



www.igalileo.cz

Bezpečnost a AI

START 09:05



Na každé informaci záleží

Na úvod něco o nás



Václav Hlaváč



Adam Sládek

Proč je důležitá bezpečnost?

Bezpečnost je základní podmínkou fungování obce, školy i organizace



Na každé informaci záleží

Deepfake jako hlavní hrozba

AI posouvá možnosti v tvorbě podvodného obsahu



Na každé informaci záleží

Deepfake (podvodná) videa

Ověřujte informace, které sledujete.
AI výrazně usnadňuje šíření
podvodného obsahu.



Deepfake (podvodná) videa

Deepfake video může vypadat jako starosta/ředitel/policie apod.



Ukázka podvodného videa



Zdroj: https://tv.idnes.cz/domaci/podvodna-video-babis-benes.V240130_095709_idnestv_heli



Na každé informaci záleží

Žena uvěřila a poslala celkem 525 000 Kč



Policie České republiky – KŘP Olomouckého kraje

„Deepfake video“ přesvědčilo seniorku

UNIČOV – Seniorka naletěla na podvodné video s českými politiky.

Ve čtvrtek 29. května se na uničovské policisty obrátila 66letá žena, která se stala obětí podvodného jednání. Oznamovatelka před několika dny zareagovala na video s českými politiky, konkrétně premiérem Fialou a Babišem, kteří na něm propagovali výhodné investice. Jelikož ji video zaujalo, klikla na odkaz, kde uvedla své telefonní číslo. Záhy ji kontaktovala údajná makléřka. Poškozenou přesvědčila, aby zaslala prvotní investici ve výši 6 500 korun. Následně se s ní spojil další údajný makléř, který jí ukázal, jak se její vklad zhodnocuje. Žena uvěřila a během několika dní poslala celkem 525 tisíc korun. Když si však chtěla zhodnocené peníze vybrat, objevil se problém. Pod různými legendami ji podvodníci přesvědčili, aby si vybrala hotovost ve výši 250 tisíc korun, kterou předala osobně kurýrovi. Ženě se celá situace rozležela a uvědomila si, že se nejspíš stala obětí podvodu a obrátila se na policii. Poškozená tak přišla celkem o více jak 780 tisíc korun.

Případ prověřujeme pro podezření ze spáchání přečinu podvod, za který dle trestního zákoníku hrozí v krajním případě až pět let za mřížemi.

Pokud se rozhodnete hodnotit peníze například investováním do akcií nebo kryptoměny, obraťte se vždy jen na důvěryhodné a zavedené finanční společnosti. Velice ostražití buďte před lákavými reklamami neznámých organizací. Uvědomte si, že investování není bez rizika.

<https://policie.gov.cz/clanek/deepfake-video-presvedcilo-seniorku.aspx?>



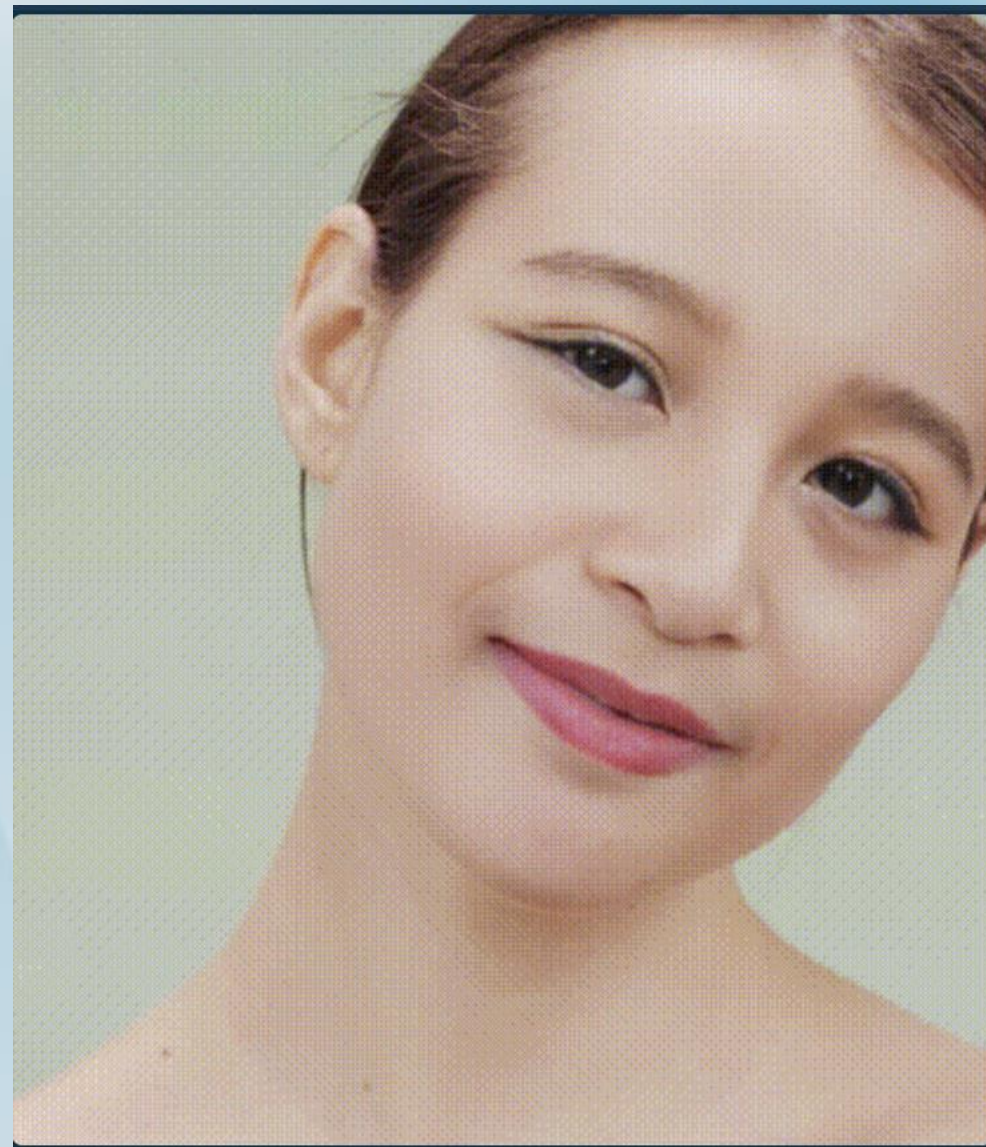
Na každé informaci záleží

Dokážete odhalit deepfake?

<https://quiz.iproov.com/>



Na každé informaci záleží



Dokážete odhalit deepfake?

<https://quiz.iproov.com/>



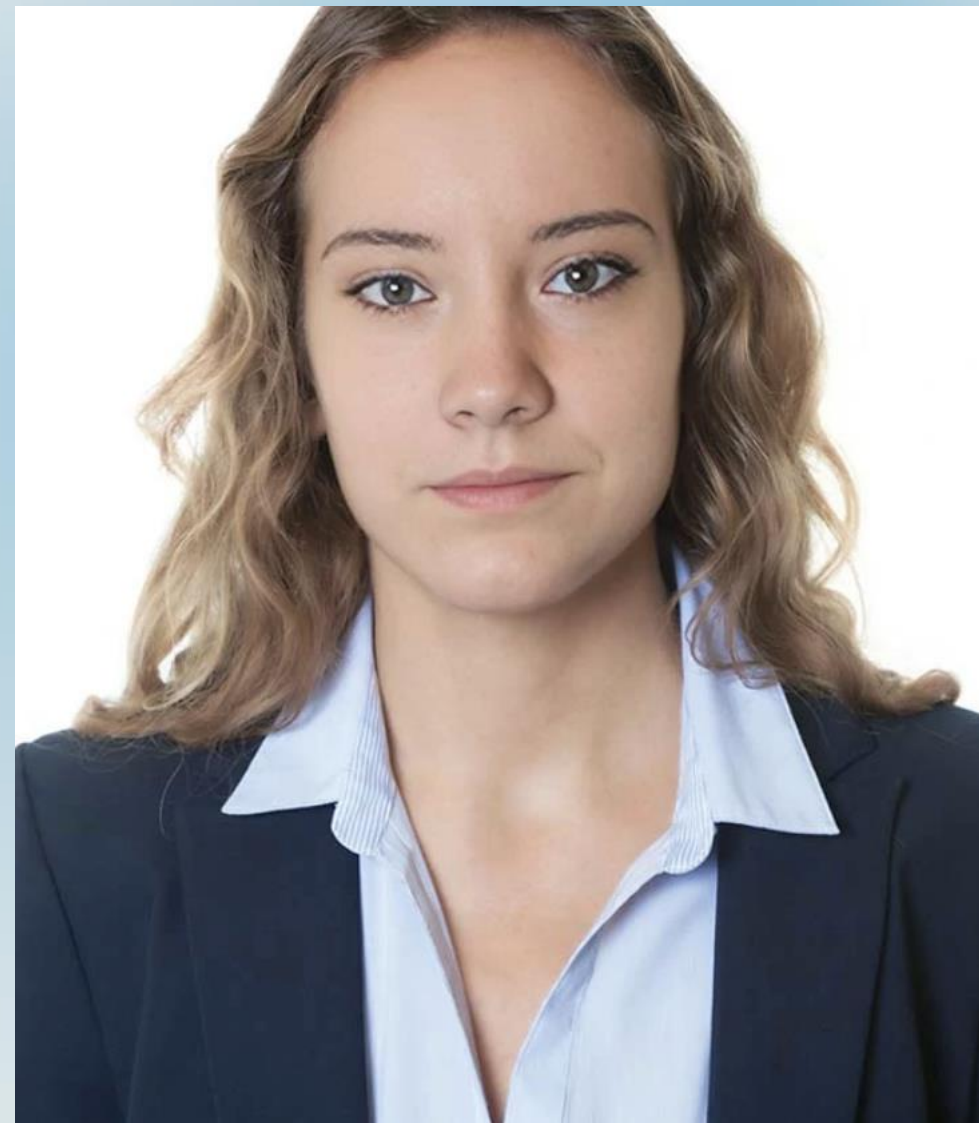
Na každé informaci záleží

Dokážete odhalit deepfake?

<https://quiz.iproov.com/>

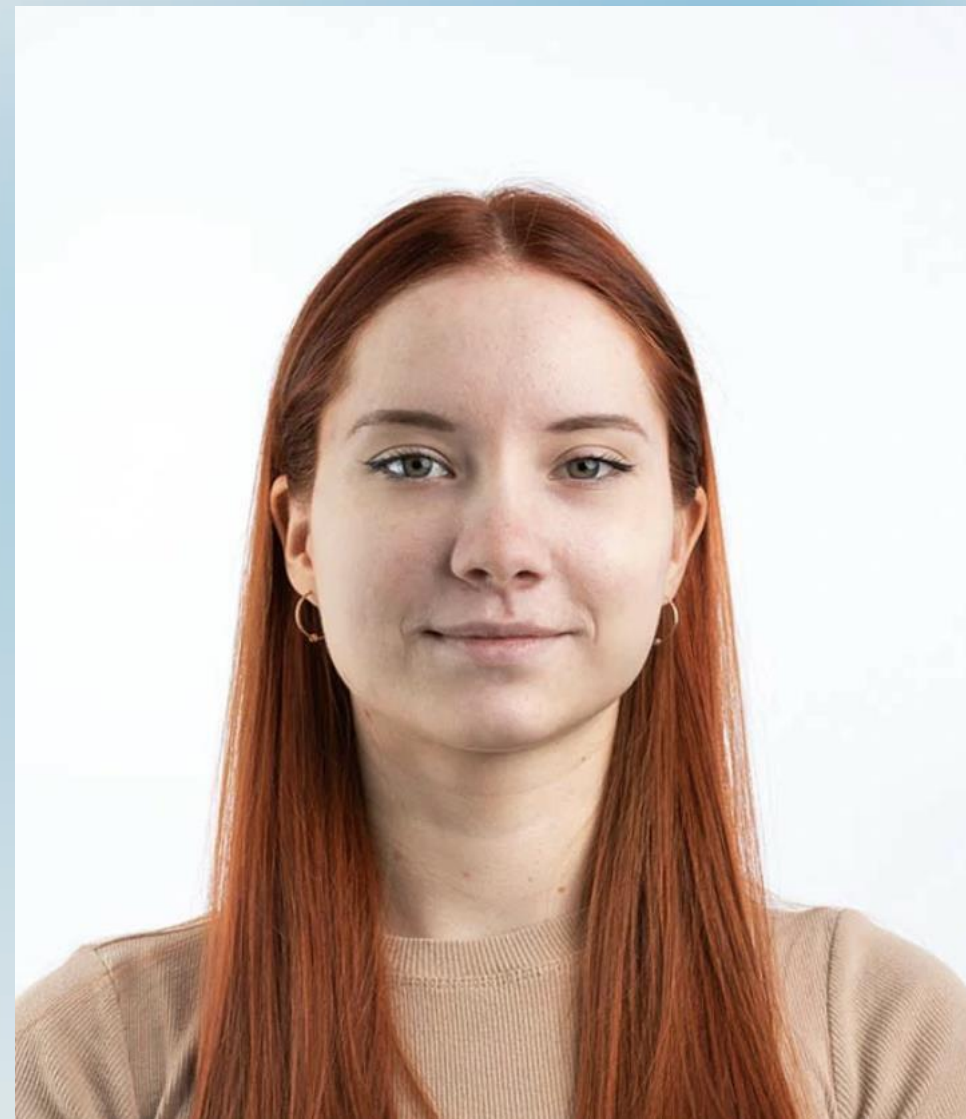


Na každé informaci záleží



Dokážete odhalit deepfake?

<https://quiz.iproov.com/>



Na každé informaci záleží

Typy častých deepfake

- Napodobení hlasu nadřízeného v telefonu
- Zveřejnění falešného prohlášení
- Tvorba videa se starostou/ředitelem
- Vydírání zaměstnanců deepfake nahotou
- Falešný telefonát



Deepfake – co mají společného?

Manipulace jako metoda sociálního inženýrství využívající psychologické triky vzbuzující důvěru, strach a naléhání.



Jak nastavit prostředí proti deepfake

- Školení a osvěta zaměstnanců
- Stanovení interních postupů komunikace
- Nastavení způsobů zavádění plateb nového dodavatele
- Použití dvoufaktorového ověření
- Připravený plán, jak reagovat na incidenty
- Pravidelné monitorování online prostředí



Digitální stopa a AI

Co za sebou necháváme při používání AI?



Na každé informaci záleží

Digitální stopa se mění

Digitální stopa

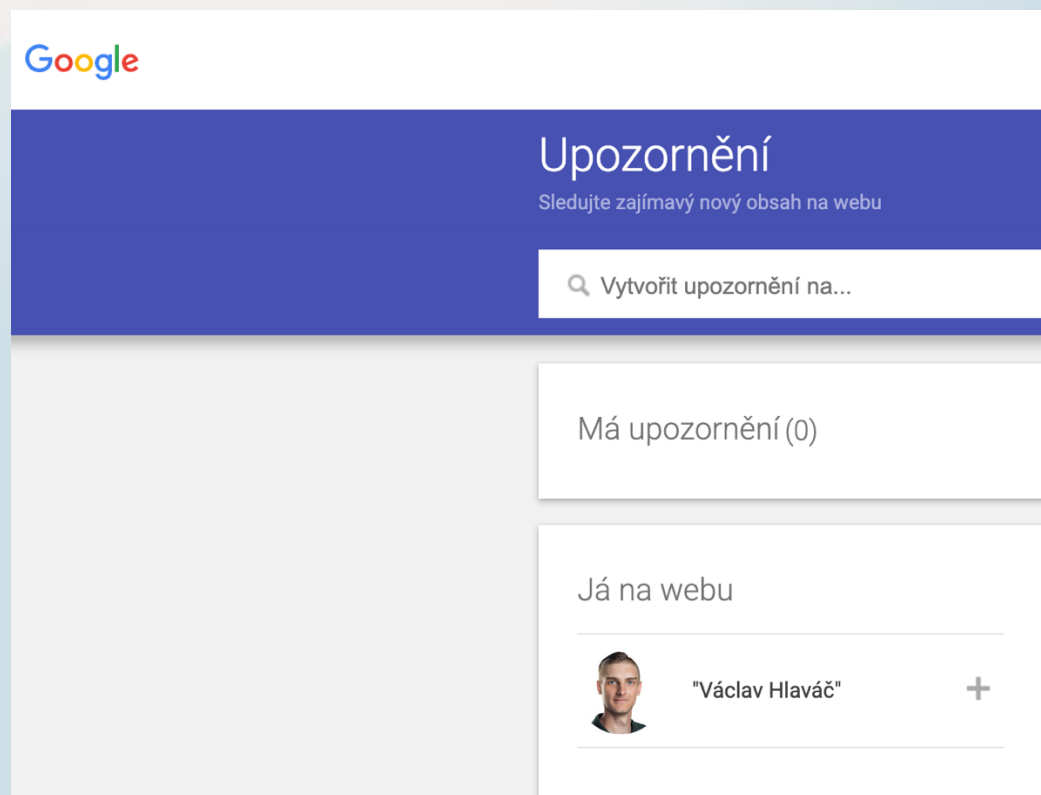
- Informace z našich online aktivit
 - Procházení webu
 - E-maily
 - Bezhotovostní transakce
 - Aktivita na sociálních sítích
 - Stahování souborů
 - Upload souborů

Jak mění digitální stopu AI?

- Více interakcí v přirozeném jazyku:
 - Zadání AI (prompty)
 - Metadata interakcí (okolnosti využití AI)
 - Odkazy na neveřejné dokumenty
 - Informace, které AI umožňuje odvodit
- AI dokáže data propojovat



Google Alerts: Monitorování svého jména



<https://www.google.com/alerts>



Na každé informaci záleží

Zjištění, zdali je heslo uniklé

Pwned Passwords

Check if your password has appeared in known data breaches

<https://haveibeenpwned.com/Passwords>



Na každé informaci záleží

Další nástroje pro bezpečná hesla

- Generování hesel: Bitwarden / 1Password
- Správce hesel: Bitwarden / 1Password / KeePass
- 2FA aplikace: Microsoft Authenticator / Google Authenticator



Co je problémem?

V obcích jsou stále běžné sdílené účty, hesla v sešitu nebo stejné heslo pro více systémů.



Co musí mít obec, škola i organizace

- ✓ Správce hesel
- ✓ Unikátní hesla pro každý systém (ne heslo typu „obec123“)
- ✓ 2FA / ověření přes mobil pro e-mail a klíčové systémy
- ✓ Pravidelná kontrola úniků (HIBP) a změna hesel při incidentu
- ✓ Žádná hesla v Excelu / Wordu / na papírku



Jak používat AI bezpečně

AI je pomocník, ale odpovědnost za výsledek nese vždy úřad



Na každé informaci záleží

Hlavní rizika pro úřad i školu

Nevědomé sdílení dat

Kus neveřejného dokumentu v promptu → data mohou být mimo kontrolu organizace.

Rekonstrukce identity / případu

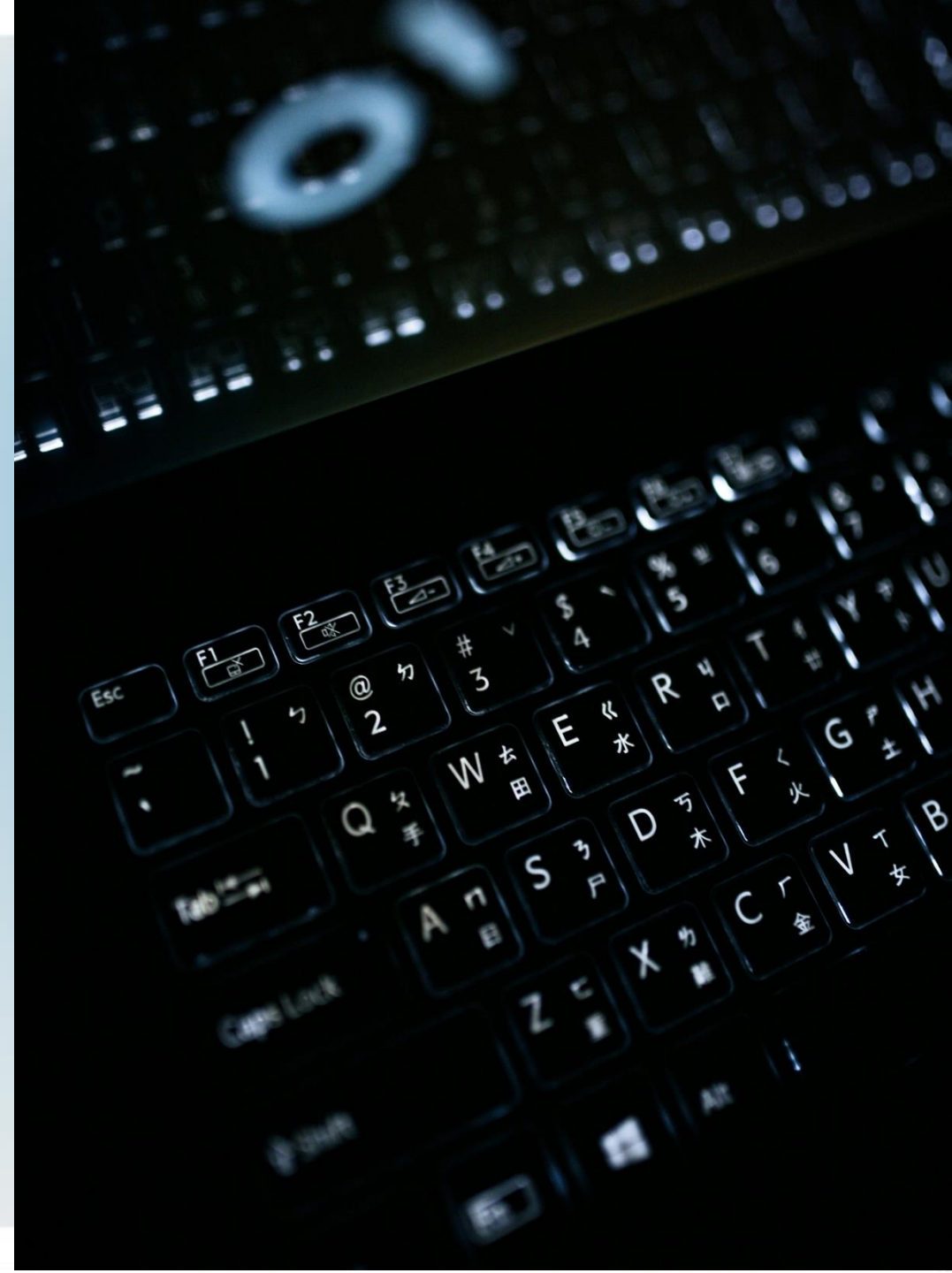
Model spojí informace z různých zdrojů a sestaví kompletní profil uživatele.

Halucinace

Přesvědčivě znějící nesmysl → špatné rozhodnutí a reputační škoda.



Na každé informaci záleží



Kam až se data mohou dostat

1) Úniky u poskytovatelů

I velké firmy zažily úniky uživatelských dat a logů.

2) Trénink modelů

U některých služeb mohou být vstupy použity k dalšímu učení (podle nastavení).

3) Subdodavatelské řetězce

Cloudové služby a analytické nástroje třetích stran.

4) Cílené kyberútoky

Databáze promptů a logů jsou atraktivní cíl.



Rychlé rozhodování: jaká data do AI patří?

Použijte 2 otázky: (1) Je to osobní / citlivé? (2) Je to neveřejné?

NEVEŘEJNÉ →	
OSOBNÍ / CITLIVÉ ↑	Veřejné, neosobní (OK pro veřejné nástroje) Příklad: veřejná vyhláška, obecní web, osnovy.
	Neveřejné, neosobní (spíš interní/tenant) Příklad: interní směrnice, rozpočet v přípravě.
	Neveřejné + osobní/citlivé (NE do veřejných AI) Příklad: spisy, žáci, HR, zdravotní, smlouvy.



Rychlé rozhodování: jaká data do AI patří?

Použijte 2 otázky: (1) Je to osobní / citlivé? (2) Je to neveřejné?

Příklad: veřejná vyhláška, obecní web, osnovy.

Příklad: veřejné seznamy, tiskové zprávy se jmény.

Příklad: interní směrnice, rozpočet v přípravě.

Příklad: interní směrnice, rozpočet v přípravě.



Doporučení k bezpečnosti

- Nevkládejte: osobní údaje, citlivé informace
- Zajistěte lidský dohled nad důležitými rozhodnutími
- Pro práci s citlivými daty požadujte od dodavatele lokální řešení
- Zaveďte pravidelné bezpečnostní audity AI nástrojů a procesů
- Kontrolujte přístupová oprávnění
- Pravidelně školte zaměstnance
- Ověřujte zdroje a autenticitu výstupů



Co si u AI nástroje zkontrolovat (praktický checklist)

1) Trénink / zlepšování na datech

Je možné ho vypnout? Platí to i pro přílohy a konektory?

2) Retence a mazání

Jak dlouho se uchovávají konverzace a logy? Co umí admin nastavit?

3) Kde jsou data fyzicky

Region / EU data boundary / subdodavatelé.

4) Audit & eDiscovery

Je možné dohledat kdo co dělal (u incidentu)?

5) Oprávnění a integrace

Je AI napojená na e-mail, Drive/SharePoint, systémy? Jak je to omezené?

Právo a AI

GDPR (osobní údaje)

Vy jako organizace jste správce. Potřebujete právní titul, minimalizaci dat, přiměřené zabezpečení a smluvní ošetření zpracovatele (pokud je).

EU AI Act (rizikový přístup)

AI se dělí dle rizik. Pro některá použití (např. v oblasti vzdělávání nebo veřejných služeb) může jít o „high-risk“ a přibývají povinnosti.

<https://asociace.ai/eu-ai-act/>

Neřešíme „můžeme AI používat?“, ale „za jakých podmínek a s jakými kontrolami“.

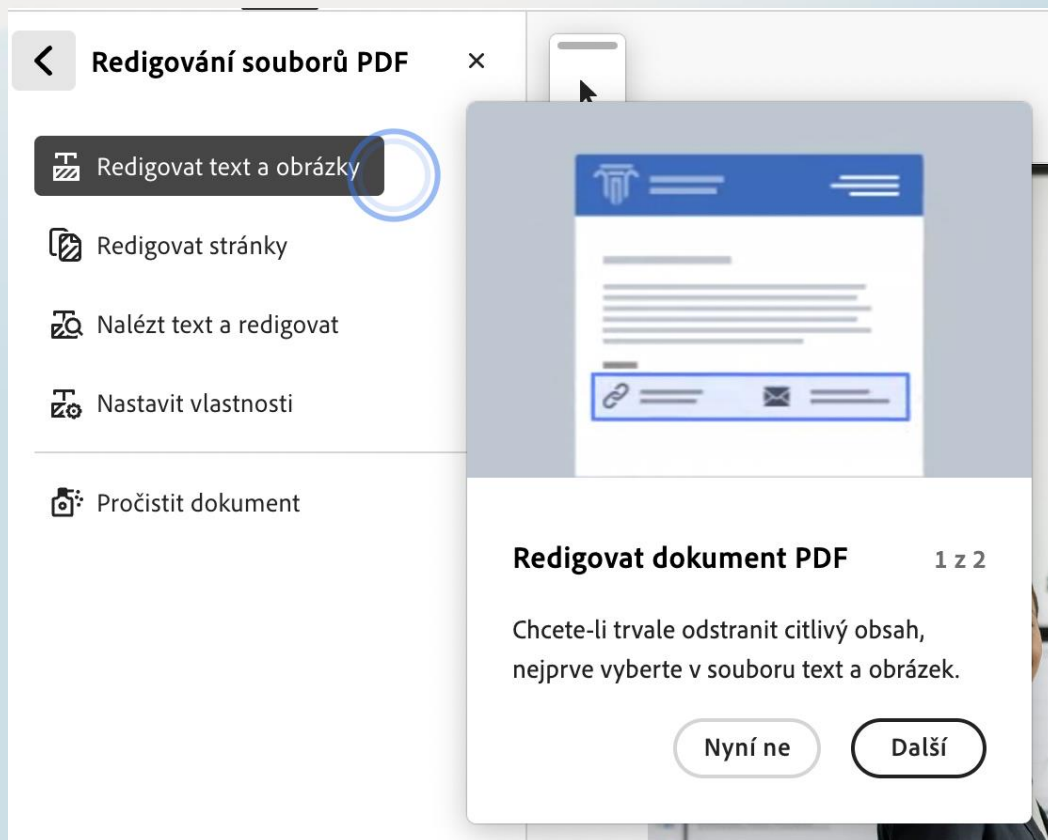


Co nikdy nevkládat do AI ve FREE verzi?

- Osobní údaje občanů/žáků (anonymizace pomáhá = “Občan A”)
- Smlouvy s citlivými údaji
- Dokumenty s viditelnými podpisy
- Přístupové údaje a API klíče



Odstranění citlivého obsahu Adobe Acrobat



Na každé informaci záleží

Anonymizace zdarma

<https://anonymizace.gov.cz/crossroad/>



Proč je to důležité?

- Březen 2023 – výpadek na straně OpenAI (open-source knihovna)
- Chyba umožnila některým uživatelům vidět názvy konverzací jiného aktivního uživatele.
- V některých případech mohla být viditelná i první zpráva nově vytvořené konverzace, pokud byli oba uživatelé aktivní ve stejnou dobu.

https://openai.com/index/march-20-chatgpt-outage/?utm_source=chatgpt.com



Proč řešit licence?

Free nástroje jsou levné na začátku,
ale drahé při incidentu.



CASB = Cloud Access Security Broker

- Zmapuje, jaké cloudové služby lidé používají (AI, úložiště, sdílení souborů...)
- Upozorní na rizika (např. upload dokumentů do veřejného AI)
- Zablokuje nebezpečné chování (např. nahrávání souborů do ChatGPT)
- Příklad: Microsoft Defender for Cloud Apps

<https://www.microsoft.com/cz/security/business/siem-and-xdr/microsoft-defender-cloud-apps#tabxf35d1115ca154ee49af0912241754d91>



Získejte úplný přehled o prostředí aplikací SaaS

Objevujte, ovládejte a konfiguruje aplikace a zajistěte, aby zaměstnanci používali důvěryhodné aplikace, které vyhovují předpisům.



Na každé informaci záleží

ChatGPT vs. Copilot vs. Gemini

	ChatGPT (Business/Enterprise/Edu)	Microsoft 365 Copilot	Google Workspace (Gemini)
Trénink na vašich datech	Ne	Ne	Ne
Izolace dat (tenant)	Ano	Ano	Ano
Kontroly pro admina	Ano	Ano	Ano
Typické riziko v praxi	Nesprávné účty / sdílení neveřejných dat do veřejné služby	Příliš široká oprávnění v M365, sdílení dokumentů + špatné sdílecí nastavení	Sdílení dokumentů v Drive + špatné sdílecí nastavení



Na každé informaci záleží

Webinářem to začíná

Nejlepší WhatsApp skupina o AI a inovacích pro obce, školy i organizace



Na každé informaci záleží

Exkluzivní obsah navíc zdarma ve WhatsApp



Jak na AI a inovace?



Na každé informaci záleží

Rizika AI prohlížečů

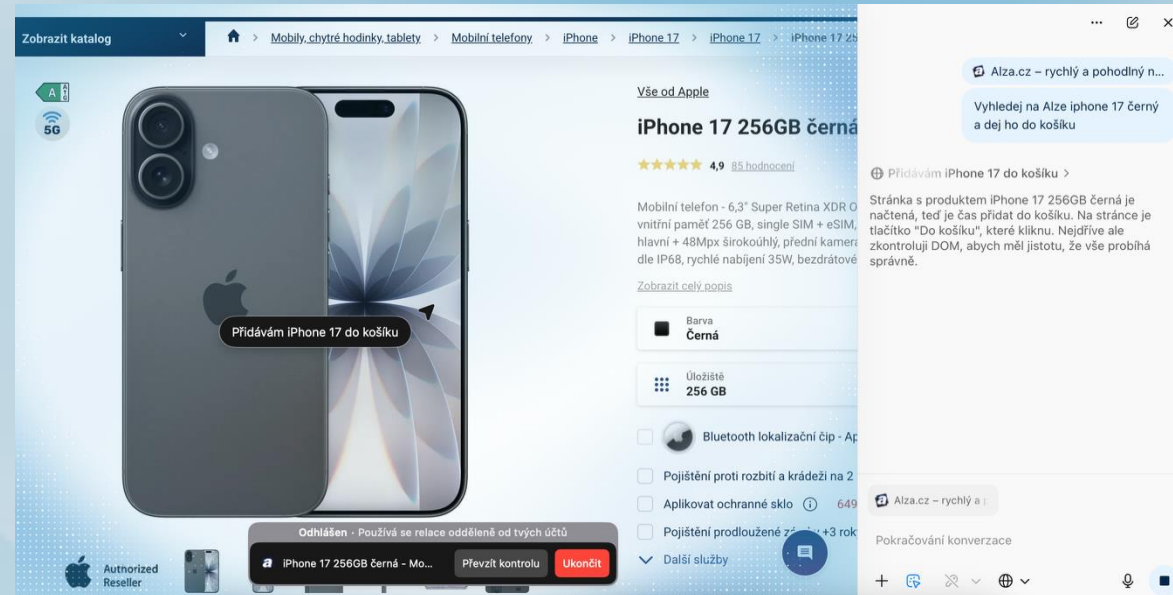
Revoluce na internetu, která zatím není bez rizika



Na každé informaci záleží

Změna prohlížení internetu

- Nové prohlížeče jako GPT Atlas nebo Perplexity Comet umožňují procházení internetu samostatně dle zadání uživatelem (vyhledání, vyplnění formuláře apod.)
- Doporučujeme prohlížeče používat bez přihlášení do systémů mimo pracovní profil



Na každé informaci záleží

AI bezpečnosti i pomáhá

AI není pro bezpečnost jen hrozba, ale i příležitost



Na každé informaci záleží

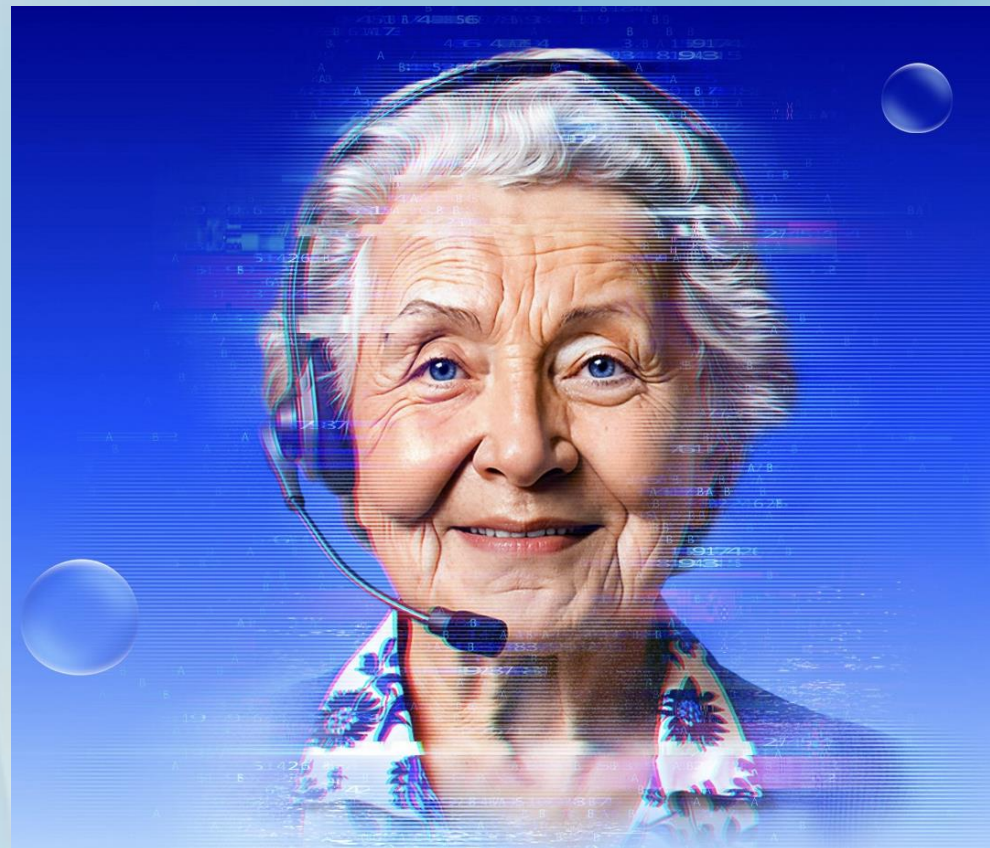
Kompletní AI asistent pro zabezpečení

- Microsoft Security Copilot
- Bezpečnostní analýza díky AI napříč daty, zařízeními, cloudy i aplikacemi
- Možnost automatického reagování na incidenty
- Odhalení skrytých rizik



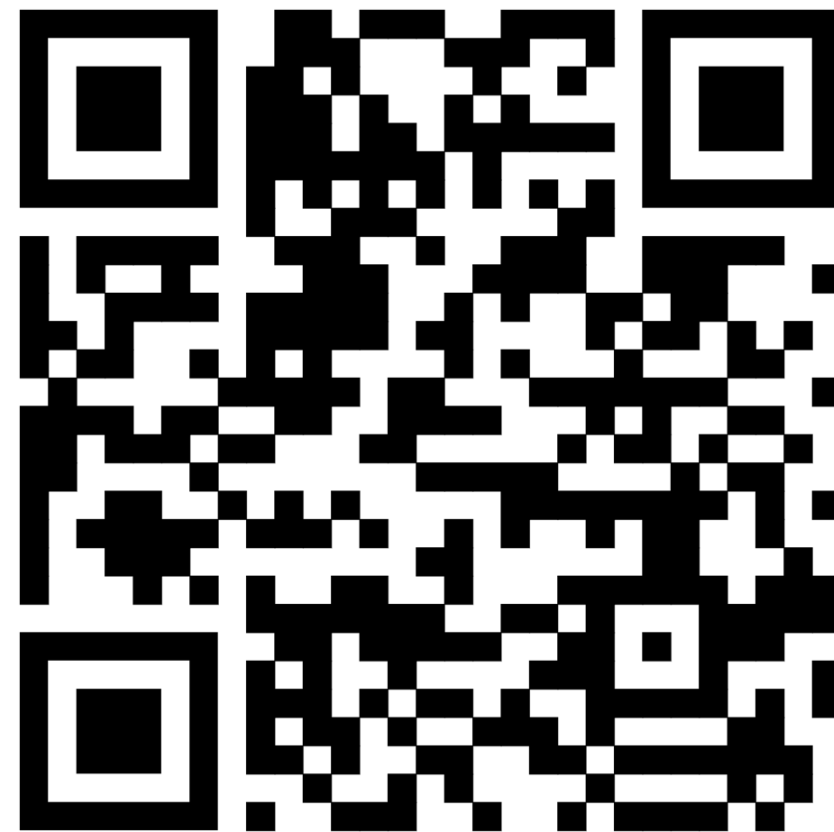
Společnost O2 zavedla "AI babičku Alenku"

- 100 000 blokováných hovorů denně
- Babička je vytrénovaná tak, aby zdržovala hovory podvodníků
- Více pro o projektu:
<https://www.o2.cz/osobni/volani/kybersmejdí>



Na každé informaci záleží

Zpětná vazba je pro nás důležitá...



Na každé informaci záleží

Exkluzivní obsah navíc zdarma ve WhatsApp



Jak na AI a inovace?



Na každé informaci záleží