

# Metodika projektu

Zvyšování digitálních kompetencí  
k úspěšné integraci lidí opouštějících  
výkon trestu



Co-funded by the  
European Union

**Projekt:** “Zvyšování digitálních kompetencí k úspěšné integraci osob  
opouštějících výkon trestu”

**Číslo projektu:** 2022-1-CZ01-KA210-ADU-000083524

# OBSAH

Úvodní slovo, tiráž.....	3
Přípravné práce, instalace modulu.....	4
Úvodní hodina.....	4
Lekce č. 1: Zázemí.....	5
Lekce č. 2: Bezpečnost a ochrana.....	6;7
Lekce č. 3: Řešení problému.....	8
Lekce č. 4: Práce s informacemi.....	9;10
Lekce č. 5: Práce s textem, čísla a obrázky.....	11
Lekce č. 6: Komunikace s roboty.....	12
Lekce č. 7: Opakování.....	13
Ukončení kurzu, zpětná vazba.....	13
Přílohy k metodice:	
Příloha č. 1 Šablona osvědčení pro absolventy.....	14
Příloha č. 2 Dotazník zpětné vazby.....	15;16
Příloha č. 3 Návod k instalaci modulu offline.....	17;18;19



Tato metodika neprošla revizí MFF UK, tudíž za ni MFF UK nenes zodpovědnost

# ÚVODNÍ SLOVO

Dobrý den,

dostává se vám do rukou metodika ke zvyšování digitálních kompetencí lidí ve výkonu trestu odnětí svobody. Metodika slouží jako průvodce prototypem výukového modulu, který v rámci projektu vznikl, a je určená pro výuku lidí ve výkonu trestu odnětí svobody nebo po propuštění v tématu digitální gramotnosti.

Výukový modul jsme vytvořili na základě našich zkušeností, dále pak rešerší domácích i zahraničních zdrojů a především díky výstupům z 2 fokusních skupin složených z klientů a klientek RUBIKON Centra po propuštění z výkonu trestu odnětí svobody.

Metodika by vám společně s prototypem výukového modulu měla pomoci při výuce. Naleznete v ní, co vše musí obsahovat jednotlivé lekce, na co se ptát účastníků a účastnic či návody a doporučení na diskuze a úkoly při výuce. Výukový modul a jeho podobu jsme vytvořili s jednoduchou grafikou. Nechtěli jsme, aby různé grafické efekty odváděly pozornost od výuky.

Modul a metodiku můžete využít při lektorování kurzu. Nezapomínejte dát účastníkům\*icím na začátku dostatek prostoru, aby si na zařízení zkusili procházení, klikání apod. Dejte jim možnost procházet menu a vyzkoušet další jednoduché, základní aktivity, aby se zbavili prvotních obav. Řada z nich z důvodu pobytu ve výkonu trestu neměla podobné zařízení v ruce velmi dlouhou dobu, někteří třeba i více než 10 let.

Přejeme vám hodně úspěchu!

Tým projektu digitalizace, RUBIKON Centrum, z.ú.

---

## METODIKA KE VZDĚLÁVACÍMU KURZU A E-LEARNING BETA MODULU

**Projekt:** „Zvyšování digitálních kompetencí k úspěšné integraci osob opouštějících výkon trestu“

**Číslo projektu:** 2022-1-CZ01-KA210-ADU-000083524



Co-funded by the  
European Union

**Texty:** Michael Daniel Jettmar, Gabriela Hendlová

**Korektury:** Marek Demner

**Grafika:** RUBIKON Centrum, z. ú.

### Partneři projektu:

RUBIKON Centrum, z. ú., web: [www.rubikoncentrum.cz](http://www.rubikoncentrum.cz)

Matematicko-fyzikální fakulta Univerzity Karlovy (MatFyz), web: <https://www.mff.cuni.cz/>

Konzultačné a informačné centrum EDUKOS, web: <https://www.edukos.sk/>

Vydalo RUBIKON Centrum, z. ú. V roce 2024

# PŘÍPRAVNÉ PRÁCE, INSTALACE MODULU

## ÚVODNÍ HODINA

**Lektorující potřebuje pro výuku kurzu:**

- E-learning beta výukový modul
- Prezentaci Power point
- Fixy, lepicí papírky
- Papíry, tužky pro účastníky

Výukový modul si můžete stáhnout podle návodu, který je přílohou č. 3 této metodiky.

**Pokud máte k dispozici internetové připojení, do modulu se dostanete online:**

**<https://rubikonapp.nango.monster/>**

**Přihlašovací heslo: RubikonModul2023**

## Úvodní hodina

**Pracujeme s:** Výukový modul, barevné lepicí papírky, fixy

**Powerpoint:** Slide 1–2

Lektor promítne z výukového modulu slide s představením organizací, následně představí projekt a jednotlivé organizace.

Následuje diskuze s účastníky\*icemi, ze které se **lektorující potřebuje dozvědět:**

- Jak dlouho jsou ve VTOS
- Předchozí zkušenosti s PC/digitálními technologiemi
- Co se chtějí dozvědět

Výstupy ze třetí otázky zapisuje na barevné papírky a lepí na viditelné místo v učebně.

Po této diskuzi má lektorující představu o tom, jaká je úroveň znalostí účastníků\*ic a jak dlouho účastníci\*ice nepracovali s PC; tomu pak může přizpůsobovat jednotlivé lekce.

Lektorující má tím pádem informace, na co se má zaměřit, co probírat více do hloubky a co případně jen zopakovat/ověřit, zda účastníci\*ice skutečně znají.

Na závěr jsou účastníci\*ice vyzváni k zapnutí tabletu a mohou si jej 15 minut procházet a zkoušet. Je dobré je požádat, aby v případě, že fotí, fotky po skončení výuky smazali.

První lekce s názvem Zázemí následuje.

# Lekce č. 1: Z Á Z E M Í

**Pracujeme s:** Výukový modul, prezentace Power point

**Powerpoint:** Slide 3-4

## Práce s výukovým modulem:

- Účastníci\*ice spustí modul, je jim vysvětleno, jak se pohybovat v modulu a jak funguje.
- Následně si projdou slide představení jednotlivých lekcí.
- Dále si účastníci\*e pustí Animaci č. 1 k lekci Zázemí (Digitální identita). Lektorující současně animaci promítá dataprojektorem. V ní je účastníkům\*icím představena digitální identita a stopa. Hlavní poselství: cokoliv, co zveřejníme na internetu, tam již zůstane a je dohledatelné. Pokud zadáváme osobní údaje např. při registraci účtu, dáváme pozor, na jakou stránku údaje zadáváme, volíme silné heslo. Citlivé údaje jsou jméno a příjmení, datum narození, telefonní číslo, adresa. Na internetu zanecháváme v prohlížečích stopu, v historii prohlížeče zůstávají stránky, které jsme navštívili. V průběhu animace přehrávání zastavujeme a diskutujeme o obsahu animace.

**Diskuze: Využití technologií v práci a v běžném životě – lektorující vede s účastníky\*icemi diskuzi na téma „kdy jste využili technologie, kdy očekáváte, že technologie využijete, jak si myslíte, že nám technologie mohou ulehčit život?**

- Účastníkům\*icím je jednoduše vysvětleno fungování zařízení prostřednictvím videa č. 1 k lekci Zázemí - Části PC, které je součástí modulu, které spoluvytvářel MatFyz.

## DIGITÁLNÍ STOPA/1

- **Digitální stopa** (DgS) jsou informace, které po sobě zanechávají konkrétní uživatelé (tedy my) v síťových a lokálních digitálních zařízeních (telefonech, počítačích, serverech apod.), především v online prostředí – tedy na internetu.
- **Pasivní část** DgS = informace o našem připojování se k veřejným WiFi sítím v různých zařízeních, užívání různých modelů a typů zařízení, historie navštívených webových stránek, platby na internetu, informace o naší poloze a další. Naše aktivity a údaje jsou zaznamenávány a ukládány, často bez našeho vědomí.
- **Aktivní část** DgS = informace, které poskytujeme aktivně a vědomě, např. prostřednictvím sociálních sítí, blogů, registracemi, objednávkami, při hledání práce na internetu, při seznamování se přes aplikace apod.
- Postupem času, díky stálému objevování nových technologií a díky množství dostupných informací naše digitální stopa obrovsky roste.
- Dojde-li ke zneužití DgS a osobních údajů, dochází k tzv. krádeži identity nebo její části (např. citlivých osobních údajů). Vlivem zneužití našich údajů pak může docházet ke kyberšikaně, kyberstalkingu (pronásledování).
- Prevence = občasná kontrola své DgS, používání více profilů, více emailových schránek, přihlašovacích jmen a využívání digitálních nástrojů, např. program pro ukládání hesel, používání anonymního prohlížeče apod.

## Práce s výukovým modulem:

Na závěr lekce si účastníci\*ice vyzkouší své znalosti formou kvízu, který patří k lekci č. 1.

## Zdroje:

1)Text vychází z IT slovníku; [https://it-slovník.cz/pojem/digitalni-stopa/?utm\\_source=cp&utm\\_medium=link&utm\\_campaign=cp](https://it-slovník.cz/pojem/digitalni-stopa/?utm_source=cp&utm_medium=link&utm_campaign=cp)

## Lekce č. 2: BEZPEČNOST A OCHRANA

**Pracujeme s:** Výukový modul, prezentace Power point

**Powerpoint:** Slide 5-10

**Výukový modul:** Účastníci\*ice si pustí na začátku lekce animaci č. 2 k lekci Bezpečnost a ochrana, kterou lektorující zároveň promítá. Animace pomáhá vysvětlit důležitost silného hesla, je zde přirovnání s klíči od dveří bytu. Je ukázáno, že je nutnost dbát na bezpečnost a ochranu počítače a jaké mohou být následky, pokud nám unikne heslo.

### BEZPEČNOST V ONLINE PROSTŘEDÍ

Během úvodní diskuze hledání dalších paralel bezpečnost online x offline.

#### Následuje práce s tabletem:

- Zapnout tablety
- Otevřít modul (OffLine Browser)
- Kliknout na 6. lekci
- KPBI video

Následuje shlédnutí videa č. 2 KPBI zaměřené na bezpečné heslo.

**Diskuze:** „Co je pro mě bezpečné heslo, jaká hesla volím?“

Následně se lektorující zeptá, na další způsoby zabezpečení. Povinné pojmy: dvoufázové ověření, odemčení gestem/kódem/rozpoznáním obličeje/otiskem prstu.

### ANTIVIR

**Diskuze:** Začneme diskuzí na téma zkušenosti s antivirem, navážeme výkladem:

- „Ochránce“ zařízení. Zachycuje a zastavuje viry a malware
- Kontroluje všechny soubory, programy
- Pokud najde něco závadného, zastaví to
- Někdy už je v zařízení nainstalovaný
- Verze placená i zdarma
- Např. Avast, Eset

### AKTUALIZACE

- Pravidelné „opravy“ nebo vylepšení
- Odstraňují „nemoci“ a chyby, díky kterým by zařízení nefungovalo správně
- Po aktualizaci je zařízení chráněno před aktuálními hrozbami
- Bez aktualizace nemusí zařízení fungovat správně
- Před aktualizací provádíme zálohování

## Lekce č. 2: BEZPEČNOST A OCHRANA

### ÚTOKY NA UŽIVATELE

- Útoky zaměřené na uživatele
- Útoky zaměřené na naše data

**PHISHING** je podvodná technika, jejímž účelem je zjistit informace o naší identitě, hesla, čísla karet apod. Útočníci nejčastěji napodobují populární sociální sítě, aukční weby, online platební portály. Získané údaje zneužívají k vykradení peněz z účtu, k podvodným půjčkám apod.

**PHARMING** je obdobná profesionální podvodná technika, jejímž důsledkem je přesměrování na weby, které vypadají např. jako webové rozhraní naší banky. Cílem je opět z nás vylákat data, nejčastěji přihlašovací údaje.

**SPAM** je nevyžádaná pošta, kterou naše emailové schránky již umí řešit. Proto tyto zprávy často „padají do SPAMu“.

**SPAM** je nositelem virů, nejčastěji trojských koní. Emaily se týkají hubnutí, půjček apod.

### PREVENCE PŘED ÚTOKY

- Od koho je email, kdo a proč chce naše údaje, styl, jak je email napsaný
- Stahujeme aplikace jen ze známých zdrojů
- Potvrzujeme, že nejsme robot

### INTERNETOVÉ BANKOVNICTVÍ

Slouží k provádění bankovních převodů přes internet, např. k úhradě faktur mobilních operátorů.

Nejprve je nutné zřídit si bankovní účet v některé bance, pokud jste v exekucích, před vstupem do osobního bankrotu je nutný chráněný účet.

Při založení bankovního účtu obdržíme (jako klienti\*ky banky) přihlašovací údaje, kterými se přihlašujeme přes bankovní domovskou stránku, a přístup k aplikaci do telefonu.

Prostřednictvím internetového bankovníctví můžeme kontrolovat bankovní převody na našem účtu, např. zda jsme obdrželi mzdu a zda obdržená výše mzdy odpovídá údajům zaměstnavatele.

Nikdy se nepřihlašujeme do internetového bankovníctví prostřednictvím počítačů v knihovnách nebo internetových kavárnách, protože bychom mohli přijít o peníze na svých bankovních účtech.

Při přihlašování přes webové stránky bank využívajících službu internetového bankovníctví musíme zkontrolovat, zda je na začátku adresy webové stránky <https://>. Pokud ne, znamená to, že stránka není dostatečně zabezpečená a neměli bychom se přes ni přihlašovat; v takovém případě je na začátku adresy webové stránky <http://>.

### ONLINE PLATBY

- Platba převodem
- Platba online kartou
- Platba přes platební bránu PayPal, GoPay
- Platba Bitcom

### ONLINE NÁKUPY

**Diskuze:** lektorující nejdříve diskutuje s účastníky\*icemi na téma výhody a nevýhody nakupování online.

- Snažíme se vždy vybírat prověřené obchody – jak je ověřím?
- Recenze na internetu
- Proces nákupu

### ONLINE HRANÍ

Kdysi: Kasina, kam musel člověk osobně dojít

Dnes: Hraní přes internet, vklad rovnou z účtu

**RIZIKOVÉ HRANÍ** je pro nás takové, které narušuje či poškozuje hráčův osobní, rodinný či pracovní život a zcela mění způsob, jakým tráví volný čas.

## Lekce č. 3 Řešení problému

**Pracujeme s:** Výukový modul, prezentace Power point

**Powerpoint:** Slide 11-12

**Diskuze:** Lektorující v úvodu vyzve k diskuzi na témata:

- Co se nám v životě může rozbít/porouchat a jak/kde to řešíme
- Co se může stát se zařízením a jak/kde to řešit

Z diskuze vyplynou druhy poruch, pravděpodobně zazní: prasklý display, NTB se přehřívá, neaktualizovaná verze systému.

- Následně možnosti, jak to řešit: sám, odnést do opravny
- Na závěr, kde to řešit: sám, u kamaráda, v servisu
- Řešení sám = např. tutoriál na internetu, servis = nutná úhrada

Dále **diskutujeme** o pojmech:

- Tovární nastavení (co to udělá, kdy ho volíme jako vhodné řešení)
- Restart (opět - co to udělá, kdy je vhodným řešením)

**Výukový modul:** Účastníci\*ice si probrané pojmy zobrazí ve výukovém modulu.

**Cvičení:** Účastníci\*ice vytvoří snímek obrazovky, který uloží na plochu

Obvykle dochází k opakování informací z předchozí lekce – problémem může být i zavirovaný počítač.



## Lekce č. 4: PRÁCE S INFORMACEMI

**Pracujeme s:** Výukový modul, prezentace Power point

**Powerpoint:** Slide 14–21

### NEBEZPEČÍ V DOBĚ DIGITÁLNÍ

Existuje několik druhů informací. Informace jsou buď správné a relevantní, nebo nepravdivé a škodlivé. Škodlivých druhů informací rozlišujeme 2 typy. Prvním z nich jsou „hoaxy“, které pro člověka uvědomělého a znalého působí od první chvíle, kdy se s nimi setká, jako žert.

#### HOAX [1]

Anglické slovo HOAX [ˈhouksː] v překladu znamená: falešnou zprávu, mystifikaci, novinářskou kachnu, podvod, poplašnou zprávu, výmysl, žert, kanadský žertík.

V počátcích internetu se nejčastěji šířily poplašné zprávy (hoaxy), které varovaly před údajně velmi nebezpečným počítačovým virem. Jak začaly počítače pronikat do běžného života, přenesly se do tohoto prostoru i fámy, drby, žertíky, které dříve kolovaly například ústně.

#### Jak HOAX poznáme?

Typický text poplašné zprávy obsahuje většinou tyto body:

- Snaží se přesvědčit svojí důležitostí (Šokující informace, nové nebezpečí, naléhavá pomoc...).
- Důvěryhodné zdroje varují (Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů, např. "FBI varuje...", "Zdravotnická organizace zjistila" atd...)
- Tajná informace unikla (Údajná informace, o které oficiální média mlčí a nesmí se o ní mluvit, ale autor zprávy ji objevil a vyzývá k jejímu sdílení.).
- Výzva k dalšímu rozeslání (Tento bod hoax vždy obsahuje! Je hnacím motorem pro další šíření. Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechnou. Právě proto se tyto nesmysly lavinovitě šíří.).

Jako hoax můžeme také označit šířenou zprávu, která obsahuje nepřesné, zkreslující informace, účelově upravené polopravdy nebo směsku polopravd a lží.

Zatímco hoaxy vznikají spíše jako žert, druhý typ, tzv. fake news, často přichází z dezinformačních webů, které se snaží ovlivnit veřejné mínění cíleným šířením nepravd. Oba typy manipulativních zpráv ale škodí stejně. Vyvolávají paniku a šíří strach. Zároveň mohou pomáhat extremistickým skupinám, nebezpečné rady mohou uškodit a ublížit, často poškozují konkrétní lidi, ale i instituce a firmy, které měly do té doby dobrou pověst, a v neposlední řadě zahlcují naše emailové schránky.

### ÚTOKY V ONLINE PROSTŘEDÍ

**KYBERŠIKANA** - šikana v online prostředí, na sociálních sítích; útok na psychiku - vydírání/nucení k něčemu, vyhrožování zveřejněním informací, fotek.

**KYBERGROOMING** - nebezpečná snaha o manipulaci; cílem je osobní schůzka za účelem napadení, sexuálního zneužití apod.

**KYBERSTALKING** - nebezpečné pronásledování online, útočník využívá online technologie k dlouhodobému, opakovanému a stupňujícímu se kontaktování; pronásleduje svou oběť za účelem vyvolání strachu o soukromí, zdraví či život.

**SEXTING** - rizikové sdílení/posílání intimních fotek; primárně zaměřeno na mladistvé, riziko zneužití fotek, vydírání.

## Lekce č. 4: PRÁCE S INFORMACEMI

### JAK SE BRÁNIT?

**Diskuze:** Lektorující položí otázku „Jak si myslíte, že se tyto problémy řeší nebo dají řešit?“ Poté vede diskuzi.

### KYBERŠIKANA

- Nebud'te přehnaně důvěřiví, nikdy nevíte, kdo je druhé straně.
- Nesděľujte citlivé informace (osobní údaje, osobní fotografie, hesla k účtům, apod).
- Respektujte ostatní uživatele.
- Seznamte se s pravidly služeb internetu a GSM sítí.
- Zablokujte útočníkovi možnost přístupu k vám, změňte svou virtuální identitu.
- Ukončete s útočníkem komunikaci, nechtějte se pomstít.
- Pokuste se útočníka odhalit, identifikovat.
- Ušchovejte si důkazy pro možné vyšetřování (zprávy, videozáznamy, odkazy na weby, blogy...).

### KYBERGROOMING

- Předejít kybergroomingu mohou rodiče důslednou kontrolou činnosti svých dětí v internetovém prostředí. V tomto případě je třeba odložit předsudky o narušování soukromí svého dítěte a na celou věc nahlížet tak, jako by bylo dítě hlídáno v hustém silničním provozu – zde by každý rodič své dítě držel pevně za ruku a raději vodil. V internetovém provozu by to mělo být obdobné.

### SEXTING

- Každý by měl opravdu důkladně zvážit, komu a jaké intimní informace a materiály poskytuje.

### DALŠÍ POJMY

**Elektronický podpis** - Elektronický podpis je v informatice označení specifických dat, které v počítači nahrazují klasický vlastnoruční podpis, respektive ověřený podpis. Je připojen k datové zprávě nebo je s ní logicky spojen, takže umožňuje ověření totožnosti podepsané osoby ve vztahu k datové zprávě.

**Datová schránka** - Elektronické úložiště, které je určeno k doručování elektronických dokumentů mezi orgány veřejné moci na straně jedné a fyzickými a právníckými osobami na straně druhé.

**Elektronický recept (e-recept)** - Recept od lékaře v elektronické podobě. Lékař ho může zaslat na email, jako sms do mobilu nebo do aplikace v mobilu.

### BLUETOOTH, PAMĚŤOVÉ ZAŘÍZENÍ

**BLUETOOTH** - Nástroj pro bezdrátovou komunikaci propojující dvě a více elektronických zařízení. Zvýšil se jeho dosah, který v otevřených prostorách činí až neuvěřitelných 200 metrů a v uzavřených prostorách až 40 metrů, což značně zvyšuje nejen možnosti poslechu hudby, ale třeba také ovládání a vzájemné komunikace mezi elektronickými zařízeními nebo třeba mezi jednotlivými prvky chytré domácnosti.

**USB FLASH DISKY, EXTERNÍ DISKY** - Zařízení s větší pamětí sloužící k uchovávání/přenášení souborů.

## Lekce č. 5: PRÁCE S TEXTY, ČÍSLY A OBRÁZKY

**Pracujeme s:** Výukový modul, prezentace Power point

**Powerpoint:** Slide 22-31

**Výukový modul:** Účastníci\*ice ve výukovém modulu vidí loga aplikací. Lektor nejdříve mluví o textových souborech a kancelářských aplikacích.

**Hlavní sdělení:** Mezi kancelářské aplikace patří textový editor, tabulkový procesor, prezentační program. Placené licence těchto programů se nazývají Microsoft Office. Pokud si kupujeme nové zařízení, bývají jeho součástí. Pokud nejsou, můžeme si je pořídit. Cena je odvozena podle počtu zařízení, pro které je licence určena. Pokud chceme bezplatnou verzi, můžeme si pořídit např. Libre Office. Programy se od sebe liší vzhledem a funkcemi. Pozor, pokud někdo pracuje se zařízením tím stylem, že si pamatuje, co kde v jakém programu je – u Libre office jsou některé funkce v programu na jiném místě, než v originál Microsoft Office programech, proto to může některé uživatele zmást.

**Diskuze:** Zkušenosti účastníků\*ic s kancelářskými programy.

Lektorující dále mluví o ukládání souborů. Kromě pevných disků můžeme využívat i online úložiště, tzv. cloudy. Výhodou je, že jsou přístupné v podstatě odkudkoliv, máme-li připojení k internetu. Naopak jejich nevýhodou je, že jsou tak snadno napadnutelné a může dojít k úniku dat při sdílení souboru.

U sdílených dokumentů můžeme nastavit uživatelská práva, a to na možnost pouze zobrazit nebo editovat dokument. U online dokumentů je výhoda, že je může editovat v jednu chvíli více uživatelů najednou.

Kancelářské programy obsahují vždy šablony dokumentů, které je možno použít. Jedná se například o šablony životopisů, rozpočtů, prezentací a dalších dokumentů.

Při psaní textů můžeme využívat hlídání gramatických chyb, kdy se nám v dokumentu zobrazí, pokud uděláme gramatickou chybu. U zařízení, jako je mobilní telefon, lze nastavit používání automatických oprav textů. Jako doplněk lze využívat překladače textů (např. Deepl nebo Google Translator).

**Cvičení:** Napište libovolný text do textového editoru a uložte jej na plochu.

**Autorské právo<sup>1</sup>** - V dnešní době existuje mnoho placených legálních online platforem s přístupem k autorským dílům (zejména filmům a seriálům) jako je Netflix, HBO GO, Disney+ atd. Další možností, jak získat počítačové soubory, je přístup přes datová úložiště typu Ulož.to. Zde jsou dostupná díla, která mají často nejasný původ a zřejmě chybějící licenční oprávnění k jejich stažení, zato jsou dostupná zdarma. A konečně, existují také weby, kde nahraný autorský obsah je zcela zjevně nelegální.

<sup>1</sup> Zdroj: <https://www.epravo.cz/top/clanky/nelegalni-stahovani-autorskych-del-z-pohledu-trestniho-prava-115052.html>

## Lekce č. 6: KOMUNIKACE S LIDMI A S ROBOTY

**Pracujeme s:** Výukový modul, prezentace Power point

**Powerpoint:** Slide 32-46

**Výukový modul:** Účastníci\*ice si přehrají animaci k lekci, dále si prohlédnou ukázkou chatbota v modulu.

**Hlavní myšlenka:** V dnešní době jsou využíváni ke komunikaci na některých webových stránkách tzv. chatboti, kteří s návštěvníky komunikují automatizovaně. Pokud komunikujeme s chatbotem, znamená to, že na druhé straně nesedí někdo, kdo by s námi komunikoval, ale jedná se o naprogramovaného robota, připraveného zodpovědět naše dotazy nebo nás provést tématem daného webu. V chatbotu tedy buď volíme přednastavené možnosti, nebo píšeme dotazy.

### UMĚLÁ INTELIGENCE

V současné době roste popularita umělé inteligence. Na stránkách, kde je dostupná umělá inteligence, např. <https://openai.com/>, je možné s umělou inteligencí komunikovat. Můžeme si po zadání požadavku nechat vygenerovat texty, životopisy, výkladové texty a další. Umělá inteligence funguje na bázi strojového učení. Využívá se také v počítačových hrách.

V rámci lekce jsou pak účastníkům\*icím ukázány další typy robotů, které jsou v dnešní době dostupné – např. ve zdravotnictví, v terapii, ve školách apod.

Cvičení: Účastníci\*ice mohou napsat svůj požadavek na obrázek, který nechají lektorující vygenerovat umělou inteligencí a přinesou jej na další hodinu.

### NADSTAVBA LEKCE

Na konci této lekce mohou lektorující prezentovat např. aplikace pro komunikaci se školami (Bakaláři, EduPage), případně programy vhodné pro výkon zaměstnání v různých oborech - program pro truhláře, program pro tvorbu návrhů interiéru, skladové hospodářství a další.

## Lekce č. 7: OPAKOVÁNÍ

**Pracujeme s:** Prezentace Powerpoint, Výukový modul, formuláře zpětné vazby

**Powerpoint:** Slide 47-61

V rámci poslední, opakovací lekce je s účastníky\*icemi zopakováno to nejdůležitější z probraných lekcí. Lektorující k tomu využívá pojmy z prezentace. Opakování je vedeno formou diskuze.

- Jaké znáte způsoby zabezpečení zařízení?
- Co je antivir?
- Do poznámkového bloku napište silné heslo.
- Co jsou fake news, jak se před podobnými věcmi chránit?
- Jaké znáte komunikační aplikace a co všechno umí?
- Uveďte alespoň jednu sociální síť. Co to vlastně jsou sociální sítě?
- Co je kybergrooming, jak ochránit děti před nástrahami internetu?
- Co je to e-recept?
- Jak přenášíme velké soubory mezi zařízeními?
- Jaké známe programy pro práci s texty a čísly? Co vše umí?
- Uveďte alespoň nějaké portály pro hledání zaměstnání. Co vše stránky nabízí?
- Jak lze platit na internetu
- Co je chatbot, jaké jeho využití?
- K čemu slouží cloudová úložiště, jaké jsou jejich výhody a nevýhody?

Ještě před ukončením lektorující ověří, že jsou zodpovězeny všechny dotazy skupiny.

### UKONČENÍ KURZU, ZPĚTNÁ VAZBA

Po shrnutí informací z kurzu je účastníkům\*icím rozdán formulář zpětné vazby.

#### **Formulář obsahuje následující body:**

1. Moje spokojenost s proběhlým kurzem (známkování jako ve škole, 1 - 5)
2. Náročnost probíraných témat (škála 1 – 4; kdy 1 je minimální a 4 maximální)
3. V rámci kurzu se mi nejvíce líbilo (textová odpověď)
4. Nejdůležitější pro mě byla témata (textová odpověď)
5. Co mi přišlo zbytečné (textová odpověď)
6. Pokud by se kurz realizoval v budoucnu, je něco co byste udělal jinak, jaká témata by měla zaznít, která témata vypustit, jak pracovat s tabletem, případně další vaše nápady (textová odpověď)
7. Prostor pro vaše náměty a komentáře (textová odpověď)

**Vzor formuláře zpětné vazby naleznete v přílohách (příloha č. 2) metodiky.**

Účastníkům\*icím, kteří absolvovali všechny lekce a odevzdali vyplněný formulář zpětné vazby, předáváme Osvědčení o absolvování kurzu. Toto osvědčení obsahuje jméno a příjmení účastníka\*ice, datum narození, název kurzu a časovou dotaci, jména lektorujících. V příloze této metodiky naleznete šablonu pro inspiraci (Příloha č. 1)

## PŘÍLOHY K METODICE

Příloha č. 1: Vzor osvědčení o absolvování kurzu



# OSVĚDČENÍ

o absolvování vzdělávacího kurzu v rámci projektu  
Zvyšování digitálních kompetencí k úspěšné integraci osob  
opouštějících výkon trestu v rozsahu 7 lekcí

---

Jméno účastníka\*ice kurzu, datum narození

Vystaveno v **místo** dne **datum**

---

Jméno, podpis lektora



---

Jméno, podpis lektora

Projekt: Zvyšování digitálních kompetencí k úspěšné integraci osob opouštějících výkon trestu  
Číslo projektu: 2022-1-CZ01-KA210-ADU-000083524  
Aktivita projektu: Aktivita 3. Příprava a testování Prototypu č. 2 a vývoj "E-learning Beta" nástroje

# PŘÍLOHY K METODICE

## Příloha č. 2 - Dotazník zpětné vazby

### DOTAZNÍK ZPĚTNÉ VAZBY

*Kurzu Zvyšování digitálních kompetencí k úspěšné integraci osob opouštějících výkon trestu*

**Termín konání:**

**Místo konání:**

Za účelem vyhodnocení kvality proběhlého vzdělávací kurz Vás žádáme o její zhodnocení. Vyplněním a zodpovězením následujících otázek přispějete k zachování a případně i ke zlepšení odborné úrovně vzdělávání.

#### 1, Moje spokojenost s tímto vzdělávacím kurzem je



#### 2, Náročnost probíraných témat pro mě byla

**MINIMÁLNÍ**

*(nebylo to náročné,  
dalo se to pochopit)*

1

2

3

4

**MAXIMÁLNĚ**

*(hodně náročné,  
neporozuměl\*a jsem více  
věcem)*

#### 3. V rámci kurzu se mi nejvíce líbilo (vypište)

.....

.....

.....

#### 4. Nejdůležitější pro mě byla témata (vypište):

.....

.....

#### 5. Co mi přišlo zbytečné (vypište):

.....

.....

Příloha č. 2 - Dotazník zpětné vazby, 2. strana

**6. Pokud by se kurz realizoval v budoucnosti, je něco, co byste udělali jinak, jaká témata by měla zaznít nebo naopak, která témata vypustit, jak pracovat s tabletem, případně další vaše nápady - vypište:**

.....

.....

.....

.....

.....

.....

.....

.....

.....

**7. Prostor pro Vaše další náměty a komentáře.**

*Děkujeme Vám za vyplnění hodnotícího dotazníku.*

Lektorská dvojice .....



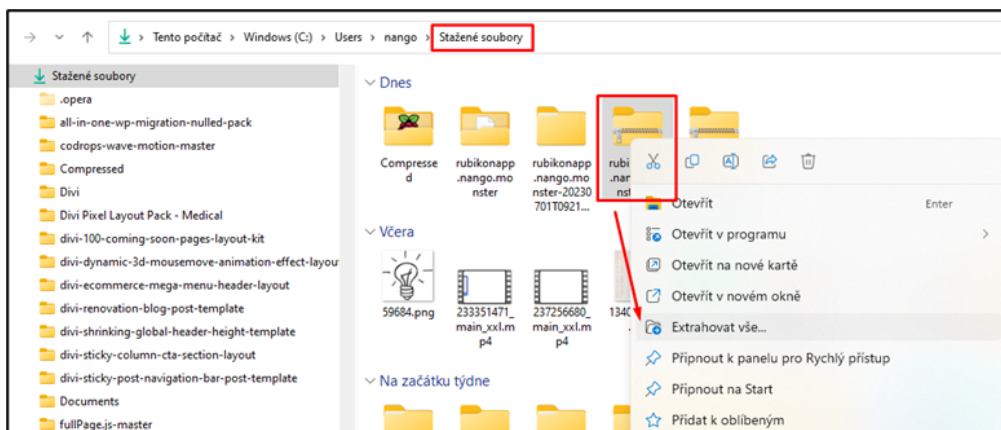
## PŘÍLOHY K METODICE

### Příloha č. 3: Postup pro instalaci offline verze výukového modulu

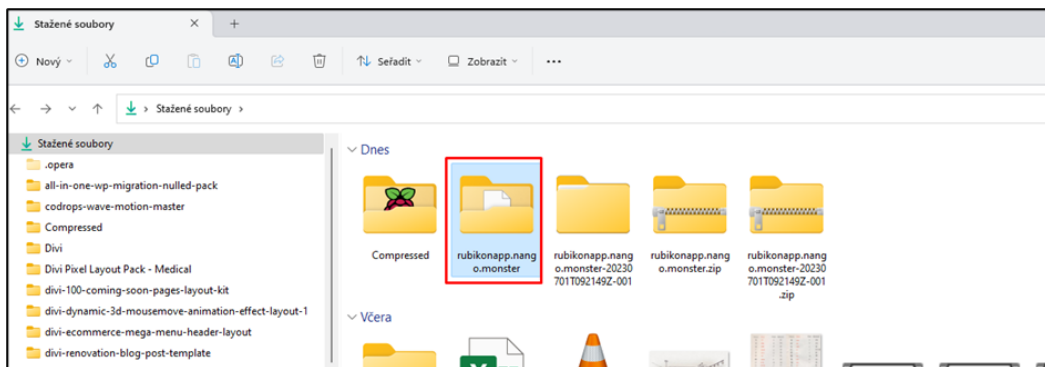
**Spuštění online verze modulu na adrese: RUBIKONAPP.NANGO.MONSTER**

### Instalace modulu pro offline výuku:

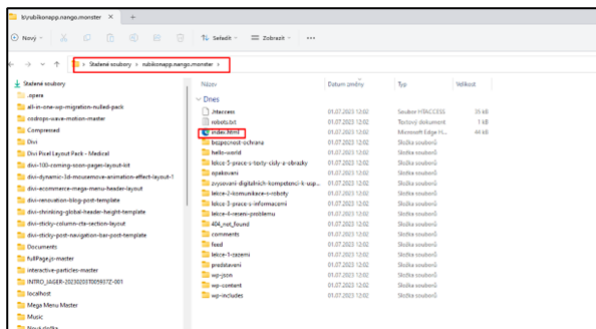
- 1) Otevřeme si umístění souborů na Google Drive: [kliknete zde](#)
- 2) Otevře se vám v prohlížeči umístění, kde stáhnete složku "[rubikonapp.nango.monster.zip](#)" [zde](#)



- 4) Poté se nám vytvoří klasická složka s názvem **rubikonapp.nango.monster**



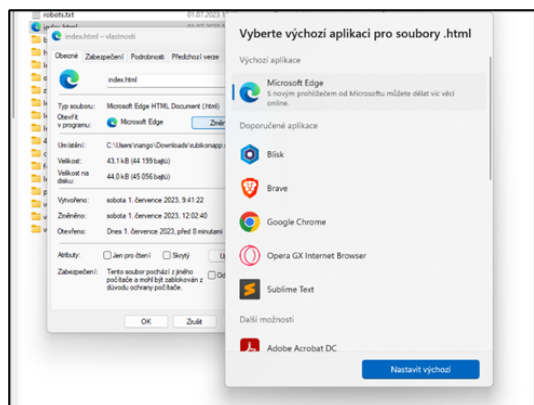
- 5) Otevřeme jí a najdeme soubor „index.html,” pokud nebude k nalezení, hledejte soubor pouze s názvem „index.“



## PŘÍLOHY K METODICE

Pokud ji uvidíte jako ikonu prohlížeče (Chrome, Edge, Opera..) je to v pořádku, pokud bude ikonou programu Word (případně jakéhokoliv jiného programu) postupujte následovně:

- Klikněte pravým tlačítkem myši na soubor „index“ a zvolte „vlastnosti“ a změňte vlastnost souboru na váš prohlížeč.
- Poté otevřeme soubor **index.html** tak, že na něj dvakrát klikneme – Tím se otevře internetový prohlížeč s modulem.
- Funkčnost offline verze můžete vyzkoušet, pokud vypnete modem nebo po vypojení ethernet kabelu.



- 1) Stáhněte si tento soubor (zazipovaný): [odkaz zde](#)
- 2) Stažený soubor uložíme na disk v zařízení, kde budeme modul využívat.
- 3) Následně klikneme pravým tlačítkem myši a zvolíme možnost exportovat.
- 4) Po skončení exportu si v nově vzniklé složce, která má stejný název, pouze chybí přípona .zip vyhledáme soubor s názvem **index.html**.
- 5) Následně u nabídky složky **index.html** vybereme „vlastnosti“ a nastavíme „otevřít v prohlížeči Opera, Chrome, Internet Edge“ podle toho, jaký prohlížeč preferujete.

a) Alternativní možnost provedete kliknutím pravého tlačítka myši na soubor **index.html**, poté otevřít.

b) Následně zvolíme jeden z preferovaných prohlížečů.

Poté otevřeme soubor **index.html**, který nás dostane na hlavní stránku webu (resp. Offline modulu).

## NÁSTROJ ONLINE PRO EXTRAKCI ZIP SOUBORU

Použijte v případě, že nemáte nainstalovaný program WinZip

<https://zipextractor.app/>

## XAMP PRO OFFLINE WORDPRESS NA ANDROID

<https://www.apachefriends.org/download.html>

## PŘÍLOHY K METODICE

### JAK SPUSTIT OFFLINE VERZI MODULU NA ANDROID TABLET HUAWEI

Pro náš projekt, jehož stěžejní součástí byla realizace 2 běhů kurzů ve věznicích jsme po zvážení několika možností vybrali jako nejvhodnější možnost vývoje a následného používání formu WordPress webu. Abychom mohli spustit lokální WordPress web na Tabletech značky Huawei s Androidem bez internetového připojení je potřeba následující postup:

- 1) Stáhněte si a nainstalujte aplikaci **XAMPP pro Android** z oficiálních stránek společnosti „Apache Friends.“ Tato aplikace vám umožní spustit lokální webový server na vašem tabletu.
- 2) Po instalaci XAMPP spusťte aplikaci a povolte potřebná oprávnění (pokud je to vyžadováno).
- 3) Ve spuštěné aplikaci XAMPP klepněte na tlačítko "Start" u modulu Apache. Tím spustíte webový server na vašem tabletu.
- 4) Nyní musíte přenést soubory WordPressu na svůj tablet. Stáhněte si nejnovější verzi WordPressu z oficiálních stránek WP a přeneste ji do paměti tabletu pomocí USB kabelu nebo jiného způsobu přenosu souborů.
- 5) Jakmile dojde k přenesení všech souborů WordPress na tablet, přejděte do složky, do které jste soubory uložili.
- 6) Následně rozbalte soubory WordPressu, pokud jsou v archivu.
- 7) Posledním krokem je zkopírování celé složky WordPress do složky "htdocs" v XAMPP.
- 8) Cesta k této složce by je buď taková: "/sdcard/xampp/htdocs" nebo podobně znějící. Tím dojde k přesunu souborů WordPressu na správné místo tak, aby mohl běžet na webovém serveru XAMPP.
- 9) Otevřte správce souborů a přejděte do složky "htdocs". Najděte složku WordPressu, kterou jste před tím zkopírovali, a změňte její název na jednoduchý název (například "wordpress"). Tím dojde k usnadnění přístupu k webu.
- 10) Spusťte webový prohlížeč na tabletu a do adresního řádku zadejte "localhost/wordpress" (pokud jste změнили název složky WordPressu, použijte ten nový název). Tím se spustí instalace WordPressu.
- 11) Postupujte podle instrukcí na obrazovce, dokud nebude instalace WordPressu kompletní. Můžete si vybrat název webu, uživatelské jméno a heslo pro administrátorský účet atd.
- 12) Jakmile bude instalace dokončena, můžete spustit výukový modul v offline režimu.

*Nezapomínejte na to, že je důležité mít na paměti, že tento postup je vhodný pro testování nebo vývoj na lokálním zařízení, ale pro provoz veřejně dostupného webu budete potřebovat internetové připojení a hostování na serveru.*

[www.rubikoncentrum.cz](http://www.rubikoncentrum.cz)

