

KYBERNETICKÁ HYGIENA PRE STREDNÉ ŠKOLY

Informačný list



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Financované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 17RO5-04-VO1-00002.

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
Forma vzdelávania:	Prednáška, prípadové štúdie, praktické úlohy.
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 kurzu

Predmetný kurz sa skladá z nasledujúcich modulov:

1. KYBERŠIKANA

Modul sa zameriava na identifikáciu a právne vymedzenie kyberšikany ako špecifickej formy agresívneho správania v online prostredí. Študenti získajú prehľad o najčastejších prejavoch kyberšikany (napr. obťažovanie, vyhrážanie, zverejňovanie citlivého obsahu bez súhlasu), o jej psychologických dôsledkoch a o možnostiach právnej ochrany obetí. Prostredníctvom interaktívnych aktivít, analýz prípadových štúdií a simulovaných modelových situácií si osvoja mechanizmy včasného rozpoznania a efektívnej reakcie na kybernetické násilie, vrátane postupu pri jeho nahlasovaní a vyhľadávaní pomoci. 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. Definícia a formy kyberšikany

- vysvetlenie pojmu kyberšikana, jej foriem, rozlíšenie medzi klasickou šikanou a kyberšikanou, identifikácia rôznych prejavov kyberšikany (textové správy, zverejňovanie citlivého obsahu a pod.)
- interaktívna aktivita: práca v skupinách – študenti analyzujú rôzne scenáre a určujú, či ide o kyberšikanu

2. Právne aspekty kyberšikany

- vysvetlenie možných dopadov kyberšikany so zameraním na trestnoprávnu zodpovednosť

3. Ako sa má brániť obeť kyberšikany?

- nahlasovanie kyberšikany, kontaktovanie autorít
- vymedzenie subjektov, ktorým je možné kyberšikanu nahlásiť (škola, polícia, linky pomoci)
- interaktívna aktivita: roleplay - nácvik správneho postupu pri nahlásení kyberšikany

4. Úloha svedkov a zodpovednosť okolia

- etická a právna dimenzia pasívneho pozorovania alebo šírenia obsahu.
- interaktívna aktivita: simulácia rôznych situácií súvisiacich s kyberšikanou a diskusia so študentami, ako by v danom prípade postupovali.

2. OCHRANA OSOBNÝCH ÚDAJOV V KYBERNETICKOM PRIESTORE

Modul poskytuje základný právny a praktický rámec ochrany osobných údajov v digitálnom prostredí. Študenti sa oboznámia so základnými pojmami ako „osobný údaj“, „súhlas dotknutej osoby“ či „zodpovednosť prevádzkovateľa“, a so základmi vnútroštátnej právnej úpravy a všeobecného nariadenia o ochrane údajov (GDPR). Cieľom modulu je posilniť schopnosť študentov identifikovať rizikové správanie pri zdieľaní údajov online, porozumieť dôsledkom ich sprístupnenia neoprávneným osobám a osvojiť si zásady bezpečného a zodpovedného nakladania s digitálnou identitou. 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. Vymedzenie pojmu osobné údaje a ako vzniká digitálna stopa

- definovanie pojmu osobné údaje, príklady osobných údajov a ich zhromažďovania v praxi, koncept digitálnej identity
- interaktívna aktivita: študenti vyhľadávajú, čo všetko sa o nich dá nájsť verejne dostupne (aj s využitím umelej inteligencie)

2. Právny rámec ochrany osobných údajov

- základné ustanovenia GDPR a vnútroštátnej právnej úpravy, vymedzenie čo znamená súhlas a práva dotknutej osoby
- interaktívna aktivita: pravda/nepravda – mýty o ochrane osobných údajov

3. Riziká zdieľania údajov na sociálnych sieťach

- vymedzenie údajov, ktoré možno považovať za citlivé

4. Bezpečné správanie v online priestore

- zásady zodpovedného zdieľania informácií
- ako predchádzať únikom osobných údajov a ako rozpoznať možné riziká
- interaktívna aktivita: simulácia „phishingového“ e-mailu a jeho rozbor v skupinách

5. Praktické nástroje pre ochranu údajov

- dvojfaktorová autentifikácia, ako si správne nastaviť heslo, anonymizácia

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.

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.