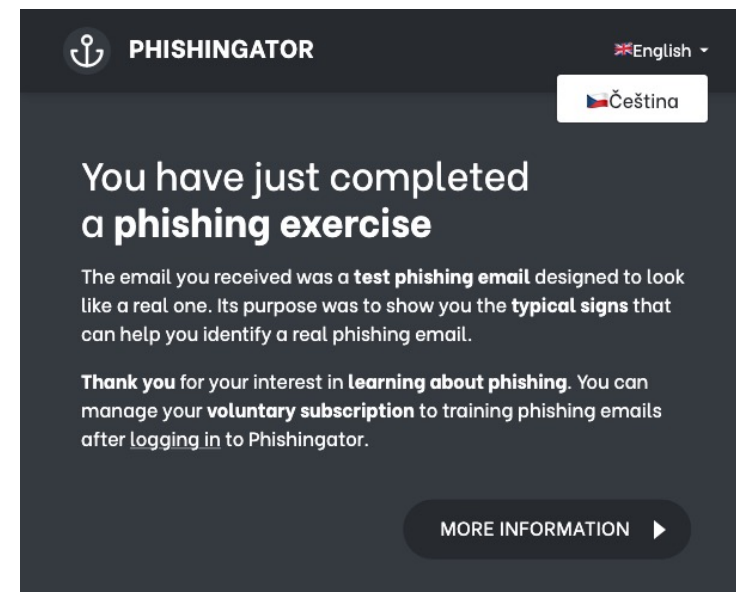
Tělo



- Quishing
 - QR kód součástí e-mailu
 - Skrytí podvodné URL adresy do QR kódu
 - Cílení na mobilní zařízení
 - Například výzva k nastavení MFA
- Možné přidat do textového i HTML e-mailu



- Vylepšené indicie
 - Přidání obecné indicie k celé zprávě
 - Delší texty a možnost odstavců
- Anglická vzdělávací stránka
 - Jazyk podle nastavení zařízení i prohlížeče s možností přepnutí
 - Anglické notifikace pro uživatele
 - Zákaznické texty přeloženy



- ☒ Odeslat příjemcům notifikaci po ukončení kampaně

Notifikace obsahuje informaci o absolvování cvičného phishingu a odkaz na vzdělávací stránku s indiciemi.

Jazyk notifikace

- ☒ Čeština ☐ Angličtina

- **Ověřování zadaných údajů**
 - Nově vůči více metodám
 - Podpora M365
- **Rychlý přehled kampaně**
 - Úvodní statistika a aktuální stav kampaně
- **Přehlednější časová osa**
 - Možnost zvýraznění aktivity konkrétního uživatele
- **Lepší exporty**
 - Grafy ve vyšším rozlišení
 - Záznam o návštěvě vzdělávací stránky
 - Možnost exportu kompromitovaných identit

Aktivní od ↓	Aktivní do ↓	Stav ↓
1. 10. 2026 10:00	3. 10. 2026 23:59	čeká na zahájení
30. 9. 2026 19:50	2. 10. 2026 12:00	probíhá
21. 9. 2026 10:00	30. 9. 2026 23:00	dnes končí
10. 4. 2026 16:35	10. 4. 2026 23:59	ukončena

↓ Export dat

Grafy

Reakce uživatelůPNG

Reakce uživatelů dle odděleníPNG

Všechny provedené akcePNG

Data

Reakce uživatelůCSV

Akce na podvodné stránceCSV

Kompromitované účtyCSV

Počet akcí každého uživateleCSV

Všechna data v archivuZIP

Spolehlivý provoz a zabezpečení

Údržba, aktualizace,
nasazování

Optimalizace, lepší
zabezpečení

Průběžné opravy
chyb

Přizpůsobení zákazníkům

Nové šablony
podvodných stránek

Aktualizace seznamů
uživatelů

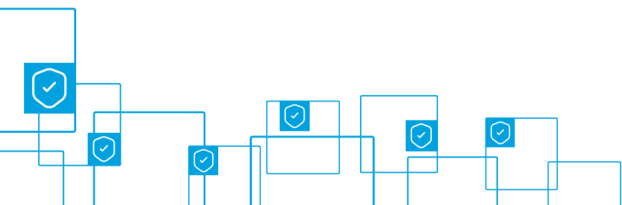
Úpravy vzdělávací
stránky

Technické zázemí

Vývoj interních nástrojů

Podpora různých VPN
připojení

Správa registrovaných
domén



Co chystáme?

Další směry rozvoje

- Smishing
 - = phishing přes SMS
 - Cvičné SMS s odkazem na podvodnou stránku
 - Zdroj dat z LDAP/AD/CSV
- Další komunikační kanály
 - Například WhatsApp
- Ověření poskytnutí druhého faktoru
 - TOTP jako další sbíraný údaj
 - Passkeys

 Kampaně Podvodné e-mailý Podvodné SMS Podvodné stránky

Hello Radomír Orkáč, 🖐️

We're contacting you on behalf of...

During our standard pre-arrival check, we found a detail that needs to be updated. This is valid from 29.09.2026 to 01.10.2026.

Please take a moment to look at the details so we can complete your visit.

You can finish the review here:

<https://travel.guest-arrival-stay.com/135050616090>

21:08

5G 80%

< es výběru pokuty... ení je následující:  +212 7 84 98 14 07 >

Systém automaticky vytvoří spis a předloží jej za prodlení ve výši 8,93 % denně, dokud nebude uhrazena celá dlužná částka.

Po 30 dnech od prodlení systém automaticky vytvoří spis a předloží jej příslušnému místnímu soudu.

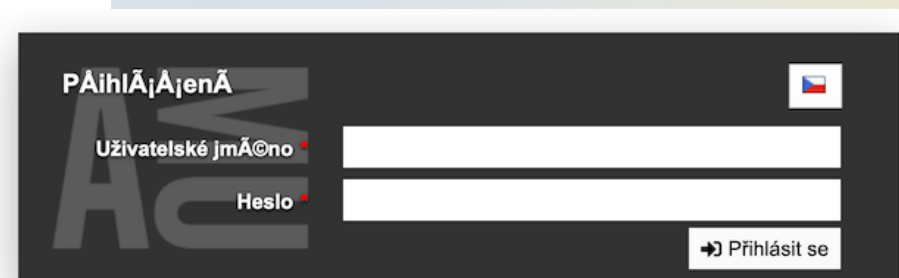
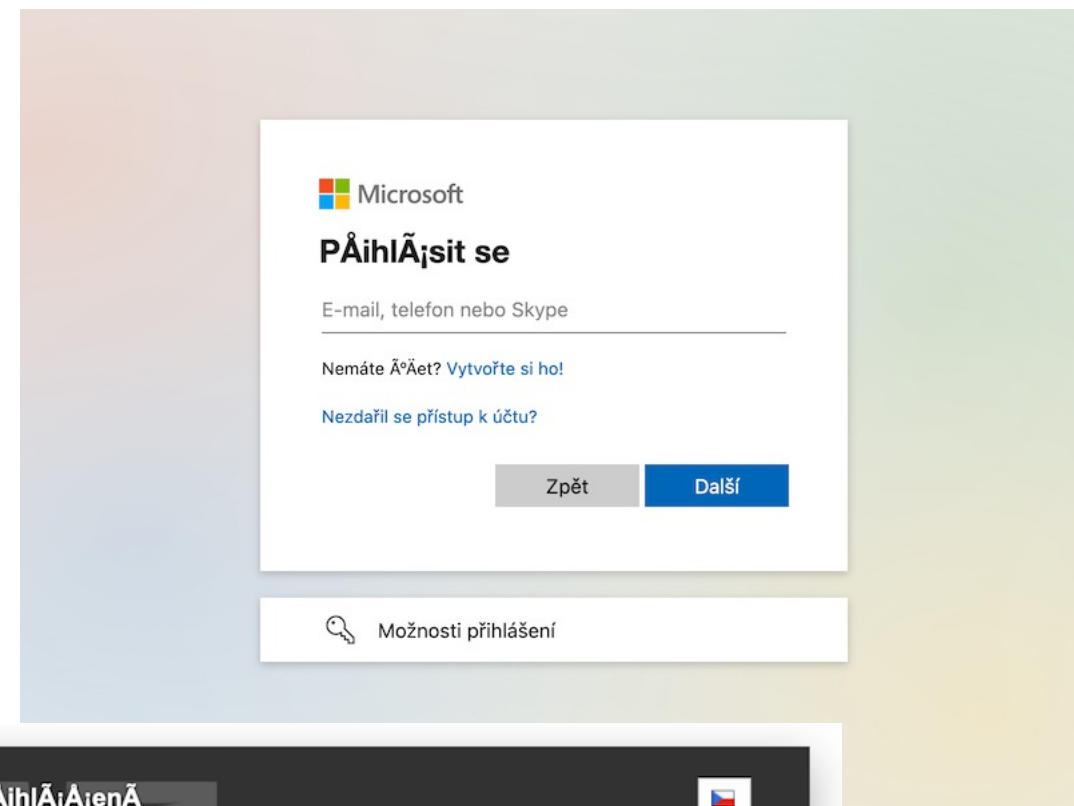
Po předložení případu soudu systém automaticky vydá bance příkaz k zablokování a denně strhává odpovídající částku z vašeho účtu.

Tato opožděná registrace bude zaznamenána v systému úvěrových informací a může ovlivnit registraci vaší společnosti, podepsání smlouvy a žádosti o veřejné služby v České republice. Prosíme, plně si uvědomte výše uvedená právní rizika a nepodstupujte žádná rizika. V současné době stačí zaplatit pouze částku pokuty.

Oficiální platební kanál:
<https://policoiiee.cc/cz>

Odešlete „1“ a znovu otevřete SMS zprávu pro zobrazení původní pokuty za překročení rychlosti a mapy místa přestupku.

- Simulace chybného kódování podvodných stránek
 - V nastavení stránky
- Přístup k odpovědím na cvičné phishingové zprávy
- Podvodná stránka jako HTML příloha
 - Scénáře s obsahem ukrytým v JavaScriptu; s přesměrováním
 - Faktura.pdf.html



Zkušenost pro uživatele

Pravidelný phishing nanečisto s vysvětlením varovných signálů

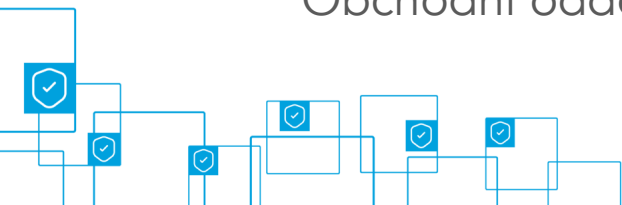
Zpětná vazba pro organizaci

Přehled reakcí uživatelů a posouzení připravenosti na phishing

Zájem o Phishingator

phishingator@cesnet.cz

Obchodní oddělení CESNET



Dotazy

Martin Šebela

CESNET FLAB

Oddělení kybernetické bezpečnosti

Konference e-infrastruktury CESNET 2026

Phishingator Workshop 2026