# RIZIKA SPOJENÁ S UMĚLOU INTELIGENCÍ PRO SENIORY

**Rizika spojená s umělou inteligencí pro seniory**

Kamil Kopecký, René Szotkowski, Lukáš Kubala

Centrum prevence rizikové virtuální komunikace
Pedagogická fakulta Univerzity Palackého v Olomouci
ve spolupráci s CEDMO (Středoevropská observatoř digitálních médií) při Univerzitě Karlově 
www.e-bezpeci.cz www.cedmohub.eu/cs

Tato příručka vznikla díky podpoře společnosti Google.

# Obsah

# Vítejte ve světě umělé inteligence

Aniž bychom si to občas uvědomovali, **žijeme ve světě plném umělé inteligence (AI)** – nástroje využívající umělou inteligenci máme ve svých mobilních telefonech i počítačích, umělá inteligence je součástí internetových vyhledávačů a sociálních sítí, doporučuje nám, jaký článek si přečíst, jaký film si pustit či jaké zboží si na internetu koupit. Jednoduché nástroje využívající umělou inteligenci najdeme třeba v chytrých vysavačích, které nám automaticky uklízejí v našich domácnostech, a jsou také součástí chytrých ledniček či chytrých termostatů, jež nám doma regulují teplotu.

Cílem této příručky je **upozornit na vybraná rizika spojená s umělou inteligencí,** na něž je třeba dát si pozor a s nimiž je nutné počítat. **Při správném a bezpečném chování na internetu jsou ovšem rizika minimální, proto se online světa nebojte a využívejte výhod plynoucích z používání AI.** Snad vám následující řádky pomohou k lepší orientaci v online světě, který se vám může zdát nepřehledný a mnohdy matoucí.

# 1. Co je to umělá inteligence?

Umělá inteligence (AI) označuje **počítačové programy** (software), jež jsou schopny napodobovat lidské myšlení a chování a dokáží řešit různé úkoly, které dříve zvládli pouze lidé.

Tyto programy využívají **algoritmy**, což jsou složité matematické postupy, jež napodobují procesy učení a rozhodování v lidském mozku. Díky tomu může AI rozpoznávat vzory v datech, učit se z minulých zkušeností, předvídat výsledky nebo rozumět lidskému jazyku. Tato schopnost umožňuje AI vykonávat rozmanité úkoly od řízení aut přes automatizaci průmyslové výroby až po osobní asistenci a zdravotní diagnostiku. Důležité je, že se umělá inteligence neustále vyvíjí a zlepšuje, což přináší nové možnosti jejího využití ve prospěch lidstva.

V současnosti je populární především tzv. **generativní umělá inteligence**, která označuje modely umělé inteligence navržené tak, aby **generovaly nový obsah** – dokážou např. psát texty (články, knihy), vytvářet obrázky a fotografie, napodobit lidský hlas, komponovat hudbu, a dokonce vytvářet videa na přání. To s sebou

nese mnoho příležitostí, ale také rizik. Umělá inteligence v současnosti **nemá vědomí** ani **emoce**, její chování je naprogramováno.

## 2. Pozitiva spojená s využíváním umělé inteligence

Umělá inteligence dokáže být velmi prospěšná a může zlepšit náš život. Jedním z nejvýznamnějších pozitiv je zvýšení efektivity a přesnosti v mnoha odvětvích, například ve **zdravotnictví** může pomáhat s diagnózou a léčbou nemocí. AI také usnadňuje každodenní úkoly, například **navigaci v dopravě** nebo správu osobních financí, a to díky inteligentním aplikacím. Ve vzdělávání umožňuje **personalizované učební programy**, které se přizpůsobují potřebám studenta. Navíc může významně přispět k **ochraně životního prostředí** optimalizací využívání zdrojů a snižováním odpadu.

V neposlední řadě nabízí AI nové možnosti pro **zábavu** a **kreativitu**, například ve videohrách nebo umění, kde může inspirovat k novým formám tvorby. Na všech těchto příkladech vidíme, jak umělá inteligence **zlepšuje kvalitu našeho života**, činí nás produktivnějšími a kreativnějšími a přináší nové možnosti osobního rozvoje.

Umělá inteligence může být **velmi prospěšná i pro seniory**. Například dokáže pomoci s **monitorováním zdravotního stavu** prostřednictvím inteligentních zařízení, která jsou schopna sledovat vitální funkce a upozornit na případné problémy nebo nezvyklé změny, jež by mohly vyžadovat lékařskou pozornost. Dále AI může podporovat seniory ve **větší samostatnosti a bezpečnosti v domácím prostředí** díky chytrým domácím asistentům, kteří reagují na hlasové příkazy a pomáhají tak s ovládáním domácích zařízení, připomínáním důležitých úkolů či léků a s poskytováním zábavy nebo informací.

Dalším významným přínosem je možnost využití AI v **komunikaci a sociálním kontaktu**, různé aplikace a platformy mohou seniorům usnadňovat videohovory s rodinou a přáteli nebo je propojit se skupinami se společnými zájmy. S generativními typy umělé inteligence (ChatGPT, Gemini, Copilot) lze také **konverzovat**, díky čemuž mohou **simulovat sociální kontakt**. AI rovněž nabízí přístup ke **vzdělávacím zdrojům** a aktivitám pro **mentální stimulaci**, což je důležité k udržení mentální svěžesti.

V neposlední řadě může umělá inteligence pomoci v **překonávání jazykových bariér** nebo obtížích s čtením, díky pokročilým nástrojům

pro překlad nebo převod textu na mluvené slovo umožňuje seniorům snadnější přístup k informacím a komunikaci v různých jazycích. Tyto technologie nabízejí seniorům nejen větší nezávislost a bezpečnost, ale také možnost sociální interakce, učení a zábavy.

Generativní AI umožňuje snadno **vytvářet umělecká díla** (obrázky, fotografie) nebo **hudbu**, aniž byste museli mít hluboké znalosti nebo dovednosti v dané oblasti. To může být zábavné a stimulující a poskytuje to prostor pro osobní vyjádření a kreativitu. Umělá inteligence se může stát skvělým pomocníkem třeba **při psaní** – ať už píšeme dopis přátelům, nebo chceme napsat sbírku příběhů ze života.

# UMĚLÁ INTELIGENCE MĚNÍ SVĚT!

# 3. Rizika spojená s využíváním umělé inteligence

Přestože může být umělá inteligence prospěšná, pojí se s ní rizika, na něž je třeba dávat si pozor a se kterými je potřeba počítat.

Nástroje umělé inteligence lze zneužít k **podvodnému jednání** – např. k vytváření a šíření podvodných e-mailů (phishing, scam) či zpráv, které se nás snaží přimět, abychom někomu **prozradili své osobní či jiné citlivé údaje** (třeba hesla, čísla bankovních karet apod.) či někomu neznámému poslali peníze. V současnosti je AI zneužívána i v rámci **podvodných reklam** slibujících zázračné zbohatnutí. V takových případech jsou vytvořena videa, na kterých k nám promlouvá známá osobnost (politik, herec apod.), jež nám doporučuje daný výrobek či službu. Ve skutečnosti jsou však takto videa často podvržena a jde o tzv. **deep fakes** (podrobněji dále v textu).

Další možností, jak lze bohužel umělou inteligenci zneužít, je **tvorba a šíření nepravdivých informací** (**dezinformací, hoaxů, fake news**), což lze realizovat velmi rychle, během krátkého času. Umělá

inteligence navíc dokáže vytvářet nepravdivé informace v podobě **textu, obrázků, fotografií, zvuku či videí**, což uživatelé často nedokážou odhalit a věří, že jde o pravdivé záznamy. Proto je důležité zvykat si na to, že fotografie ani videa nemusejí pravdivě zachycovat realitu.

Také je třeba si uvědomit, že **umělá inteligence se učí z dat** (textů, zpráv), **která do ní zadáváme**, proto bychom si měli vždy **promyslet**, zda do nástrojů AI **nevkládáme i něco citlivého** – např. rodná čísla, hesla, informace ze zdravotní dokumentace apod. Tato data by mohla uniknout a být zneužita. Jakmile totiž naše citlivé údaje vložíme do systému, **je velice obtížné sledovat, k čemu jsou využívány**, a jejich odstranění může být v budoucnu problematické. Mimochodem umělá inteligence dokáže na základě těchto dat vytvořit naše psychologické profily, které se dají využít k zobrazování personalizované reklamy – to znamená, že každý uživatel internetu vidí na webových stránkách či sociálních sítích reklamy, jež jsou cíleny přesně na něj. Kvůli výše zmíněným rizikům bychom měli využívat důvěryhodné AI nástroje a nezapomenout si pečlivě přečíst **zásady ochrany osobních údajů**,

abychom věděli, jak jsou naše citlivé údaje shromažďovány, k čemu se používají, případně s kým jsou sdíleny.

Pokud jste některý z nástrojů umělé inteligence vyzkoušeli, možná jste si všimli, že **umělá inteligence občas dělá chyby** (tzv. halucinuje). To je dáno např. tím, že nemusí být zcela dokonale natrénována, nemusí mít dostatek relevantních dat k danému tématu apod. Proto je třeba výstupy umělé inteligence (především té generativní) **pořádně zkontrolovat**.

Umělá inteligence již nyní **zasahuje do trhu práce**, některé profese tak mohou zaniknout a živé pracovníky nahradí nástroje umělé inteligence. Na druhou stranu další profese budou vznikat. Každopádně platí, že **ti, kteří budou umělou inteligenci aktivně využívat, budou mít oproti těm, kteří budou AI přehlížet a ignorovat, výhodu.**

Se stále větším používáním umělé inteligence roste také míra **závislosti na této technologii**, což může vést k tomu, že lidé přestanou rozvíjet vlastní znalosti, dovednosti a kritické myšlení a budou se příliš spoléhat na pokročilé technologie. A to může být skutečně nebezpečné.

# 4. Vybraná rizika spojená s umělou inteligencí

V této kapitole se podrobněji zaměříme na **vybraná rizika**, která jsou spojena s využíváním (a často zneužíváním) **nástrojů generativní umělé inteligence**. Text je doplněn o příklady a obrazový materiál ilustrující zneužití generativní umělé inteligence v praxi.

Věnovat se budeme především:

1. **Internetovým podvodům**
2. **Nepravdivým zprávám (dezinformacím, misinformacím)**
3. **Deep fake videím**
4. **Narušení soukromí pomocí umělé inteligence**

# 4.1 Internetové podvody

Hned úvodem je nutné zmínit, co je to **Podvod § 209** (Trestní zákoník 40/2009 Sb.). Podvod je trestným činem a dopouští se ho ten, kdo sebe nebo jiného obohatí tím, že někoho uvede v omyl, využije něčího omylu, zamlčí podstatné skutečnosti a způsobí tak na cizím majetku škodu **nikoli nepatrnou**. **Škoda nikoli nepatrná** je škoda dosahující částky nejméně **10 000 Kč**. (§ 138 Hranice výše škody, prospěchu, nákladů k odstranění poškození životního prostředí a hodnoty věci.)

**Za podvod hrozí trest** odnětí svobody až na **2 roky**, zákaz činnosti nebo propadnutí věci či jiné majetkové hodnoty. **Trest za větší škodu** je 1–5 let, trest za podvod velkého rozsahu pak 5–10 let.

Má tedy smysl oznámit Policii ČR i podvod malého rozsahu? Např. když vám někdo podvodem způsobí škodu **500 Kč**.

**Určitě ano, každý podvod nahlaste!**

Škody pachatele se **sčítají** a pro právní posouzení je tedy důležitá **celková škoda u všech poškozených**.

# Internetové podvody a umělá inteligence

Internetové podvody podpořené nástroji **generativní umělé inteligence** se stávají stále dokonalejšími, proto je nezbytná ostražitost. Většina online podvodů se zaměřuje na **finanční prostředky** poškozených osob, ojedinělé nejsou ani případy, kdy jsou lidé okradeni o celoživotní úspory.

Vybrané internetové podvody:

A. **Podvodné investiční nabídky**

B. **Podvodní online bankéři**

C. **Vyděračské podvody**

# A. Podvodné investiční nabídky

K novým typům podvodů patří podvody spojené s investicemi do **akcií a kryptoměn (virtuálních peněz)**. Mnohdy využívají **falešnou reklamu s celebritami**, které doporučují danou investici jako skvělý způsob zbohatnutí.


# Průběh podvodu

**1. Falešná reklama s celebritou** vás dovede na **podvodné stránky se „zaručeně výdělečnou investicí“**.

Falešná reklama je často doplněna o **falešné video s celebritou**, která doporučuje investici u dané společnosti. Falešné video je často vytvořeno **umělou inteligencí** (tzv. deep fake).

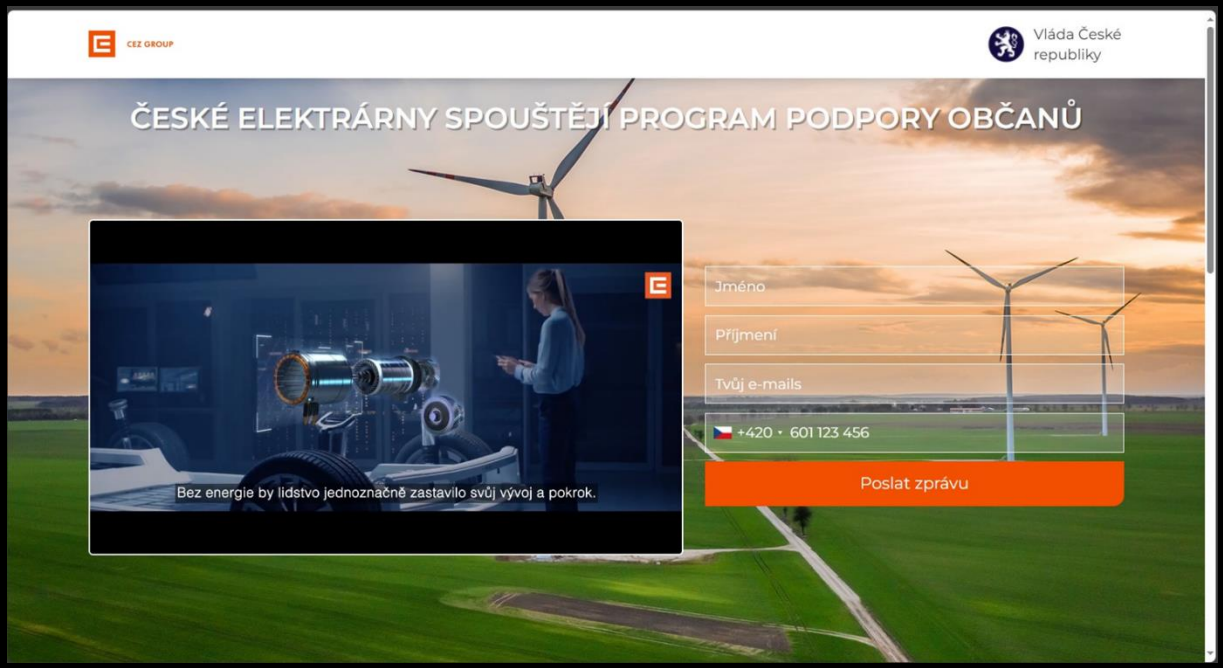
**2. Podvodná stránka** vás vyzývá k tomu, abyste **vložili své osobní údaje** (především kontaktní telefonní číslo a e-mailovou adresu). Pokud na stránce své telefonní číslo zanecháte, ozve se (např. telefonicky) „pracovník“, který vám vysvětlí další postup.

**3.** Prvním krokem je obvykle nutnost nainstalovat program pro **přístup ke vzdálené ploše vašeho počítače** (např. **AnyDesk, TeamViewer** apod.). Takto bude přes váš účet daná instituce „investovat“ (u některých typů podvodu investují **„živí lidé“**, u jiného různí automatičtí roboti) a zajistí vám trvalý zisk. **Ve skutečnosti však jde o podvod – útočník získal přístup k vašemu účtu a může z něj převádět finanční prostředky**.

# Falešná videa zneužívající známé osobnosti (tzv. deep fake)


## Falešná videa zneužívající známé osobnosti (tzv. deep fake)


## Ukázka podvodné stránky, na kterou odkazuje podvodné video




*Falešná investiční stránka, která se zobrazí po kliknutí na falešnou investiční reklamu. Falešné stránky často zneužívají loga velkých společností, jako jsou např. ČEZ, MND, nebo státních institucí, např. Vlády České republiky.*

# B. Podvodní online bankéři

Velmi nebezpečným typem podvodů jsou tzv. **online podvodní bankéři**, kteří vás osloví prostřednictvím e-mailu. E-mail, který obdržíte, vypadá velmi autenticky a věrohodně, často je odeslán ze **skutečné e-mailové adresy banky**.

Podvodný online bankéř informuje o problému, který se vyskytl na vašem účtu, např. tvrdí, že do něj někdo pronikl a chce vám odcizit peníze. Novinkou je e-mail, ve kterém se objeví **falešné video online bankéře**, jež je vytvořeno umělou inteligencí a instruuje vás, jak dále postupovat. Dalším typem tohoto podvodu je tzv. **vishing** – telefonní podvod, kdy pachatel obvolává své oběti.


Podvržené video s falešným bankéřem vytvořené umělou inteligencí vypadá věrohodně, jde však o produkt umělé inteligence vytvořený často z fotografie existujícího člověka.

# Průběh podvodu (vishing)

**1.** Nejprve vám zatelefonuje člověk, který se představí jako **zaměstnanec banky (nebo jiné společnosti)** a sdělí vám, že váš účet je napaden a on jediný může pomoci zachránit vaše prostředky.

**2.** K záchraně vašeho účtu potřebuje **bezpečnostní údaje k internetovému bankovnictví** (ID a heslo, datum narození) nebo k **platební kartě** (číslo, platnost, jméno na kartě, PIN apod.).

**3.** Následně se vás snaží přesvědčit, abyste mu **předali bezpečnostní kódy ze SMS nebo potvrdili operaci v aplikaci či zaslali bankovní klíč**.

**POZOR** – pomocí nástrojů umělé inteligence může útočník napodobit jakýkoli hlas! Telefonát zaměstnance banky tudíž může působit naprosto věrohodně!

# C. Vyděračské podvody

Například prostřednictvím e-mailu jste informováni, že si vás **někdo natočil přes webkameru, získal přístup do vašeho počítače** nebo má k dispozici **kompromitující obsah**.

Vyděrač následně **vyhrožuje zveřejněním kompromitujících fotografií, videí či informací** a požaduje peníze.

Vydírání je často podpořeno kompromitujícím materiálem v podobě fotografie, videa či textu, jež jsou vytvořeny prostřednictvím **generativní umělé inteligence**.

Nástroje generativní umělé inteligence jsou schopny **vytvořit kompromitující materiál z již existující reálné fotografie (svlékací umělá inteligence)**, případně útočník vytvoří fotografii zcela novou, kde pouze doplní obličej poškozené osoby.

**Ukázka vyděračského e-mailu**

Ahoj drahý uživateli,
do vašeho přístroje jsme nainstalovali jeden software RAT. Pro tento okamžik je váš e-mailový účet napaden (viz „from address“, nyní mám přístup k vašim účtům).

Vaše heslo z novak@volny.cz: je *******. Stahoval jsem všechny důvěrné informace z vašeho systému a dostal jsem další důkazy.

**Nejzajímavějším okamžikem, který jsem objevil, jsou videozáznamy o vás masturbující**. Zveřejnil jsem virus na pornografickém webu a pak jste jej nainstalovali do svého operačního systému. Po klepnutí na tlačítko Přehrát na porno video, v tom okamžiku byl můj trojan stažen do vašeho zařízení. **Po instalaci vám přední fotoaparát natáčí video pokaždé, když masturbujete, software se synchronizuje s vybraným videem.** Prozatím software získal všechny vaše kontaktní informace ze sociálních sítí a e-mailových adres.

Pokud potřebujete smazat všechny shromážděné údaje, pošlete mi $550 v BTC (kryptoměně).

## Ukázka možného zneužití osobního údaje v podobě fotografie

*Ukázka možného zneužití tzv. svlékací umělé inteligence. Vyděrači mohou tímto způsobem zneužít osobní údaj v podobě fotografie k vydírání. Na fotografii není skutečný člověk! Pro ilustrační účely byla vytvořena fotografie seniorky pomocí umělé inteligence.*

# Obrana proti internetovým podvodům

**Neklikejte na reklamu** s celebritami slibujícími velké zisky. V rámci podvodu byli zneužiti např. Petr Pavel, Andrej Babiš, Karel Havlíček, Jakub Prachař, Jan Kraus, Leoš Mareš a další známé osobnosti.

Nikdy si do svého počítače **neinstalujte program pro přístup ke vzdálené ploše**.

Pokud chcete investovat své finanční prostředky, navštivte svoji banku – ideálně osobně.

Pravý e-mail od banky **nikdy neobsahuje instruktážní video bankéře**, které by upozorňovalo na problém na vašem účtu.

Praví zaměstnanci banky po vás **nikdy nebudou požadovat přihlašovací údaje k online bankovnictví**.

Praví zaměstnanci banky po vás **nikdy nebudou požadovat citlivé ani bezpečnostní údaje z platební karty**.

**Nikdy nikomu nesdělujte a ani nepřeposílejte bezpečnostní/ autorizační kód**, který vám byl doručen formou SMS zprávy.

Útočník dokáže **napodobit jakékoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu**.

Na vyděračské podvody **nijak nereagujte, neodpovídejte a hlavně nic neplaťte!** Je minimální pravděpodobnost, že by vyděrači měli přístup do vašeho počítače.

**Neotevírejte přílohy vyděračských e-mailů.** V příloze se může skrývat nebezpečný vir, který si otevřením přílohy můžete nainstalovat do svého počítače.

**Neklikejte na odkazy umístěné ve vyděračském e-mailu.** Kliknutím na odkaz si opět můžete nainstalovat nebezpečný vir.

Aby vyděrači nemohli zneužít váš osobní údaj v podobě fotografie, **omezte nahrávání svých fotografií i jiných osobních údajů na internet**.

## 4.2 Nepravdivé zprávy, dezinformace

Generativní umělá inteligence může být **zneužita k výrobě nepravdivých zpráv, obrázků, videí** apod., ovšem může být zneužita i k **napodobení jakéhokoli lidského hlasu**. Běžný posluchač či divák často nedokáže odlišit fotografie či videa zachycující reálnou situaci od produktů vytvořených umělou inteligencí.

*Fotografie osob, které nikdy neexistovaly a vytvořila je umělá inteligence (Zdroj: thispersondoesnotexist.com)*

Umělou inteligenci lze také zneužít pro tvorbu tzv. **dezinformací**, fake news apod., což jsou lživé a nepravdivé zprávy, které jsou záměrně vytvářeny a šířeny internetem.

Nepravdivé zprávy mohou být zcela vymyšlené, ale mohou mít i pravdivý základ, který je doplněn o nepravdivé informace. Jejich cílem je nás vystrašit, ovlivnit naše názory nebo navádět k neetickému, či dokonce trestnímu jednání.

**Narušení demokracie – ovlivnění voleb**

Stále častěji se objevují případy, kdy jsou produkty umělé inteligence (text, fotografie, videa) zneužity k **ovlivňování názorů voličů** – v roce 2023 se v rámci parlamentních voleb na Slovensku objevila nahrávka rozhovoru jednoho z kandidátů, která jej měla dehonestovat a jež byla kompletně vytvořena umělou inteligencí, a to pomocí metody klonování hlasu. V průběhu volební kampaně kandidátů na amerického prezidenta (2024) se objevily jak uměle vygenerované fotografie, tak nahrávky klonovaného hlasu prezidentského kandidáta.

## Ukázka nepravdivých obrázků vytvořených umělou inteligencí

*Fiktivní fotografie papeže Františka vytvořená umělou inteligencí.*

## Ukázka nepravdivých obrázků vytvořených umělou inteligencí

*Fiktivní fotografie Donalda Trumpa při zatýkání vytvořená generativní umělou inteligencí.*

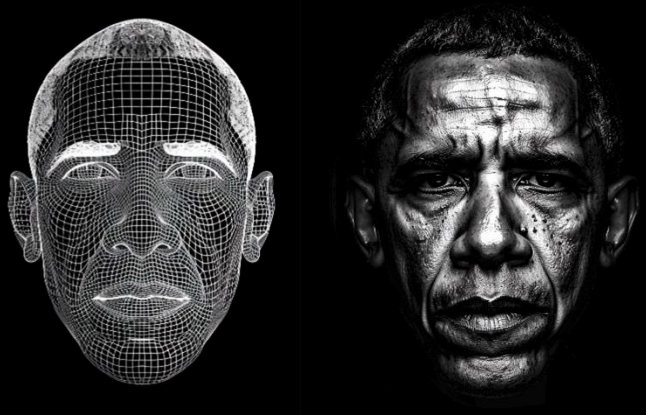

*Fotografie vygenerovaná AI, která má ukázat oblibu Donalda Trumpa u afroamerických voličů.*

## 4.3 Deep fake videa

Velmi nebezpečný druh nepravdivých informací představují videa vytvořená umělou inteligencí, která dokáží věrně napodobit hlas, vzhled, ale také např. mimiku a gestiku konkrétního člověka. Tato videa se označují jako **deep fake videa**. Pro laického uživatele je takřka nemožné rozpoznat, zda se dívá na záznam reality, nebo na uměle vytvořené video.

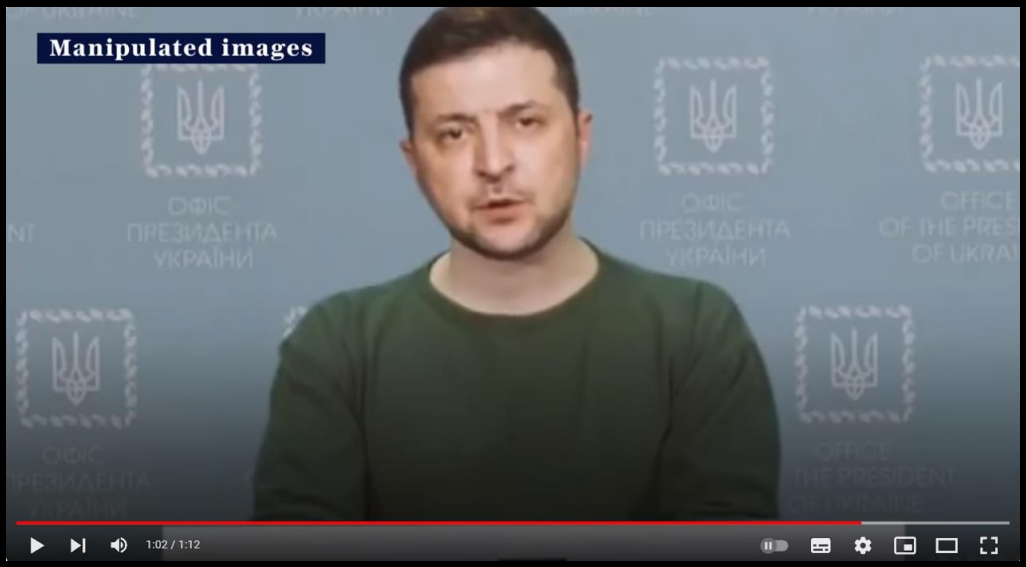
K tomu, aby mohlo deep fake video vzniknout, stačí mít k dispozici co nejvíce fotografií, videí a hlasových záznamů daného člověka. Umělá inteligence je nejprve zanalyzuje a poté dokáže vytvořit jejich klon, který se však chová tak, jak chceme my – např. říká věty, jež mu napíšeme nebo sami vyslovíme.

K vytvoření jednoduchého deep fake videa stačí pouhá fotografie, kterou dokáže umělá inteligence rozhýbat a rozmluvit. Přestože výsledek není dokonalý, laického uživatele dokáže zmást.



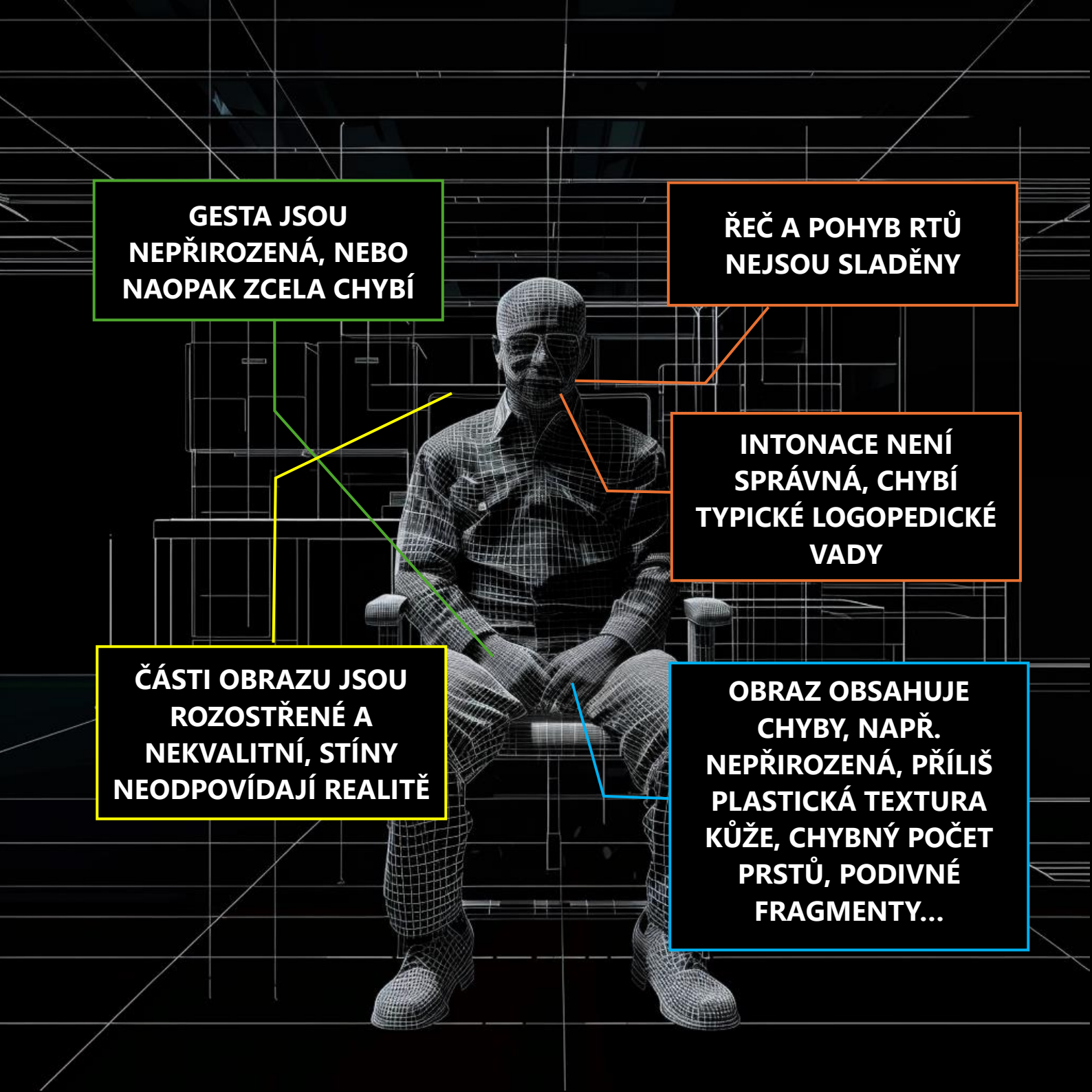
*Umělá inteligence je schopna napodobit mimiku a hlas člověka.*

Deep fake videa se mnohdy využívají v **zábavním** či **pornografickém** průmyslu, stále častěji však bývají součástí různých typů vojenských konfliktů, objevují se v průběhu volebních kampaní a jsou běžným nástrojem podvodů. V průběhu války na Ukrajině se např. objevilo **video s ukrajinským prezidentem, který vyzýval vojáky, aby přestali bojovat a složili zbraně**. V případě podvodů jsou velmi populární uměle vytvořená videa týkající se investicí a slibující zázračné zbohatnutí, přičemž jsou zneužity známé osobnosti (dříve v textu), výjimkou nejsou ani nejrůznější uměle vytvořená videa politiků.




*Ukázka z deep fake videa ukrajinského prezidenta, na kterém ohlašuje, že se vzdává (2022).*

Videa vytvořená umělou inteligencí **bývají většinou nedokonalá**, stačí se zaměřit na detaily: např. **hlas mluvčího a pohyb rtů nejsou sladěny** (tzv. lip sync), některé **části obrazu jsou rozostřené či nekvalitní**, osoba na videu provádí **nepřirozená gesta** nebo se naopak **vůbec nepohybuje a hýbe se pouze obličej**, **intonace není správná** (např. dochází ke stoupání a klesání v řeči), osoby s logopedickými vadami najednou na videu hovoří bezchybně apod.


GESTA JSOU NEPŘIROZENÁ, NEBO NAOPAK ZCELA CHYBÍ
ŘEČ A POHYB RTŮ NEJSOU SLADĚNY
INTONACE NENÍ SPRÁVNÁ, CHYBÍ TYPICKÉ LOGOPEDICKÉ VADY
ČÁSTI OBRAZU JSOU ROZOSTŘENÉ A NEKVALITNÍ, STÍNY NEODPOVÍDAJÍ REALITĚ
OBRAZ OBSAHUJE CHYBY, NAPŘ. NEPŘIROZENÁ, PŘÍLIŠ PLASTICKÁ TEXTURA KŮŽE, CHYBNÝ POČET PRSTŮ, PODIVNÉ FRAGMENTY...

## 4.4 Narušení soukromí pomocí AI

Umělá inteligence bohužel dokáže narušit naše soukromí, což se projevuje např. tak, že někdo **zneužije naši podobu či hlas a vytvoří citlivý materiál** (fotografii, video, zvukový záznam), který nás může poškodit nebo donutit k ukvapené reakci – třeba platbě.

Velmi rozšířené je tzv. **prohazování obličejů na fotografiích či videích** (tzv. **face swap**), k němuž stačí pouze fotografie obličeje. Umělá inteligence nahradí tvář jedné osoby jinou.

Novinkou v této oblasti jsou pak tzv. **svlékací AI aplikace (tzv. deep nude)**, které dokáží z fotografie oblečeného člověka vytvořit fotografii svlečenou. To je velmi nebezpečné – tyto materiály mohou být zneužity k poškození naší pověsti, v případě fotografií dětí může dokonce vznikat dětská pornografie, která je trestná.

*Ukázka „svlékacích aplikací“ (deep nude) v praxi.*
*Vytvářet pornografii zachycující děti je tak velmi snadné.*

# 5. Doporučení a základní pravidla

Pokud budete aktivně využívat nástroje umělé inteligence, držte se následujících pravidel:

**1. Ověřujte si informace** – veškeré informace, jež vám umělá inteligence poskytne, si vždy ověřte. Tato technologie může občas poskytovat nepřesné či neúplné informace.

**2. Chraňte si soukromí** – nikdy do veřejných systémů umělé inteligence nezadávejte své osobní či jiné citlivé údaje. Mohou uniknout a být zneužity.

**3. Dávejte si pozor na nové formy podvodů** – umělá inteligence se bohužel stále častěji zneužívá v rámci různých typů podvodů, ať už jde o podvody využívající zfalšovaná a upravená videa (deep fake), naklonované lidské hlasy či upravené fotografie. **Nenechte se nachytat!**

# 6. Užitečné nástroje umělé inteligence

**Nástroje pro generování/analýzu textu** (tzv. velké jazykové modely)

| | |
|---|---|
| Google Gemini | **gemini.google.com** |
| ChatGPT | **chat.openai.com** |
| Microsoft Copilot | **copilot.microsoft.com** |

**Nástroje pro generování a úpravu obrázků**

| | |
|---|---|
| Midjourney | **www.midjourney.com** |
| Stable Diffusion | **stablediffusionweb.com** |
| Copilot Designer | **www.bing.com/images/create** |
| Photopea | **www.photopea.com** |

**Další užitečné nástroje**

| | |
|---|---|
| DeepL (překladač) | **www.deepl.com/translator** |
| Wisdolia | **www.wisdolia.com** |

# 7. Kde hledat pomoc

**Česká asociace pracovníků linek důvěry**

- **Web:** www.capld.cz

**E-Bezpečí**

- **Web:** www.napisnam.cz

**Linka seniorů**

- **Web:** www.elpida.cz

**CEDMO (Středoevropská observatoř digitálních médií)**

- **Web:** www.cedmohub.eu/cs/medialni-gramotnost/aktivity

**Policie ČR**

- **Web:** www.policie.cz
- **Tel.:** 158

**Transitions**

- **Web:** www.tol.org

# 8. Slovníček

**Deep fake** – jde o technologii, jež využívá umělou inteligenci a pomocí níž lze upravovat videa či zvukové nahrávky, a to tak, že **změní obličej nebo hlas osoby ve videu na někoho jiného**. To znamená, že můžete vidět video, v němž nějaká známá osobnost nebo váš přítel říkají nebo dělají něco, co ve skutečnosti nikdy neřekli ani neudělali. Videa a nahrávky působí velmi realisticky, takže může být těžké poznat, že jsou upravené.

**Deep nude** – označení pro tzv. „svlékací aplikace" umožňující pomocí umělé inteligence vytvořit fotografii svlečeného člověka, a to na základě běžné fotografie.

**Face swap** – technologie „prohazování obličejů" pomocí umělé inteligence, která dokáže nahradit tvář člověka na fotografii či videu libovolnou tváří.

**Generativní umělá inteligence** – druh umělé inteligence, která dokáže vytvářet (generovat) něco nového, např. text, obrázky, fotografie, mluvené slovo, hudbu či video.

**Halucinování** – označení pro situace, kdy umělá inteligence udělá chybu, tzv. halucinuje.

**Kryptoměny** – digitální peníze, které můžete používat na internetu. Nejsou to fyzické peníze, jako jsou bankovky nebo mince, ale počítačové kódy, které se ukládají v počítači nebo na speciálním elektronickém zařízení.

**Velké jazykové modely umělé inteligence** (LLM) – umělá inteligence, která je natrénována na velkém množství textů (Wikipedie, knihy, časopisy apod.) a dokáže s nimi velmi dobře pracovat. Dokáže texty nejenom tvořit, ale také analyzovat či překládat a pomocí textů odpovídá na otázky a konverzuje s námi.

**Dezinformace** – lživé a nepravdivé informace a zprávy, které jsou záměrně vytvářeny a šířeny internetem za účelem oklamání lidí.

**Phishing** – druh nebezpečných komunikačních praktik zaměřených na krádež citlivých osobních údajů – např. PIN kódů, čísel platebních karet, hesel a údajů k bankovnímu účtu či dalších informací, které by mohly být zneužity.

**Scam** – označení pro internetový podvod.

**Vishing** – internetový podvod, jehož základem je podvodný telefonát od tzv. bankéřů či policistů, kteří jsou ale ve skutečnosti podvodníci.

**Smishing** – forma podvodu realizovaná pomocí SMS zpráv, které obsahují internetový odkaz na podvodné www stránky. Podvodníci se tímto způsobem snaží získat osobní nebo citlivé údaje k účtům (přihlašovací údaje, hesla, mobilní klíče apod.).

**Romance Scam** (romantický podvod) – podvod zaměřený na osamělé lidi toužící po přátelství, partnerství, lásce apod. Podvodník, který se vydává např. za lékaře, právníka, vojáka na misi, osloví na internetu (e-mailem, na sociální síti, zprávou v telefonu) podvedenou osobu a následně se od ní snaží vylákat peníze.

Central European
Digital Media
Observatory

Pedagogická
fakulta

Univerzita Palackého
v Olomouci

Tento materiál vytvořil tým Centra prevence rizikové virtuální komunikace (E-Bezpečí) Pedagogické fakulty Univerzity Palackého v Olomouci ve spolupráci s CEDMO při Univerzitě Karlově s podporou společnosti Google.

Google