KYBERNETICKÁ HYGIENA PRE STREDNÉ ŠKOLY

MODUL 3

Efektívne bránenie sa pred kybernetickými hybridnými hrozbami, ktorým čelia študenti stredných škôl ako používatelia internetu

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-0000

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

KYBERNETICKÁ HYGIENA PRE STREDNÉ ŠKOLY

MODUL 3
Efektívne bránenie sa pred kybernetickými hybridnými hrozbami, ktorým čelia študenti stredných škôl ako používatelia internetu

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-0000

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

MODUL 3
„Efektívne bránenie sa pred kybernetickými hybridnými hrozbami, ktorým čelia študenti stredných škôl ako používatelia internetu"

Modul sa venuje analýze aktuálnych foriem hybridných hrozieb v kybernetickom priestore, ktoré sú zamerané na mladých používateľov – najmä formou dezinformačných kampaní, manipulácie verejnej mienky a zneužívania sociálnych sietí. Študenti sa naučia rozpoznávať rôzne typy nepravdivého alebo manipulatívneho obsahu (napr. fake news, deepfake), osvojia si základy mediálnej gramotnosti a kritického myslenia a získajú nástroje na overovanie pravdivosti informácií. Modul prepája právny, spoločenskovedný a technický rozmer tejto problematiky, čím vytvára ucelený základ pre aktívnu digitálnu odolnosť. Modul bude vedený interaktívnou formou, ktorá kombinuje odborný výklad s diskusiou, analýzou prípadových štúdií a zapojením študentov stredných škôl do praktických aktivít zodpovedajúcich ich veku a skúsenostiam.

Stručná osnova:

1. Čo sú hybridné hrozby a ako sa prejavujú v online prostredí

- vymedzenie pojmov hybridné hrozby a dezinformácie

2. Typy dezinformácií a techniky manipulácie

- vymedzenie pojmov clickbait, cherry-picking, deepfake
- interaktívna aktivita: „lovci fake news" (tímová práca v rámci ktorej budú študenti vyhľadávať "fake news")

3. Základy kritického myslenia

- overovanie zdrojov, analýza zámeru autora, identifikácia propagandy

4. Právne a etické dôsledky šírenia dezinformácií

- trestnoprávna a občianskoprávna zodpovednosť, spoločenský vplyv
- diskusia: Sloboda prejavu verzus zodpovednosť za zdieľaný obsah

1. METODIKA MODULU 3

1.1 Charakteristika modulu 3 „Efektívne bránenie sa pred kybernetickými hybridnými hrozbami, ktorým čelia študenti stredných škôl ako používatelia internetu"

Modul „Efektívne bránenie sa pred kybernetickými hybridnými hrozbami, ktorým čelia študenti stredných škôl ako používatelia internetu" predstavuje súčasť kurzu Kybernetická hygiena pre stredné, ktorý sa skladá z troch modulov. Jeho cieľom je podporiť u žiakov rozvoj kritického myslenia, digitálnej gramotnosti a právneho povedomia v oblasti kybernetických hybridných hrozieb. Počet týchto hrozieb vzrastá, spoločnosť má príliš veľa informácií, ktoré musí filtrovať a preto narastá potreba naučiť študentov zručnostiam, ktoré im dokážu odhaliť tieto hrozby..

Tematická orientácia modulu vychádza zo základných princípov kritického hodnotenia informácií. Dôležitou súčasťou je aj zdôraznenie zodpovednosti pri vytváraní a šírení online obsahu, ako aj pochopenie hraníc slobody prejavu v kontexte škodlivých a manipulatívnych informácií. Obsah modulu reaguje na aktuálne výzvy, akými sú masívny rozvoj sociálnych sietí, rýchle šírenie dezinformácií, používanie umelej inteligencie na generovanie manipulatívneho obsahu, kybernetické hrozby a zraniteľnosti digitálnych účtov, ktoré môžu ovplyvniť bezpečnosť, reputáciu a informačné prostredie študentov v kyberpriestore. Modul kladie dôraz na to, aby žiaci nadobudli schopnosť bezpečne sa orientovať v digitálnom prostredí, rozpoznali rizikové vzorce správania a osvojili si praktické stratégie na efektívne bránenie sa pred hybridnými hrozbami.

1.2 Cieľová skupina

Modul je určený pre študentov stredných škôl vo veku približne od 15 – 19 rokov. Predpokladá sa heterogénne zloženie skupiny, pozostávajúce zo žiakov s pokročilými digitálnymi zručnosťami, ako aj zo žiakov, ktorí potrebujú niektoré súvislosti dovysvetliť. Obsah je prispôsobený tomu, aby bol zrozumiteľný pre všetkých, bez ohľadu na ich predchádzajúce znalosti.

Pri práci so skupinou sa kladie dôraz na vekovú primeranosť, používanie príkladov z reálneho prostredia sociálnych sietí a aplikácií, ktoré študenti môžu používať (Instagram, Messenger, TikTok, Discord, Snapchat, X).

1.3 Lektori

Modul je vyučovaný lektormi, ktorý sa venujú výučbe problematiky kybernetických hrozieb na Právnickej fakulte Univerzity Komenského v Bratislave. Modul vedú jednotliví lektori záživným spôsobom, aby si študenti odniesli nielen teoretické poznatky, ale vedeli ich aj prakticky aplikovať. Lektori vedú diskusie na tému kybernetických hrozieb. Diskusie dopĺňajú interaktívne aktivity, ktoré zahŕňajú analýzu brainstorming a riešenie prípadových štúdií. Študenti sa učia aplikovať nadobudnuté vedomosti individuálne alebo v rámci skupinovej práce. Hlavným cieľom lektorov je zapojiť aktívne študentov do výučbového procesu kurzu.

1.4. Ciele modulu 3 „Efektívne bránenie sa pred kybernetickými hybridnými hrozbami, ktorým čelia študenti stredných škôl ako používatelia internetu"

Po absolvovaní modulu 3 „Efektívne bránenie sa pred kybernetickými hybridnými hrozbami, ktorým čelia študenti stredných škôl ako používatelia internetu" by mal študent:

- vysvetliť pojmy hybridné hrozby, dezinformácie, manipulatívny obsah
- rozlíšiť techniky vykonávania kybernetických hybridných hrozieb
- identifikovať právne a etické dôsledky šírenia nepravdivého obsahu
- rozumieť slobode prejavu a zodpovednosti za takýto prejav
- dokázať pracovať v tímoch
- uplatniť zásady bezpečného zdieľania v praxi (bez polohy v reálnom čase, s ohľadom na publikum a dlhodobú digitálnu stopu)

2 Vzdelávacie materiály

2.1 Prezentácia

Prezentácia obsahuje pätnásť snímok a slúži ako vizuálny rámec celej výučby. Podporuje diskusiu a dopĺňa teoretické vysvetlenia. Hlavné časti prezentácie sú:

- Hybridné hrozby
- Dezinformácie a metódy manipulácie
- Postup ako analyzovať dezinformácie (podľa Európskeho parlamentu)
- Ako fungujú dezinformácie (video)
- Prípadová štúdia 1
- Prípadová štúdia 2
- Reuters Fact Check
- Aktivita: Vyhľadajte dezinformácie na internete

Prezentácia uvádza študentov do problematiky kybernetických hybridných hrozieb a ich pôsobenia v online priestore. Úvodná časť sa venuje **vymedzeniu hybridných hrozieb** a vysvetľuje, ako kombinujú techniky ovplyvňovania, dezinformácie a psychologické operácie s cieľom manipulovať verejnú mienku, vyvolávať chaos či zasahovať do demokratických procesov. Následne prezentácia nadviaže na **dezinformácie a metódy manipulácie**, pričom žiaci spoznajú najčastejšie techniky využívané v online obsahu. Tieto pojmy sú doplnené o **postup Európskeho parlamentu na analýzu dezinformácií**, ktorý poskytuje jednoduchý a praktický rámec pre hodnotenie pravdivosti a dôveryhodnosti informácií. Súčasťou výučby je aj ukážkové video o tom, ako fungujú dezinformácie, ktoré žiakom vizuálne priblíži mechanizmy ich šírenia, úlohu algoritmov a dôvody, prečo nepravdivý obsah často získava väčší dosah ako faktické informácie.

Praktickú rovinu dopĺňajú **dve prípadové štúdie**:

- prvá analyzuje šírenie virálneho „šokujúceho" videa bez uvedenia zdroja,
- druhá sa venuje manipulatívnemu grafu, ktorý predstiera vedeckú dôveryhodnosť.

Obe štúdie umožňujú študentom aplikovať teóriu na konkrétne situácie a precvičiť si rozpoznávanie manipulatívnych prvkov v rámci informácií.

Súčasťou prezentácie je aj krátke predstavenie nástroja **Reuters Fact Check**, ktorý slúži na overovanie virálnych tvrdení a vizuálov a ilustruje význam dôveryhodných fact-checkingových platforiem. Na záver prezentácia obsahuje interaktívnu aktivitu, v ktorej majú študenti za úlohu vyhľadať aktuálne dezinformácie na internete, identifikovať ich manipulatívne prvky a navrhnúť postup ich overenia. Aktivita prepája teoretické poznatky s praktickou prácou s obsahom, s ktorým sa bežne stretávajú na sociálnych sieťach.

2.2 Prípadové štúdie

Prípadové štúdie predstavujú praktickú aktivitu, ktorá umožňuje študentom aplikovať teoretické poznatky z oblasti boja proti dezinformáciám a bezpečného správania v online prostredí na reálne situácie. Ich cieľom je podporiť kritické myslenie, schopnosť identifikovať riziká, porozumieť právam dotknutých osôb a navrhovať vhodné riešenia.

Študenti diskutujú o predložených scenároch, identifikujú problémy a hodnotia možné následky. Aktivita rozvíja nielen právne a etické povedomie, ale aj spoluprácu a komunikáciu v tíme.

Prípadová štúdia 1: Šokujúci incident na vlakovej stanici

V nedeľu podvečer sa na platforme TikTok začalo šíriť krátke video v trvaní 12 sekúnd, ktoré údajne zachytáva „násilný incident na železničnej stanici včera večer". Video má dramatickú hudbu, zrýchlené prechody medzi dvoma rozmazanými zábermi a emotívny titulok:

„ŠOKUJÚCE! Toto sa stalo včera na stanici! Média to zatajili!"

Video bolo zverejnené na účte @pravda_na_vlastne_oci, ktorý bol vytvorený len tri dni pred incidentom a má minimálny obsah, prevažne senzácie, clickbaitové titulky a opätovne nahrávanie virálnych videí.

Počas prvých 24 hodín nahrávka dosiahla:

- *364 000 zhliadnutí*
- *8 900 zdieľaní*
- *stovky komentárov obsahujúcich výrazy ako* „konečne pravda", „cenzúra médií", „už nám nič nepovedia".

Do šírenia videa sa rýchlo zapojili účty, ktoré bežne publikujú polarizačný alebo manipulatívny obsah.

Otázky

1. Prečo majú podľa Vás práve takéto šokujúce videá tendenciu šíriť sa veľmi rýchlo?
2. Aké môžu byť dôsledky toho, že ľudia začnú veriť neoverenému videu?

3. Ako by Ste reagovali, keby Vám takéto video poslal kamarát s komentárom „Pozri, toto je hrozné!"?

Prípadová štúdia 2: Zverejnenie fotografií bez súhlasu

Na platformách Instagram, Telegram a TikTok sa začal šíriť vizuálne graf označený veľkým titulkom:

„TOTO OFICIÁLNE POTVRDILI ODBORNÍCI! ÚČINNOSŤ VAKCÍN JE MIZIVÁ!!!"

Graf údajne dokazuje „mizivý účinok" bližšie neurčenej vakcíny. Graf je často zdieľaný profilmi, ktoré propagujú prírodné liečiteľstvo, odmietajú medicínske postupy a používajú polarizačný jazyk. V príspevku neboli uvedení autori ani dátum kedy sa takáto štúdia uskutočnila.

Počas 48 hodín:

- *bol zdieľaný viac ako 120 000-krát,*
- *objavil sa v 50+ stories,*
- *viac ako 200 ľudí to okomentovalo.*

Otázky

1. Prečo podľa Vás ľudia veria grafu, ktorý nemá zdroj ani jasné označenie?
2. Aké škody môže spôsobiť šírenie zavádzajúcej informácie v oblasti zdravia?

2.3. Interaktívne aktivity

Aktivita Brainstorming prostredníctvom aplikácie Slido predstavuje interaktívny spôsob zhromaždenia nápadov v reálnom čase, na ktorom študenti môžu priamo participovať. Takýto spôsob participácie na kurze, dokáže zapojiť študentov, ktorí sa necítia komfortne hovoriť pred skupinou. Študenti majú možnosť cez svoje zariadenia odpovedať na otázky:

- Akým spôsobom by mali reagovať na šírenie nepravdivých informácií, ktoré sa deje pomocou informačných technológií?
- Ako možno vyvážiť právo na informácie, slobodu prejavu a zodpovednosť platforiem pri prevencii nepravdivých informácií?

Ich odpovede sa zobrazia na slide v prezentácií okamžite. Tým vzniká mapa rôznych myšlienok, ktorá slúži ako východisko pre ďalšiu diskusiu a nadviazanie na teóriu ochrany osobných údajov.

Aktivita vyhľadávanie a analýza e-dezinformácií v rámci časti základy kritického myslenia predstavuje skupinovú aktivitu, kde študenti pracujú s internetom a vyhľadávajú dezinformácie. Cieľom aktivity je naučiť sa identifikovať techniky manipulácie, ktoré sú skryté v dezinformáciách. Študenti v rámci tejto aktivity budú analyzovať dezinformácie a súčasne si rozvíjať kritické myslenie pri posudzovaní informácií v digitálnom prostredí. Následne študenti v rámci diskusie „peer-to-peer" budú o jednotlivých aspektoch hovoriť ostatným skupinám. Táto aktivita zároveň podporuje prácu v tímoch, spoluprácu a praktické uplatnenie vedomostí nadobudnutých v tomto kurze.

3 Dokumentácia

3.1 Informačný list kurzu Kybernetická hygiena pre stredné školy

NÁZOV A ADRESA VZDELÁVACEJ INŠTITÚCIE:	Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality, Univerzita Komenského v Bratislave, Právnická fakulta, Šafárikovo nám. č. 6, P.O.BOX 313, 810 00 Bratislava (ďalej aj ako „kompetenčné centrum")
NÁZOV KURZU:	Kybernetická hygiena pre stredné školy
CELKOVÝ ROZSAH:	40 minút na školenie
TERMÍNY KURZU:	Kurz je poskytovaný v termínoch dohodnutých s jednotlivými strednými školami.
FORMA VZDELÁVANIA:	Prednáška, seminár, prípadové štúdie.
METÓDA VZDELÁVANIA:	Prezenčne v priestoroch kompetenčného centra alebo prezenčne na strednej škole.
CIEĽOVÁ SKUPINA:	študenti stredných škôl
PROFIL ABSOLVENTA:	Absolvent kurzu „Kybernetická hygiena pre stredné školy" získal základný, prakticky orientovaný prehľad o tom, ako bezpečne a zodpovedne fungovať v online prostredí. Rozumie hlavným hrozbám, ktoré na internete číhajú na mladých používateľov, a vie, ako im predchádzať prostredníctvom jednoduchých, ale účinných pravidiel kybernetickej bezpečnosti. Oboznámil sa so základmi právnej úpravy kybernetickej bezpečnosti, so zásadami ochrany osobných údajov a s dôsledkami nezodpovedného správania na internete. Vďaka kurzu vie, ako rozoznať rizikové správanie, ako reagovať na kyberšikanu či podvody a ako zodpovedne využívať technológie v každodennom živote.
LEKTORI:	JUDr. Zoltán Gyurász, PhD., Mgr. Maroš Pavlovič, PhD., LL.M., Mgr. Roland Hochmann, prof. JUDr. Jozef Čentéš, DrSc., JUDr. Laura Fotopulosová, PhD. LL.M., Mgr. Marek Adamkovič
VYUČOVACÍ JAZYK:	Slovenský jazyk
DOKLAD O ABSOLVOVANÍ KURZU:	Osvedčenie o účasti na kurze

3.2 Sylabus modulu 3 „Efektívne bránenie sa pred kybernetickými hybridnými hrozbami, ktorým čelia študenti stredných škôl ako používatelia internetu"

1. Čo sú hybridné hrozby a ako sa prejavujú v online prostredí

OBSAH

- vymedzenie pojmov hybridné hrozby a dezinformácie (Európsky parlament)

AKTIVITA: Brainstorming

Prípadové štúdie

2. Typy dezinformácií a techniky manipulácie

OBSAH

- Techniky manipulácie s informáciami (Európsky parlament)

ODPORÚČANÝ OBSAH

- Európske centrum excelentnosti pre boj proti hybridným hrozbám (HybridCoE)
- Strategický kompas pre bezpečnosť a obranu (Európska rada)
- Tímy rýchlej reakcie (Európska rada)

3. Základy kritického myslenia

OBSAH

- overovanie zdrojov (Reuters)
- analýza zámeru autora
- identifikácia propagandy

AKTIVITA: „Lovci fake news"

4. Právne a etické dôsledky šírenia dezinformácií

OBSAH

- trestnoprávna a občianskoprávna zodpovednosť, spoločenský vplyv (Monografia)

AKTIVITA: Brainstorming