Upozornění: následující odpovědi jsou pouze osobním názorem přednášející, nikoliv názorem úřadu či právním poradenstvím, a vycházejí ze současných poznatků a best practices k dubnu 2026.

Dotaz:

Dovoluji si požádat o váš návrh postupu v situaci, kdy mi opakovaně chodí na e-mail zprávy o falešných objednávkách a falešné faktury ze zahraničních e-mailových adres, se kterými nejsem v kontaktu a nic jsem si u nich neobjednala. Tyto e-maily neotevírám. Jak ale zabránit tomu, aby mi chodily, a jak zamezit tomu, aby sledovaly mou aktivitu (aniž bych na něco klikla)?

Odpověď:

Čím více takových zpráv chodí, tím pravděpodobnější je, že se váš e-mail objevil v některém datovém úniku. V takovém případě je vhodné e-mail lépe zabezpečit, případně zvážit jeho změnu.

Obecně doporučuji:

- Nesdílet a neotevírat tyto e-maily – neklikat ani na odkazy, ani na „unsubscribe“.
- Zakázat načítání vzdáleného obsahu (obrázků) v nastavení e-mailového klienta – tím zabráníte sledovacím pixelům.
- Nastavit filtry nebo blokaci odesílatelů/domén – většina e-mailových služeb to umožňuje.
- Označovat zprávy jako spam/phishing, aby se systém učil je filtrovat.
- Zkontrolovat únik e-mailu (např. přes službu HaveIBeenPwned) a případně zvážit novou adresu.
- Používat dvoufaktorové ověření pro e-mailový účet.

Dotaz:

Chodí mi 10–20 spamových e-mailů denně (seznamování, sexuální podtext, výhry apod.). Řešila jsem to i s policií. Prý to chodí z různých zemí a z cloudových služeb. Můj e-mailový poskytovatel říká, že pokud to padá do spamu, je to v pořádku.

Odpověď:

Odpověď je v zásadě stejná jako výše. Klíčové je:

- mít silné heslo (dlouhé, neslovníkové),
- zapnuté vícefaktorové ověření,
- využívat filtry (např. blokace slov jako „seznamka“, „krypto“ apod.).

Takto častý spam obvykle znamená, že se e-mail dostal do databází spammerů.

Dotaz:

Kde v ChatGPT nastavím soukromí, co přesně zaškrtnout?

Odpověď:

Klikněte na svůj profil → **Nastavení** → **Ovládací prvky pro data** →
vypněte možnost **„Vylepšovat model pro každého“**.

Dotaz:

Na LinkedInu je také spousta falešných kontaktů. Jak se chránit?

Odpověď:

Bohužel je to čím dál častější. Doporučuji:

- Prověřit profil (historie, kontakty, aktivita, ověření).
- Všímat si typických znaků podvodu: **urgence, autorita, vybočení z normy**.
- Položit si otázky:
    - Je nabídka „až moc dobrá“?
    - Tlačí mě někdo k rychlé reakci?
    - Vydává se za důležitou osobu?
- Ověřit informace i mimo platformu.
- Nikdy nesdílet hesla ani citlivé údaje.
- Do CV osobně neuvádím zbytečné osobní informace (např. adresu či věk).
- Podezřelé účty nahlašovat.

Dotaz:

Umožňují telefony nastavit více než 6místný PIN, například 12–15místný?

Odpověď:

Ano, iPhone i většina zařízení s Android to umožňují. Záleží na výrobci a nastavení, někdy je tato možnost méně viditelná.

Obecně platí:

- lze nastavit delší a bezpečnější kód než výchozí 4–6 číslic,
- případně i plnohodnotné heslo,
- některá zařízení umožňují vyžadovat kód častěji (např. místo biometrie v určitých situacích nebo pro citlivé aplikace či vždy po vypnutí).

Dotaz:

Je lepší při kybernetickém útoku shodit služby, nebo monitorovat, kam až se útočník dostane?

Odpověď:

Neexistuje univerzálně správná odpověď resp. netroufám si jí ze své pozice nikomu dát. Obecně platí, že standardnější praxí je útok co nejdříve omezit.

Současně ale může dávat smysl útočníka kontrolovaně sledovat. Záleží na:

- hodnotě systémů a dat,
- míře rizika,
- schopnostech a kapacitách týmu,
- typu a sofistikovanosti útoku,
- možných škodách (únik dat vs. výpadek služeb).

Dotaz:

Jak nakládat s údaji dětí, které rodiče sdílejí na sociálních sítích?

Odpověď:

Obecně doporučuji sdílení výrazně omezit, ideálně se mu vyhnout. Důvody:

- dětská data jsou na „datovém trhu“ velmi cenná,
- dítě má právo na soukromí.

Základní pravidla:

- nikdy nesdílet nahé ani polonahé fotografie,
- omezit viditelnost i u běžných fotografií,
- sdílet pouze velmi uvážlivě a s vědomím, že obsah může zůstat online trvale,
- počítat s tím, že data mohou využívat nejen lidé, ale i automatizované systémy (např. AI).

O čem ještě jsme na semináři „AI podvody a vaše digitální stopa: jak chránit své údaje“ mluvili?

Přednášející zdůrazňovala zásadu „**limit, guard, delete**“, kde **limit** znamená omezení sběru i tvorby osobních údajů, **guard** znamená povinnost je chránit online i offline pro každého, kdo k nim má přístup (nikoliv spoléhat na IT, HR nebo výrobce zařízení), a **delete** prezentuje praktiku automatického vymazávání starších údajů. Nebýt data hoarder je základ.

Také jsme detailněji probírali **psychologické postupy podvodníků**, kteří dokáží využít nátlaku tak, že i vzdělaný jedinec v produktivním věku může nabýt dojmu, že jedná správně, a poskytnout až nepochopitelné částky, či svá hesla k zařízení nebo PINY do aplikací.

Vyvolat pocit známosti či urgence je při zapojení dobře nastavené AI a připravenosti útočníka jednodušší než před lety, navíc díky AI je možné takové operace škálovat prakticky do nekonečna

a spoléhat na to, že „aspoň někdo se chytí“. Je tedy lepší mít mentálně nastaveno „toto se může stát i mně“ místo „já bych na to nikdy neskočil“.

Přednášející také zdůrazňovala, že pocit, že „moje data neunikla“, „má firma nikdy nebyla obětí útoku“ a „já problém vždy poznám“, je velmi často, ne-li vždy, mylný a vede k větší laxnosti.

Přístup „důvěřuj, ale prověřuj“, nebo dokonce „nedůvěřuj a prověřuj“, se vyplácí více.