BOIT

Linux Days 2025

VZDĚLÁVÁNÍ V KYBER
CO FUNGUJE, CO JE BULLSHIT?

Přednáška, která nebude nudná.
Snad.

TLP:GREEN

Whoami

PAVEL SPAJK MATĚJÍČEK

CEH, C|OSINT a další, 16 let v cybersecu, exESET

I use Fedora bdw...

Drony, 3D tisk, foto, kempig, gym, Nintendo

V BOITu školíme lidi, děláme moderní phishtesty, fyzickej red-teaming a pentesty webových appek a on-prem prostředí.

KONTAKTY

BOIT.CZ

TLP:GREEN

BOIT

Víte co je hustý? Že jsme tu už přes hodinu a ještě nepadly dvě slova, který nesmí chybět na žádný konferenci...

AI a NIS2

NZKB A VZDĚLÁVÁNÍ

§ 11 Bezpečnost lidských zdrojů

Konkrétní opatření, která přímo souvisejí se školením a povědomím zaměstnanců (security awareness), jsou zahrnuta pod hlavičkou **Bezpečnost lidských zdrojů**.

- Školení musí být **pravidelná** a **evidence** jejich absolvování je **povinná součást** bezpečnostní **dokumentace**.
- Pro **vrcholové vedení** platí povinnost seznamovat se s klíčovými **bezpečnostními dokumenty a absolvovat školení**, což je podmínka pro obhajitelnost jejich rozhodnutí vůči regulátorovi a auditorům.
  Zajistí pravidelná školení **a ověřování bezpečnostního povědomí zaměstnanců** v souladu s jejich pracovní náplní...

DOPORUČENÁ TÉMATA
PRO ROZVOJ BEZPEČNOSTNÍHO POVĚDOMÍ

a) Techniky zabezpečení zařízení.
b) Firewall, antivirový program a jejich omezení.
c) Škodlivé programy a jejich projevy.
d) Rizika stahování programů a aplikací.
e) Aktualizace softwaru.
f) Rizika povolení/zakázání spouštění maker.
g) Rizika spustitelných souborů.
h) Zásady zabezpečení uživatelských účtů.
i) Používání, tvorba a správa hesel.
j) Vícefaktorová autentizace.
k) Techniky sociálního inženýrství.
l) Online identita, digitální stopa a její minimalizace.
m) Zásady práce v počítačové síti.
n) Používání vzdáleného připojení (VPN).
o) Bezpečná elektronická komunikace.
p) Bezpečnost webových stránek.
q) Zálohování, ukládání a šifrování dat.
q) Zálohování, ukládání a šifrování dat.
r) Bezpečné používání přenosných technických nosičů dat.
s) Využívání cloudových úložišť.
t) Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti.
u) Základní postup reakce na kybernetickou bezpečnostní událost nebo incident.
v) Zásady bezpečného používání pracovních zařízení pro soukromé účely.
w) Zásady bezpečného používání soukromých zařízení pro pracovní účely (tzv. BYOD).
64
x) Osobní odpovědnost zaměstnance při dodržování zásad kybernetické bezpečnosti.
y) Aktuální hrozby v kybernetické bezpečnosti.

Z) chybí. My přidáváme AI a její secure použití.

TLP:GREEN

BOIT

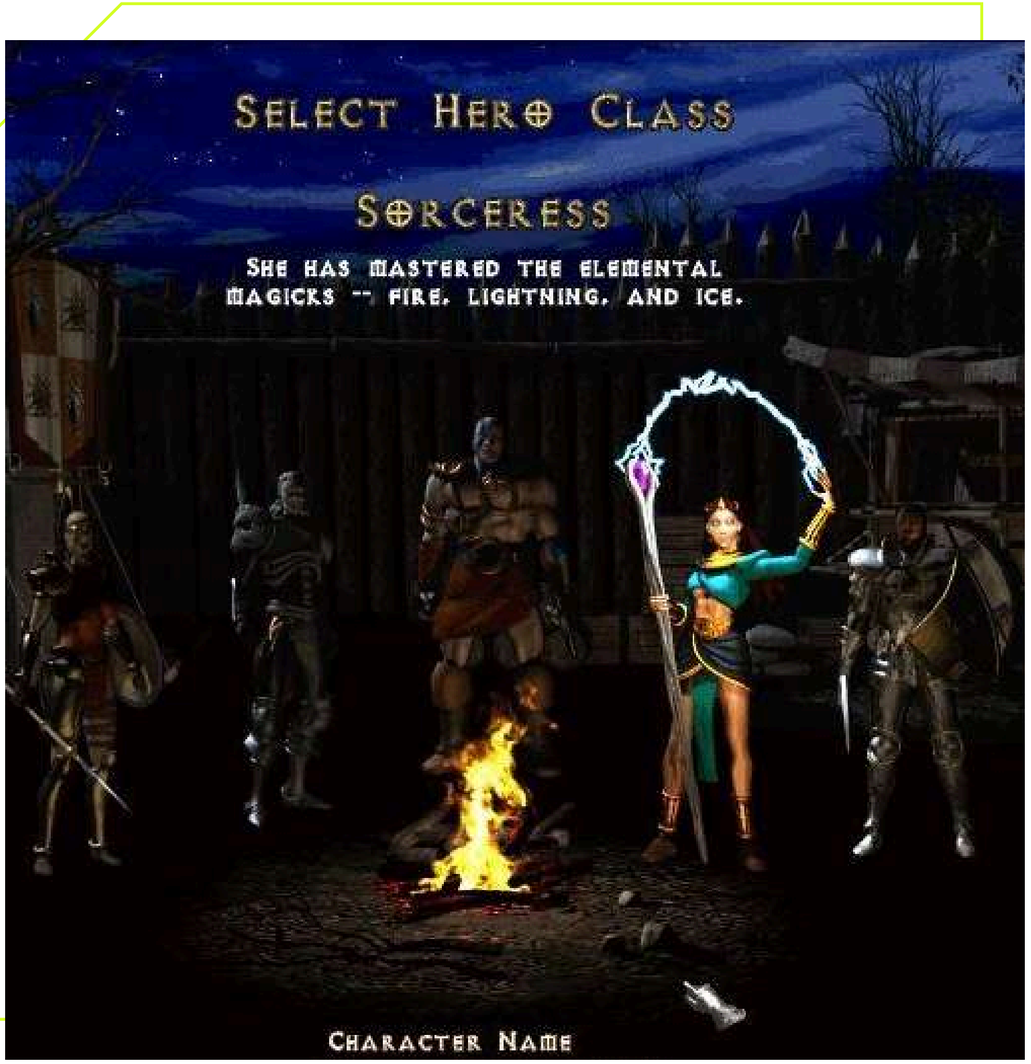
🎯 Můj a náš cíl

VYTVOŘIT OSVĚTU

která:

- mění chování lidí,
- dává smysl pro všechny role,
- je měřitelná,
- a přináší konkrétní výsledky

Jsme **BOIT** Cyber Security. Náš rozdíl oproti konkurenci? **Neděláme školení pro školení.** Každá lekce má přesah do osobního života, protože víme, že když to lidi pochopí doma, použijí to i v práci.



🎯 Můj cíl

ROZDĚLENÍ OBSAHU PODLE ROLÍ (RPG)

Každý slide nebo sekce přednášky se přirozeně dotýká všech ~~tří~~ čtyř perspektiv. Níže je struktura, jak jsem to celé propojil do konceptu, který reflektuje:

- 👤 Zaměstnance (účastníka školení)
- 👨‍🏫 Lektora / tvůrce školení
- 🏛️ Management / HR / decision-makery

New game +

- 🐧 Admin

🎯 Zformulujte vlastní očekávání.

ÚVOD A OČEKÁVÁNÍ

Role a co čekají

👤 **Uživatel**

Chci rady do praxe, nástroje, žádný kecy a domu

👩‍🏫 **Lektor**

Chci zaujmout, něco předat, neuspávat

🏛️ **Management**

Chci výsledky, měření, dopad = ROI

🐧 **Admin**

Chci míň false negative a bezpečnostních incidentů od Růženy a Franty

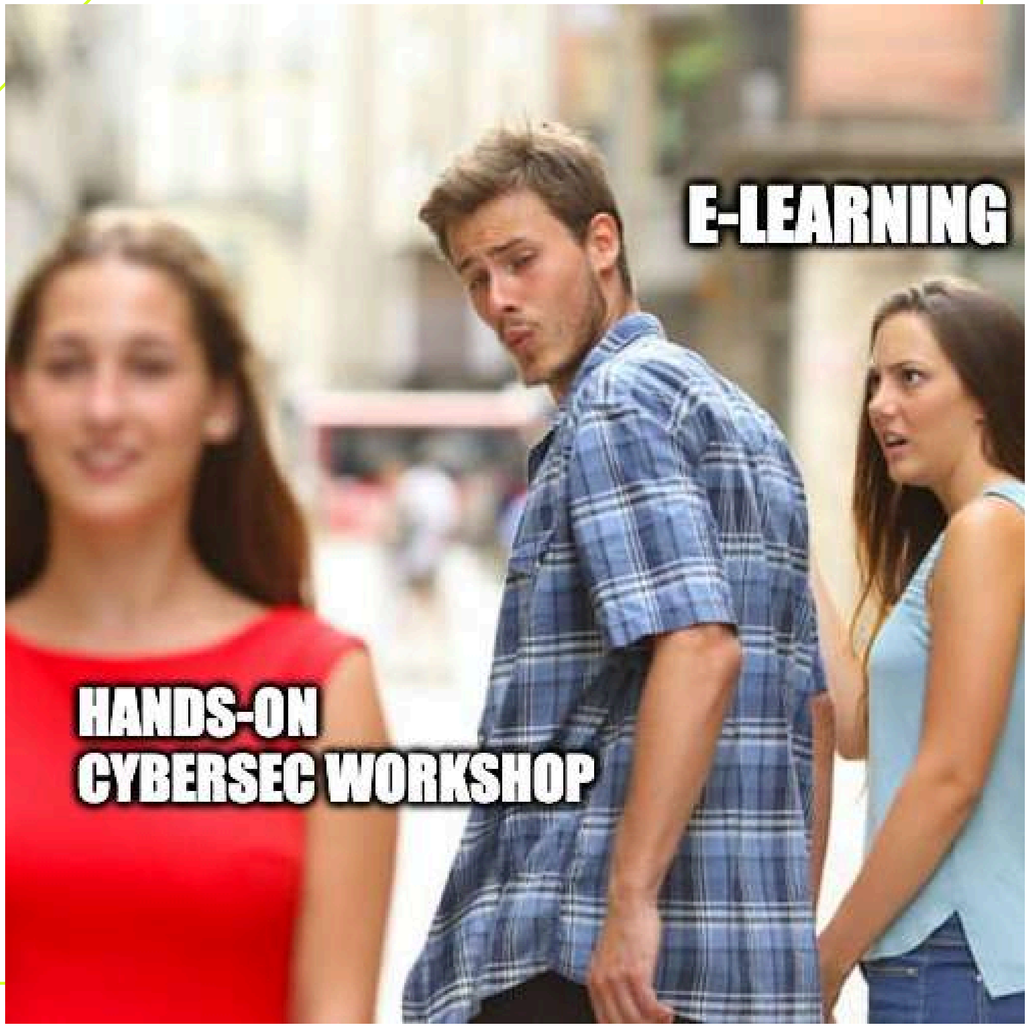
CO DĚLÁ ŠKOLENÍ

(ne)funkční

🎯 Diskutujme. Potom u kafe.

PROBLÉMY KLASICKÝCH E-LEARNINGŮ

✅ Nerelevantní obsah – mluví o věcech, které běžný zaměstnanec nikdy nezažije (SQL injection, místo toho jak poznat podvodný e-mail).
✅ Nuda a pasivita – jen klikání „Další“ a test na konci.
✅ Jednorázová akce – 1× ročně, bez návaznosti, vše se zapomene.
✅ Žádná zpětná vazba – nikdo neřekne, jestli jsem to pochopil dobře, nebo ne.
✅ Žádné měření dopadu – management má jen seznam „kdo odklikl“, ale neví, jestli se lidi chovají jinak.



🎯 Diskutujme.

PROBLÉMY KLASICKÝCH E-LEARNINGŮ

👤 Uživatel | Odkliknu → Zapomenu

👩‍🏫 Lektor | Nudný obsah, bez kontextu, musí se udržovat

🏛️ Management | Splněno pro audit, ale nula dopadu

🐧 Admin | Umí to SSO, nebo zas budu resetovat hesla? Kde to poběží? Na čem? Na koho padne maintenance? A co na to Jan Tleskač?

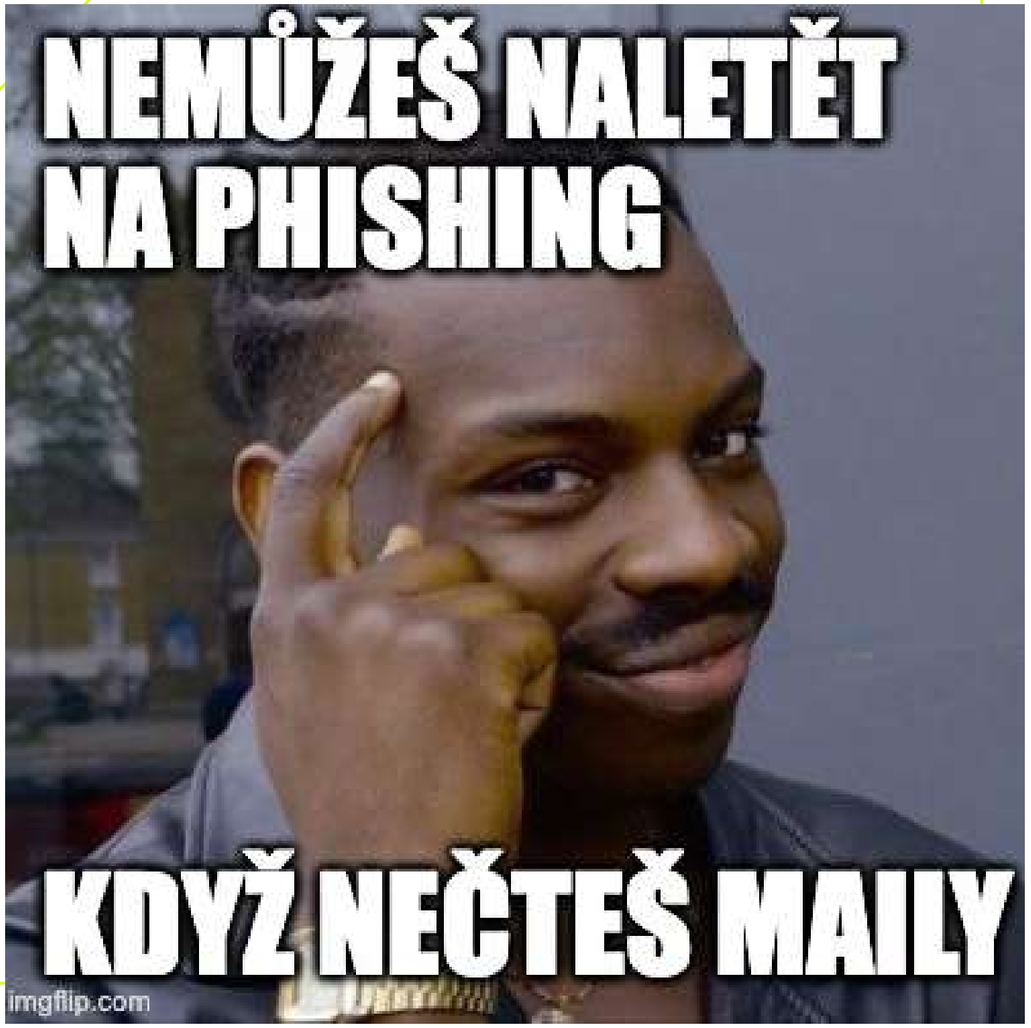
🎯 Diskutujme. Po přednášce.

VÝHODY KLASICKÝCH E-LEARNINGŮ

Lze integrovat do inhouse systémů a navázat do procesů

Jsou z něj data

Jak jinak byste měřitelně proškolili 13k+ zaměstnanců?



🎯 Diskutujme.

BEHAVIORÁLNÍ MODEL B=MAP (FOGG BEHAVIOR MODEL)

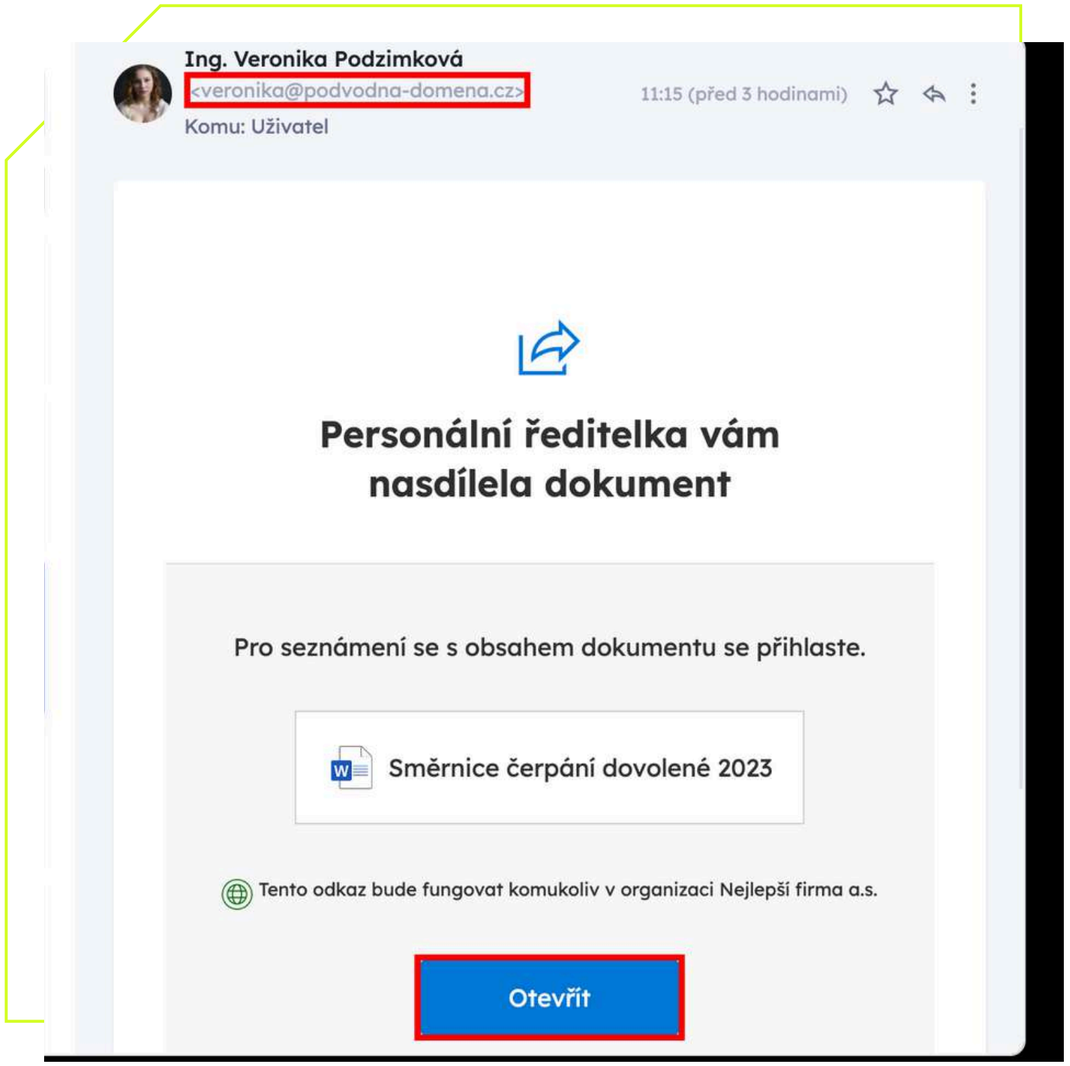
Stanfordský psycholog B.J. Fogg popsal, že změna chování (Behavior) nastane, jen když se sejdou tři prvky najednou:

M = Motivation (**motivace**) - **proč** by to měl dělat, co z toho má.
A = Ability (**schopnost**) - jestli je to pro něj snadné a **zvládnutelné**.
P = Prompt (**spouštěč**) - co ho v tu chvíli k akci „šťouchne“
(např. vidí podezřelý mail → **má v hlavě** tip ze školení → **klikne** na „Report phishing“).

Pokud uživatel ví co dělat, rozumí proč je to důležité a má jasné tlačítko v Outlooku „Nahlásit phishing“ → jeho **chování se** opravdu **změní**.

§ 11, odstavec 3, písmeno c)

hodnotí účinnost plánu **rozvoje bezpečnostního povědomí**, provedených poučení, školení a dalších činností spojených se zlepšováním bezpečnostního povědomí...



Phishtest - Icebreak & diagnostika

JAK UDĚLAT PHISH V RÁMCI AWARNESS

- vlastní zdroje
- on-line matroš : https://boit.space/53rd9
- interně (baiting,QR,SMS,e-mail)
- externě - TOP

👤 Uživatel | Wow, tohle bych nepoznal!
👨‍🏫 Lektor | Takhle zaujmu hned od začátku
🏛️ Management | První metrika → kolik lidí klikne / nahlásí
🐧 Admin | Nastavim výjimky a jsem zvědavej jak to dopadne, mám podklad komu cutnout práva, trénink dělá mistry

POHLED NA ŠKOLENÍ

ze 3 úhlů

TLP : GREEN

ÚČASTNICTVO - EMPATICKÝ DESIGN

PRAKTICKÝ POHLED ÚČASTNÍKA

👤 Z pohledu zaměstnance - co chce

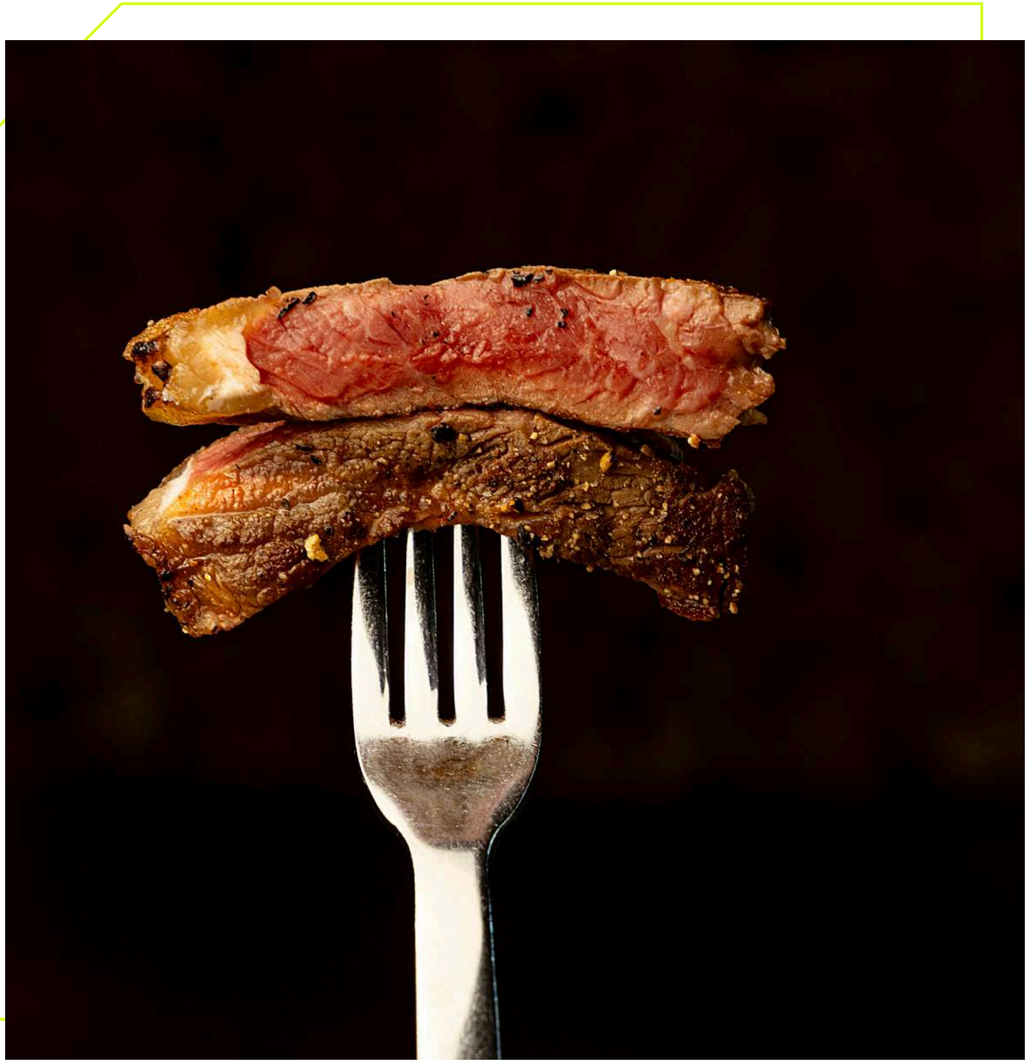
- Praktické rady a konkrétní scénáře
- Interaktivita: testy, gamifikace, sdílení zkušeností, bejt chytrej a přispět
- Tooly, návody, refreshe
- Bez ostudy - chyby jsou součást procesu

PERSPEKTIVA LEKTORA

TVORBA ŠKOLENÍ - LEKTOR

👨‍🏫 Pohled lektora

- Personalizace podle rolí a situací
- Fakt nechci točit furt to samý
- Propojení s firemními reáliemi
- Gamifikace, pravidelné microlearningy
- Měření dopadu, ne jen „spokojenosti“
- Budget a timing

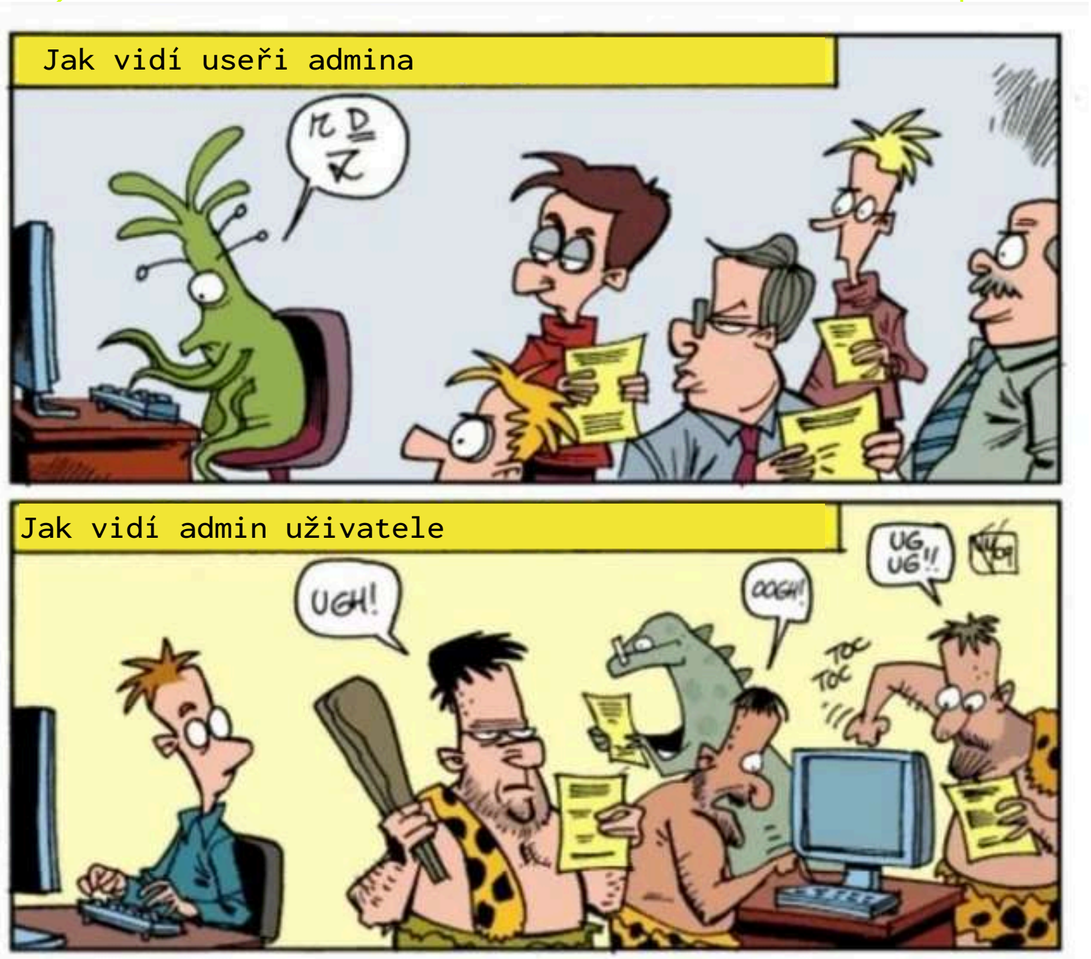


PERSPEKTIVA MANAGEMENTU

ROZHODOVACÍ HRA: CO A KDO KOUPÍ

🏛️ Pohled managementu/HR):

- Chci výsledky, ne jen razítko
- Potřebuji školení pro všechny, ne jen IT
- Nechci střídat dodavatele
- Hledám měřitelnost, přínos, plán follow-upu



Případná podobnost s vaší firmou je čistě náhodná ;)

PERSPEKTIVA roota

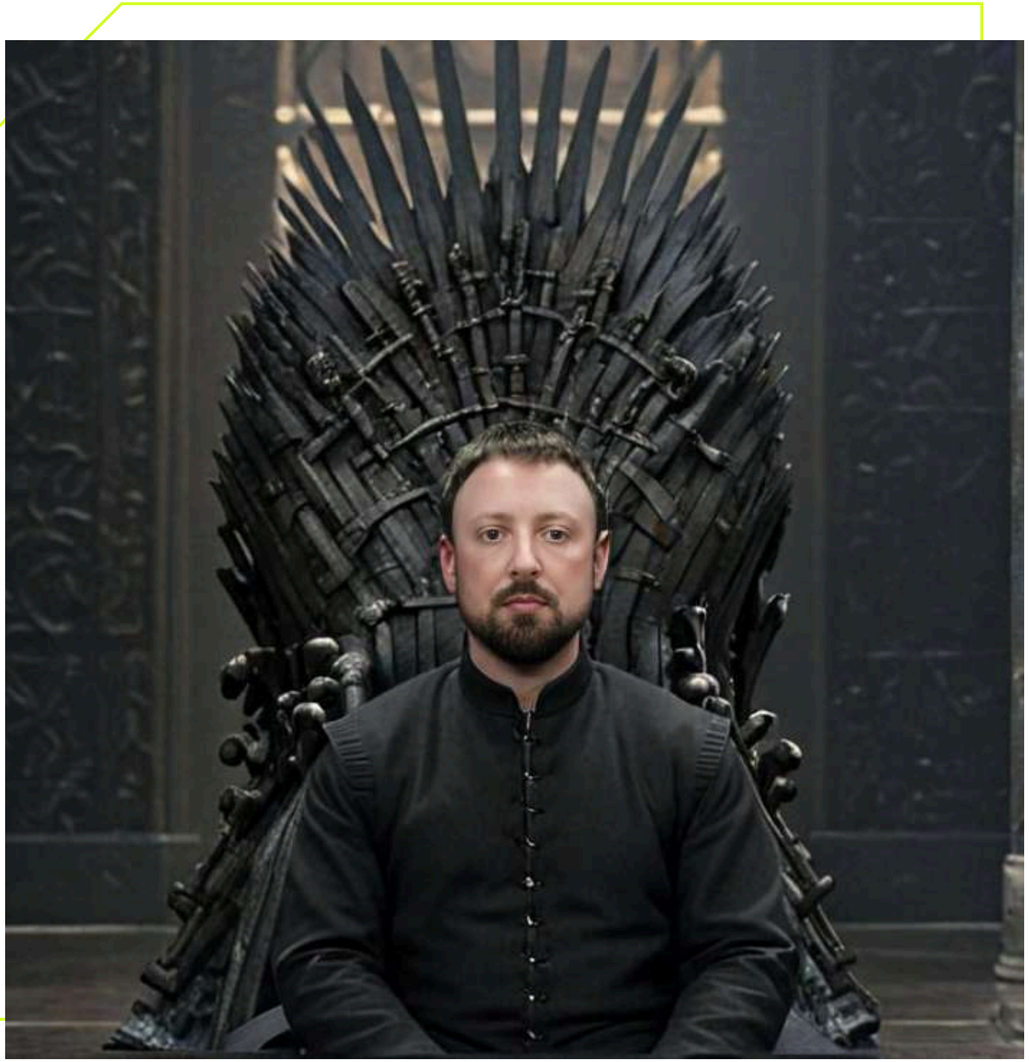
CO SI MYSLÍ ADMIN

🐧 Pohled admina:

- Tvl, snad už potrénujou a já tam nebudu muset furt lítat
- Míň krizí a fuckupů (rychlejší incident handlingů)
- Ještě že je nemusim školit já
- Mám levnej lidskej firewall, další vrstva ochrany
- Lidi ví co a kam hlásit - sice sem to já, ale aspoň konečně vim co prováděj

HANDS-ON

live pohled za oponu



Hands-on ukázky

LIDI CHTĚJÍ TOOLY A BEJT HACKER

👤 Uživatel | Zajímavé, chci to zkusit doma
👨‍🏫 Lektor | Super forma gamifikace / wow efekt
🏛️ Management | Zážitek → dopad → sdílení
🐧 Admin | Zvýšení povědomí, jinej úhel pohledu

🎯 **Ukázky & aktivity:**

- Vygenerování deepfake
- Detekce deepfake
- TheySeeYourPhotos
- Překlad DeepL

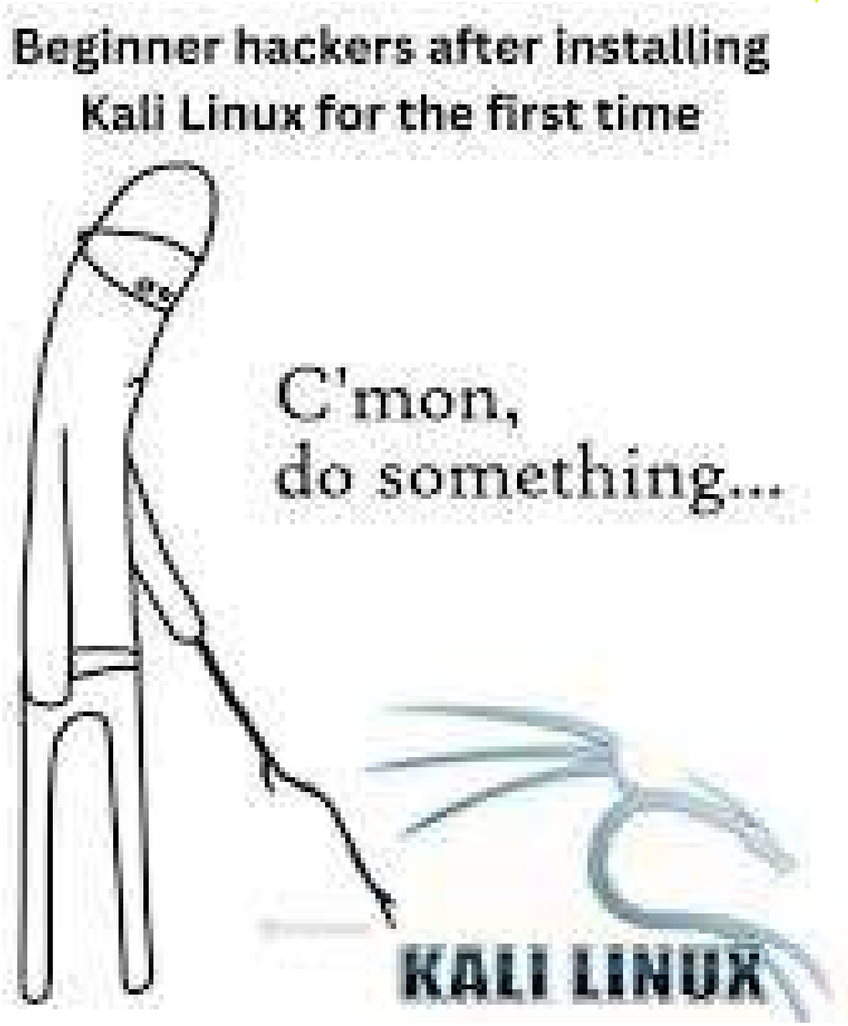
4 hustý tooly, nechat je, ať si to zkusí sami s vámi, jakožto průvodcem

TLP:GREEN

DEJTE JIM TY TOOLY

pro který si přišli

TLP : GREEN



Toolbox pro zaměstnance

OD LEKTORA I OD FIRMY

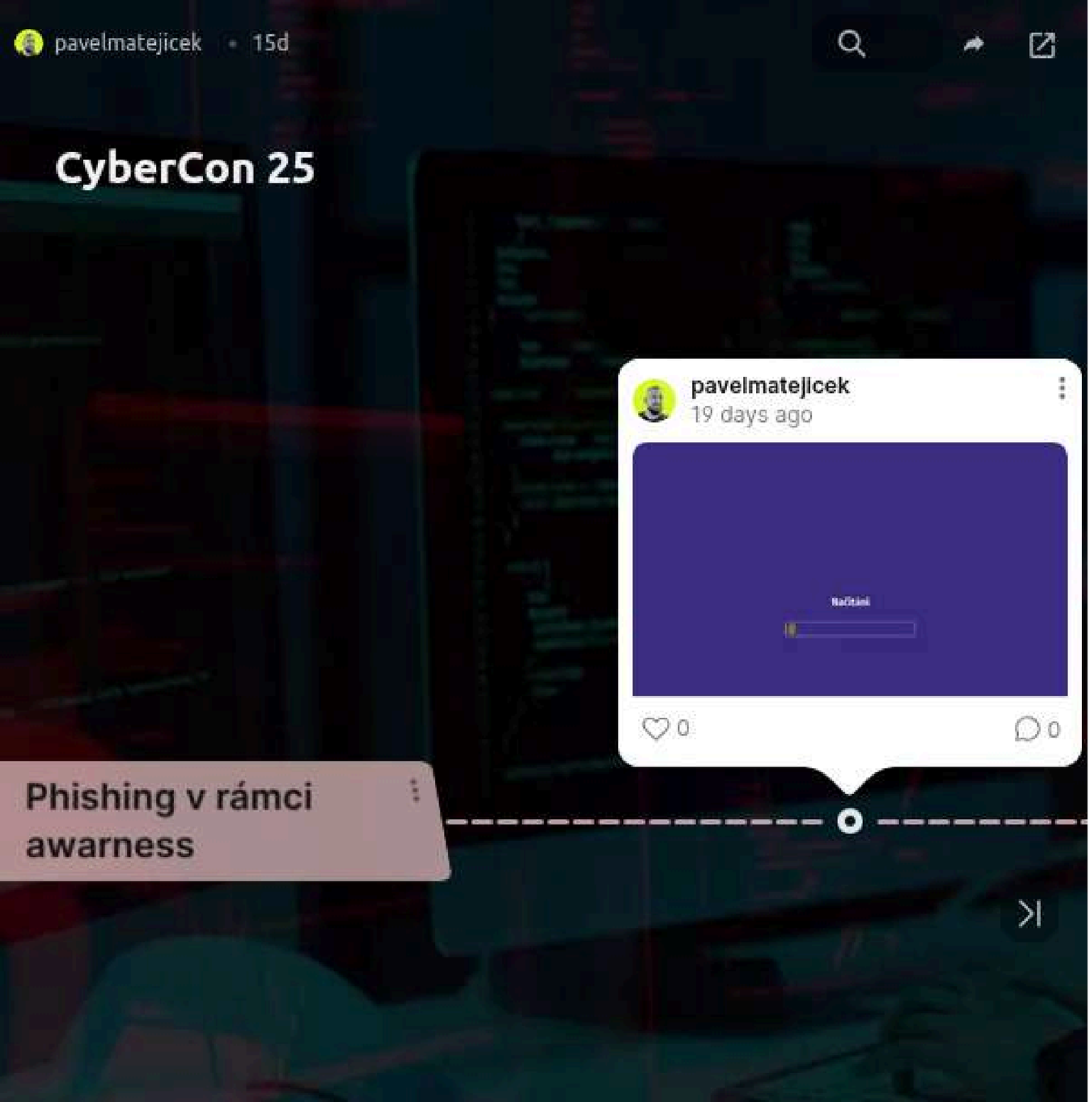
Forma: PDF, microsite, Confluence stránka, QR kód na wiki, Screen Saver, plakáty, comix.

➡️ Z pohledu uživatele: mám konkrétní nástroje, které mi pomůžou.

➡️ Z pohledu lektora: dávám lidem hmatatelný výstup, který prodlužuje efekt školení.

➡️ Z pohledu managementu: vidí, že školení má výstupy, které se dají znovu použít a podporují kulturu bezpečnosti.

TLP: GREEN

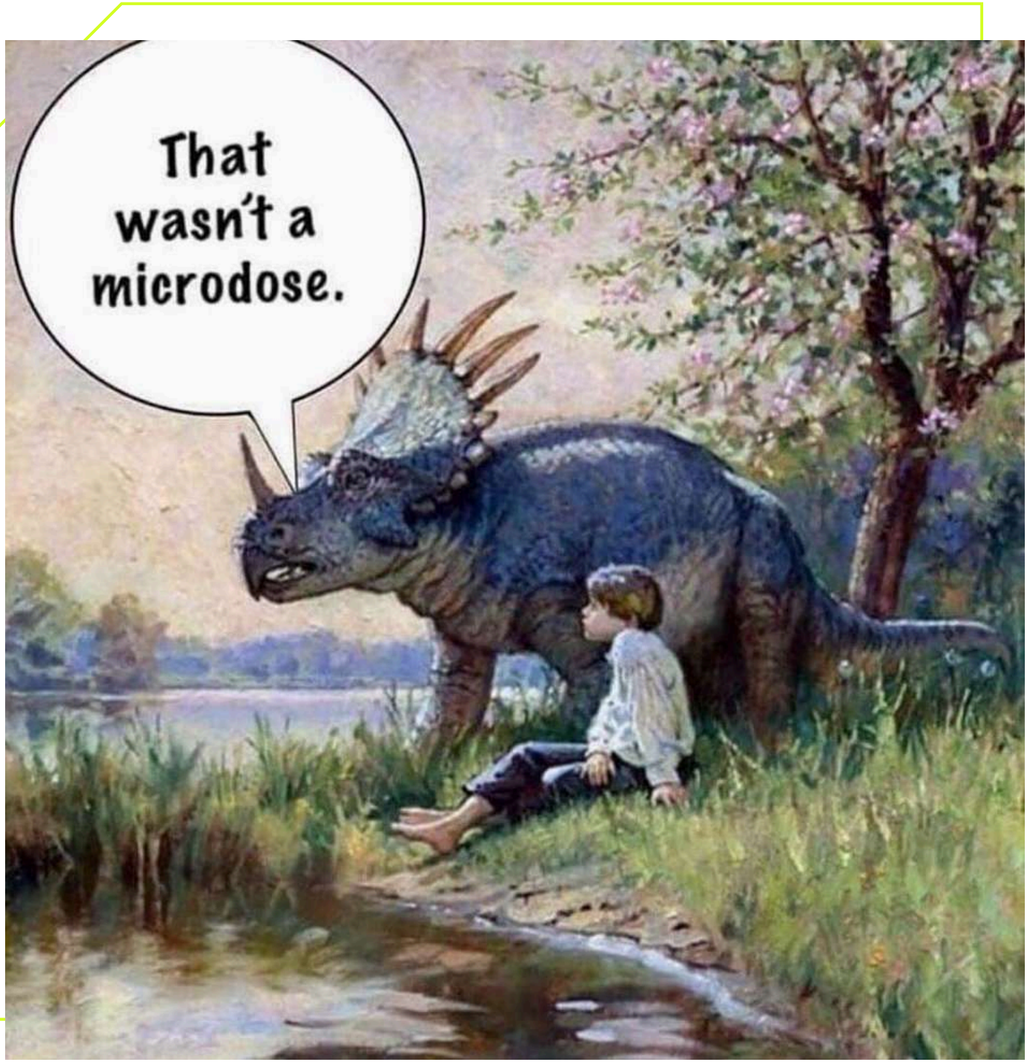


PADLET - NÁSTĚNKA

nebo cokoliv jiného

JDEME DO FINÁLE

tak poslyšte vážení



Z pohladu managementu a lektora

MĚŘENÍ DOPADU OSVĚTY

Nestačí, že někdo prošel kurzem → potřebujeme vědět, jestli se lidi opravdu chovají jinak. Fogg, BMAP (změna chování), pamatujeme?

Typické metriky:

- openrate, clickrate < **nahlášení** při phishing testech,
- čekujte trendy ve výsledcích kvízů, co lidi ba, co nedávaj
- feedback účastníků,
- počet a kvalita hlášených incidentů,
- engagement (kolik lidí si stáhlo / použilo toolbox).

Z pohladu všech

MĚŘENÍ DOPADU OSVĚTY

👤 **Uživatel**: vnímám, že se mnou někdo počítá - moje reakce se měří a vyhodnocuje, nejsem jen „checkbox“,

👨‍🏫 **Lektor**: mám data, kterými ukážu managementu hodnotu práce.

🏛️ **Management**: mám čísla, grafy, trendy → vidím ROI a můžu školení obhájit.

🐧 **Admin**: snížil se počet incidentů a false hlášení, mám víc času na svojí práci a nezdržují mě banality

Měření je most mezi zážitkem a business dopadem - aby to nebylo jen „fajn školení“, ale i data pro rozhodování a pokračování.

Škola hrou

OD KARET PO VR

Je toho ranec, takže zmíním jen:

- Clashing
- Odpal hackera, Cyber knights, NePINdej
- The Inside Man (seriál)
- Company (Un)Hacked

Víc na nástěnce:
https://padlet.com/pavelmatejicek/security-n-st-nka-nejen-ke-kolen-m-3dlmvuv2jzahkvd5

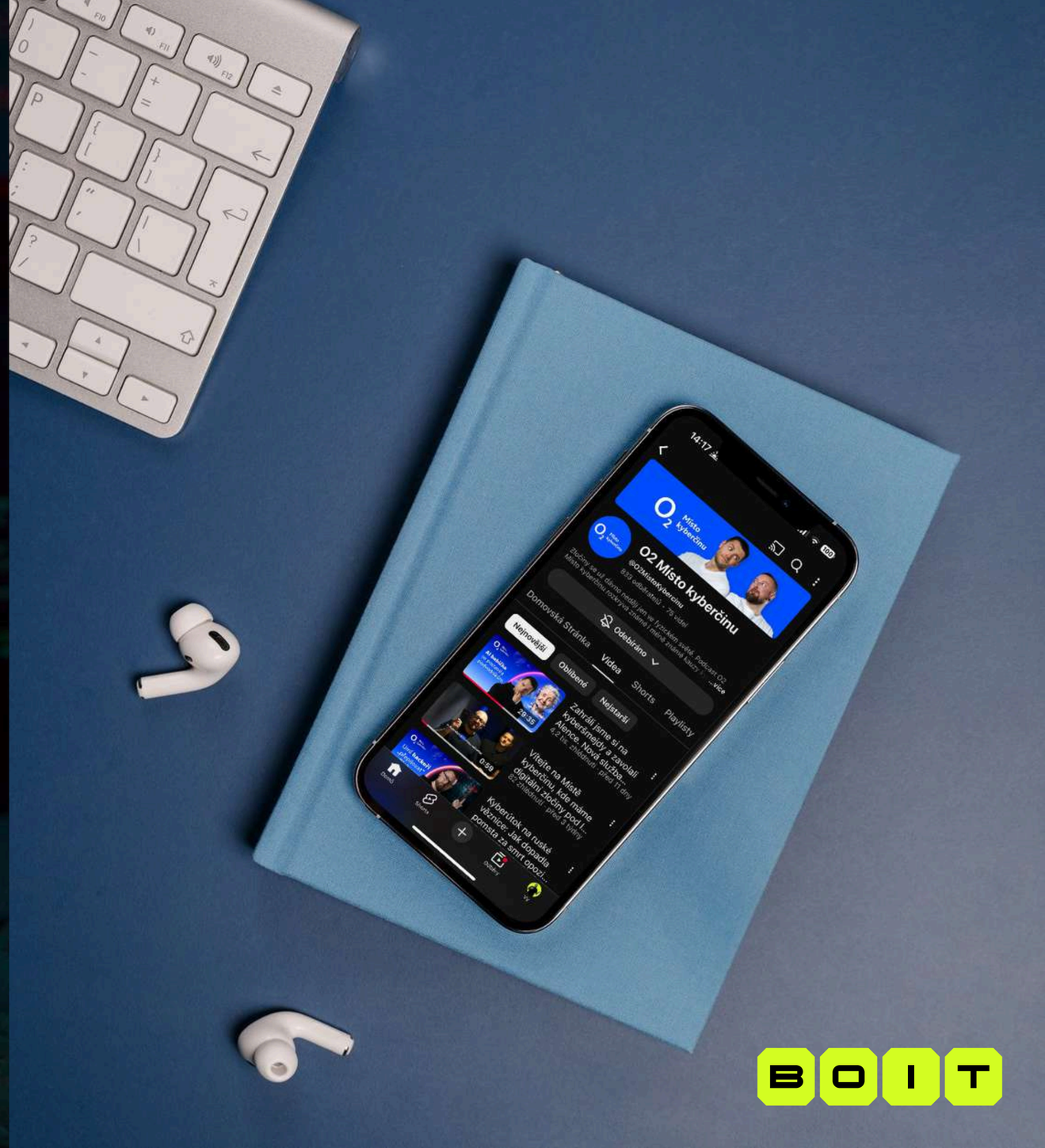
NEPROPADEJTE PANICE!

mám pro vás příručku, ať víte, co teď dělat

TLP : GREEN

BOIT

Podcast
“Místo kyberčinu”



TLP : GREEN

Link

TLP : GREEN

CO UDĚLEJTE NAHNED

Nestojí to nic a skočíte o pár levelů

- Správce hesel
- Zálohovaný MFA
- Updaty na všem
- Dejte odběr, like a zvoneček ;)

Kontaktní informace

Pavel Matějíček

ten týpek co školil

pavel.matejicek@boit.cz

https://boit.cz

TLP:GREEN