

“Umělá inteligence a já: Jak se nenechat napálit”

Délka kurzu : 4 hodiny

- Varianta A: 2,5 h přednáška + 1,5 h diskuze
 - Varianta B: 2 h přednáška + 2 h praktické ukázky
-

Cílová skupina :

Senioři 60+, běžní uživatelé internetu a mobilních telefonů, kteří chtějí rozumět rizikům spojeným s moderními technologiemi a umělou inteligencí.

Cíl kurzu :

- Pochopit, co umělá inteligence (AI) umí – a co je zatím jen marketing.
 - Naučit se rozpoznat manipulativní, podvodné nebo nebezpečné situace.
 - Umět si poradit v praxi, pokud se stanou terčem AI podvodu (např. deepfake hovor).
 - Zvýšit digitální sebevědomí seniorů.
-

Osnova kurzu

I. Úvod do umělé inteligence (30 min)

- Co je a co není umělá inteligence
- AI v našem každodenním životě (příklady: navigace, chatboti, překladače)
- Mýty vs. realita

II. Jak může být AI zneužita – hrozby pro běžného občana (45 min)

- Telefonáty s falešnými hlasy dětí a vnoučat (deepfake audio)
- Podvržená videa a fotografie (deepfake video)
- Automatické generování věrohodných e-mailů a zpráv (phishing s pomocí AI)
- Manipulace na sociálních sítích a cílená propaganda
- Chatboti vydávající se za živé osoby
- Hrozby typu „vydírání přes e-mail“, podvodné výzvy k platbám

III. Co dělat, když něco podezřelého přijde (45 min)

- Kontrola faktů a zdravý rozum
- Jak ověřit zprávu nebo hovor
- Praktické zásady bezpečnosti (dvoufaktorové ověřování, zabezpečení telefonu)
- Kde hledat pomoc – linky důvěry, technická podpora, rodina
- Příklady konkrétních incidentů z ČR i světa

Varianty druhé poloviny kurzu:

✓ Varianta A – Diskuzní a sdílecí část (90 min)

- Moderovaná diskuze: Co už jste zažili?
- Příběhy z praxe účastníků
- Prostor pro dotazy a individuální konzultace
- Sdílení rad mezi účastníky

✓ Varianta B – Praktické ukázky a trénink (120 min)

- Ukázky:
 - Deepfake video vs. originál
 - Podvodný e-mail vs. skutečný
 - Podvodný telefonát
- Praktický trénink:
 - Ověřování identity (např. zpětné volání)
 - Využití webových nástrojů pro ověření informací (např. hoax.cz, fact-checkery)
 - Vyplnění testu „Poznáš podvod?“
- Krátké cvičení: “Jak bych se zachoval(a), kdyby...”

Doplňkové materiály pro účastníky :

- Tištěný přehled rizik a doporučení
- Návod „10 rad, jak se nenechat napálit“
- Sešit pro poznámky + checklist pro vlastní telefon / počítač

Sada **tréninkových kartiček pro seniory** na téma „**Poznáš podvod?**“.
Každá kartička obsahuje situaci, otázku a správnou odpověď s vysvětlením.
Kartičky budou využity při praktické části kurzu a budou účastníkům ponechány.

Volá vnouče z neznámého čísla

Zvoní vám mobil. Neznámé číslo. Ozve se uplakaný hlas: „Babičko, prosím tě, stalo se mi něco strašného, ale nesmíš to nikomu říct...“ Zní jako vaše vnouče.

? Otázka: Co uděláte ?

- a) Okamžitě se ptám, co se stalo a kde můžu poslat peníze.
- b) Ukončím hovor a zavolám vnoučeti zpět na jeho známé číslo.
- c) Hovor nepřijmu a rovnou ho smažu.

✓ **Správná odpověď: b)**

Vysvětlení: Jde pravděpodobně o tzv. **deepfake podvod**, kdy někdo napodobí hlas vnoučete. Vždy si ověřte, že volá skutečný člen rodiny – položte mu kontrolní otázku nebo hovor zavěste a zavolejte vnoučeti zpět na Vám známé číslo !

E-mail z banky

Přišel vám e-mail z Vaší BANKY. Píší, že váš účet byl z bezpečnostních důvodů zablokován. Stačí kliknout na odkaz a přihlásit se.

? Otázka: Co uděláte ?

- a) Kliknu na odkaz a přihlásím se – je to přece moje banka.
- b) Přepošlu mail vnoučatům, ať ho prověří.
- c) E-mail smažu a raději zavolám do své banky.

✓ **Správná odpověď: c)**

Vysvětlení: Banky nikdy nepošílají odkazy k přihlášení e-mailem. Jde o **phishing** – cílem je ukrást vaše přihlašovací údaje.

Zpráva na WhatsApp

Přijde vám zpráva: „Ahoj babi, mám nové číslo, starý mobil jsem ztratil. Potřebuju pomoc, můžeš mi poslat 8 000 Kč na účet?“

? Otázka: Co uděláte ?

- a) Pošlu peníze, je to přece moje vnouče.
- b) Zavolám mu zpět na jeho původní číslo nebo jinak ověřím, že je to on.
- c) Sepíšu si údaje a ověřím je později.

✓ **Správná odpověď: b)**

Vysvětlení: Tohle je velmi častý podvod. Vždy je potřeba **ověřit identitu osoby**, která vám píše, než uděláte cokoliv.

Facebook soutěž o mobil

Na Facebooku se objeví příspěvek: „Vyhráli jste nový iPhone! Klikněte na odkaz a vyplňte své údaje.“

? Otázka: Co uděláte ?

- a) Vyplním údaje, třeba to konečně vyšlo!
- b) Přepošlu to přátelům, aby mohli soutěžit taky.
- c) Ignoruji to – zní to příliš dobře, aby to byla pravda.

✓ **Správná odpověď: c)**

Vysvětlení: Takové soutěže bývají podvodné. **Cílem je získat vaše osobní údaje.** Nikdy nezasílejte nic bez ověření.

Úřad vám píše, že máte dluh

Dostanete dopis nebo e-mail, že máte dluh u České pošty nebo exekutora. Hrozí pokuta nebo soud, pokud hned nezaplatíte přes platební odkaz.

? Otázka: Co uděláte ?

- a) Okamžitě zaplatím, raději neriskuji.
- b) Ignoruji to, je to nesmysl.
- c) Zkontroluji web úřadu, případně zavolám na oficiální linku.

 **Správná odpověď: c)**

Vysvětlení: I **podvodné úřední zprávy** existují. Vždy si ověřte, že je zpráva pravá – ideálně přes oficiální web nebo telefonní číslo.

Pomoc Ukrajině / nemocnému dítěti

Na sociálních sítích se objeví dojemný příběh: dítě s rakovinou, sbírka na pomoc Ukrajině... S výzvou k daru na účet.

? Otázka: Co uděláte ?

- a) Přispěju, i kdyby to byla lež – chci pomoci.
- b) Zjistím, kdo za sbírkou stojí, a ověřím si ji.
- c) Pošlu peníze raději do sbírky, co sdíleli moji známí.

 **Správná odpověď: b)**

Vysvětlení: Bohužel existuje i **zneužívání empatie**. Používejte ověřené portály (např. Darujme.cz) nebo transparentní účty.

Doplňkové materiály pro účastníky - přehled rizik a doporučení

1. Podvodné telefonáty s falešným hlasem („deepfake“)

Riziko: Někdo vám zavolá a zní přesně jako vaše vnouče nebo dítě. Říká, že je v problémech a potřebuje peníze.

Doporučení:

- ✓ Nikdy neposílejte peníze bez ověření.
 - ✓ Zavolejte zpět na číslo, které znáte.
 - ✓ Zeptejte se na něco, co znáte jen vy dva.
-

2. Falešné zprávy přes WhatsApp, SMS a e-mail

Riziko: Zpráva od „vnuka“ z nového čísla, výzva k platbě, nebo e-mail z banky, že musíte něco potvrdit.

Doporučení:

- ✓ Vždy ověřujte identitu odesílatele.
 - ✓ Neotvírejte podezřelé odkazy.
 - ✓ Banky vás nikdy nežádají o přihlášení přes e-mail.
-

3. Podvodné soutěže, slevy a nabídky na sociálních sítích

Riziko: Zpráva typu „Vyhráli jste mobil! Klikněte zde“. Ve skutečnosti jde o sběr dat nebo vir.

Doporučení:

- ✓ Neposkytujte osobní údaje cizím stránkám.
 - ✓ Dávejte si pozor na soutěže, které vypadají „až moc dobře“.
 - ✓ Nešířte dál zprávy, které jste si neověřili.
-

4. Falešné sbírky a emocionální manipulace

Riziko: Emočně silné příběhy o nemocných dětech, zvířatech nebo válečných obětech – výzva k daru.

Doporučení:

- ✓ Přispívejte pouze přes ověřené sbírky (Darujme.cz, Post Bellum, Člověk v tísni).
 - ✓ Vždy si ověřte číslo účtu a organizaci.
-

5. Šíření dezinformací a strachování

Riziko: Umělá inteligence může generovat falešné články, fotografie, videa (např. o očkování, politice, migraci).

Doporučení:

- ✓ Nevěřte hned všemu, co čtete.
 - ✓ Porovnávejte informace z více zdrojů.
 - ✓ Používejte seriózní zpravodajství (ČT24, iRozhlas, Deník N apod.).
-

6. Zneužití identity a přístupových údajů

Riziko: Někdo získá vaše přihlašovací jméno a heslo do e-mailu, banky nebo sociální sítě.

Doporučení:

- ✓ Používejte silná a různá hesla.
- ✓ Zapněte dvoufázové ověření (např. SMS kód).
- ✓ Nesdílejte své přístupové údaje s nikým.

● 7. Automatizované hovory a „roboti“ (AI chatboti)

Riziko: Volá vám „úředník“ nebo „operátor“, ve skutečnosti jde o naprogramovaného robota.

Doporučení:

- ✓ Ukončete podezřelý hovor.
- ✓ Neříkejte žádné osobní údaje, dokud si nejste jistí s kým mluvíte.
- ✓ Pokud si nejste jisti, poraďte se s někým blízkým.

● OBECNÁ DOPORUČENÍ

- ✓ Mluvte se svými blízkými – před podvodem vás často ochrání rodina.
- ✓ Mějte přehled – podvody se vyvíjejí, sledujte, co je „nové“.
- ✓ Při pochybnostech nejednejte pod tlakem. Udělejte si čas.
- ✓ Nebojte se říct si o pomoc – je to projev síly, ne slabosti.

10 rad, jak se nenechat napálit

(v době chytrých telefonů, umělé inteligence a podvodníků)

1 Nikdy neposílejte peníze na základě jednoho telefonátu nebo zprávy

Ani když volá někdo, kdo zní jako vaše dítě nebo vnouče. Vždy si informaci ověřte – zavolejte zpět na známé číslo.

2 Když se něco zdá až příliš výhodné, je to podvod

Vyhrát iPhone bez soutěžení? Sleva 90 % jen dnes? Tohle bývají podvodné triky, jak vás nalákat ke kliknutí.

3 Neříkejte své heslo nebo rodné číslo nikomu po telefonu

Ani „bankovnímu poradci“, „úředníkovi“ nebo „policistovi“. Skutečné instituce tyto údaje nikdy po telefonu nevyžadují.

4 Nikdy neklikejte na podezřelé odkazy v e-mailech nebo SMS

Můžou vést na falešné stránky, které vypadají jako skutečné (např. Česká pošta, banka, e-shop).

5 Používejte různé hesla pro různé účty

Alespoň pro e-mail, banku a Facebook. Nechte si je napsat do bezpečného papírového sešitu.

6 Nenechte se vystrašit větami jako „okamžitě zaplat’te“

Podvodníci často tlačí na čas. V klidu si vše ověřte – tlak a strach jsou jejich zbraně.

7 Sbírky ověřujte – přispívejte jen tam, kde znáte organizaci

I dobré srdce může být zneužito. Využívejte ověřené platformy (např. Darujme.cz, Člověk v tísni).

8 Neptejte se AI (např. ChatGPT) na věci jako: „Jak obejít bankovní zabezpečení“

Takové otázky mohou být nebezpečné nebo mohou vést k manipulaci.

9 Pokud si nejste jisti – zavolejte někomu blízkému

Není žádná ostuda se zeptat. Lepší zdržení než litování.

10 Co si řeknete vy, než někam kliknete nebo odpovíte?

„Zní to divně? Může to být past. Raději si to ověřím.“