

# KYBERNETICKÁ HYGIENA PRE STREDNÉ ŠKOLY

## MODUL 2

Ochrana osobných údajov v kybernetickom priestore



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

# KYBERNETICKÁ HYGIENA PRE STREDNÉ ŠKOLY

## MODUL 2

Ochrana osobných údajov v kybernetickom priestore



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 2

### „OCHRANA OSOBNÝCH ÚDAJOV V KYBERNETICKOM PRIESTORE“

Modul 2 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

##### 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 analýza v skupinách

##### 5. Praktické nástroje pre ochranu údajov

- dvojfaktorová autentifikácia, ako si správne nastaviť heslo, anonymizácia

# 1. METODIKA MODULU 2

## 1.1 Charakteristika modulu 2 „Ochrana osobných údajov v kybernetickom priestore“

Modul „Ochrana osobných údajov v kybernetickom priestore“ 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 ochrany osobných údajov. Digitálny priestor prináša množstvo príležitostí, no zároveň riziká, ktoré si mladí ľudia často neuvedomujú. Modul pracuje s kombináciou teoretického výkladu, praktických ukážok, interaktívnych aktivít a diskusie.

Tematická orientácia modulu vychádza z kľúčových častí Všeobecného nariadenia o ochrane údajov (GDPR) a vnútroštátnej úpravy v Slovenskej republike zakotvenej v Zákone č. 18/2018 Z.z. o ochrane osobných údajov. Dôležitou súčasťou je aj zdôraznenie zodpovednosti pri narábaní s údajmi online. Obsah druhého modulu kurzu Kybernetická hygiena pre stredoškóľákov reaguje na aktuálne výzvy akými sú masívny rozvoj sociálnych sietí, umelej inteligencie, kybernetických hrozieb, zraniteľností digitálnych účtov a ich vplyv na osobné údaje v kybernetickom priestore.

## 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). Často ide o platformy, kde mladí ľudia spontánne zdieľajú obsah, ktorý môže byť považovaný za osobné údaje alebo dokonca citlivé údaje.

## 1.3 Lektori

Modul je vyučovaný lektormi, ktorý sa venujú výučbe problematiky ochrany osobných údajov v kybernetickom priestore 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 ochrany osobných údajov so študentmi. Diskusie dopĺňajú interaktívne aktivity, ktoré zahŕňajú analýzu phishingových emailov, či 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 2 „Ochrana osobných údajov v kybernetickom priestore“

Po absolvovaní modulu 2 „Ochrana osobných údajov v kybernetickom priestore“ by mal študent:

- rozumieť pojmu osobný údaj a vedieť uviesť príklady
- vysvetliť rozdiel medzi osobným údajom a citlivým osobným údajom
- chápať ako vzniká digitálna stopa a ako sa formuje digitálna identita
- poznať základné práva dotknutých osôb podľa Všeobecného nariadenia o ochrane osobných údajov
- poznať riziká spojené so zdieľaním informácií na sociálnych sieťach
- vedieť identifikovať podvodné správanie na internete
- poznať zásady zodpovedného zdieľania informácií na internete
- vedieť si nastaviť silné heslo a zapnúť dvojfaktorovú autentifikáciu

# 2 Vzdelávacie materiály

## 2.1 Prezentácia

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

- Právo na súkromie (pojem)
- Ochrana osobných údajov (vo všeobecnosti)
- Osobný údaj (definičné znaky)
- Prípadová štúdia 1
- Prípadová štúdia 2
- Digitálna identita a digitálna stopa
- Aktivita: Vyhľadaj svoju digitálnu stopu na internete
- Zásady ochrany osobných údajov
- Právne základy spracúvania osobných údajov
- Súhlas ako právny základ
- Príklad z praxe
- Práva dotknutej osoby
- Citlivý osobný údaj
- Aktivita: Rozoznávajúce podvodných správ a sociálneho inžinierstva
- Zásady bezpečného zdieľania a ochrany súkromia

Prezentácia systematicky uvádza študentov do problematiky ochrany osobných údajov a bezpečného správania v digitálnom prostredí. Spočiatku sa venuje pozornosť pojmu **právo na súkromie** a jeho významu pre jednotlivca, úvodu do **ochrany osobných údajov** a definičným znakom osobného údaje. Súčasťou výučby sú aj dve **prípadové štúdie**, ktoré umožňujú študentom aplikovať teóriu na reálne situácie. Nasledne sa študenti oboznámia s pojmami **digitálna identita a digitálna stopa**, doplnené praktickou aktivitou, v ktorej študenti skúmajú vlastnú online stopu. Prezentácia sa zameriava na **zásady ochrany osobných údajov**, prehľad **právnych základov spracúvania** a osobitný dôraz kladie na **súhlas** ako jeden z právnych základov spracúvania osobných údajov. Zahrnutý je aj **príklad z praxe**, ktorý demonštruje fungovanie GDPR v reálnych situáciách a prehľad **práv dotknutej osoby**.

V ďalšej časti sa pozornosť venuje aj pojmu **citlivý osobný údaj** a jeho špecifickej ochrane. Druhá praktická aktivita je zameraná na **rozpoznávanie podvodných správ a techník sociálneho inžinierstva**. Záverečná časť sa venuje **zásadám bezpečného zdieľania a ochrany súkromia**, ktoré upevňujú zodpovedné správanie v online prostredí.

## 2.2 Prípadové štúdie

Prípadové štúdie predstavujú praktickú aktivitu, ktorá umožňuje študentom aplikovať teoretické poznatky z oblasti ochrany osobných údajov, digitálnej identity 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: Falošný profil

*Neznámy človek vytvorí na sociálnej sieti falošný profil študenta. Používa jeho meno, fotografie prevzaté z internetu bez súhlasu a kontaktuje jeho spolužiakov. Vystupuje akoby za neho a žiada osobné informácie, prípadne zdieľa nepravdivé alebo nevhodné správy.*

#### Otázky

1. Aká škoda môže vzniknúť pre študenta (dotknutú osobu) v škole, medzi známymi alebo na sociálnych sieťach?
2. Môže dôjsť k psychologickému tlaku alebo kyberšikane?
3. Je vytvorenie falošného profilu porušením práva na ochranu osobných údajov?

### Prípadová štúdia 2: Zverejnenie fotografií bez súhlasu

*Škola zverejní fotografie zo školského výletu na svojej webovej stránke. Niektorí rodičia však nedali súhlas so zverejnením podobizne svojich detí. Fotografie sú verejne dostupné a viditeľné pre kohokoľvek.*

#### Otázky

1. Je fotografia osobným údajom?
2. V čom spočíva problém, ak chýba súhlas zákonného zástupcu?
3. Prečo môže byť zverejnenie bez súhlasu nebezpečné alebo citlivé?

## 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 otázku „Čo si predstavujete pod ochranou osobných údajov?“ pričom ich odpovede sa zobrazia na slide v prezentácii okamžite. Tým vzniká mapa rôznych myšlienok, ktorá slúži ako východisko pre ďalšiu diskusiu a nadviazanie na teóriu ochrany osobných údajov.

**Aktivita vyhľadávanie a analýza vlastnej digitálnej stopy** v rámci časti vymedzenie pojmu osobné údaje a ako vzniká digitálna stopa má demonštrovať, že všetci v digitálnom prostredí zanechávame svoju digitálnu stopu. Každý komentár, fotografia, kliknutie, či objednávka tovaru z e-shopu vytvára obraz o našej digitálnej identite. Digitálna stopa v súčasnosti ovplyvňuje nielen fungovanie medzi priateľmi a známymi, ale aj pracovnej sfére, kedy algoritmy vyhodnocujú uchádzačov o zamestnanie. Aktivita „Vyhľadávanie vlastnej digitálnej stopy“ dáva študentom priestor kriticky preskúmať, čo o nich internet vie, aké informácie sú o nich dostupné verejne a ako tieto dáta formujú ich online identitu. Cieľom je naučiť ich bezpečne pracovať s vlastnou digitálnou stopou, rozumieť rizikám spojeným so zverejňovaním informácií a uplatňovať zásady digitálnej gramotnosti a ochrany súkromia (vrátane základných princípov GDPR) v praxi.

**Aktivita analýza e-mailov** v rámci časti bezpečné správanie v online priestore predstavuje skupinovú aktivitu, kde študenti pracujú s autentickými ukážkami e-mailov. Cieľom aktivity je naučiť sa identifikovať varovné signály, ktoré sú skryté v rámci podvodných e-mailov. Študenti v rámci tejto aktivity budú analyzovať phishingové e-maily 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.

Študenti v rámci práce v skupinách obdržia nasledovné kartičky s e-mailom:

From: Microsoft <rmicrosoft@rmicrosoft.eu>

---

Subject: **[Action Required] Vaše konto bude odpojené**

Ahoj uživatel,

zaznamenali sme chyby vo vašom konte. Ak problém neodstránite do 2 hodín, účet ti bude natrvalo odstránený.

Klikni na [RIEŠIŤ TERAZ](#)

S pozdravom,  
Microsoft Security Team

*Obrázok 1: Phishingový e-mail*

From: Tatra Banka <info@tb.sk>

---

Subject: **Vaša platba čaká na overenie!**

Vážený klient,

z dôvodu bezpečnosti došlo k pozastaveniu vašej poslednej platby.

Na obnovenie služieb kliknite tu a zadajte číslo karty, bezpečnostné číslo a následne kód na potvrdenie platby:  
<https://www.tatrabnka.sk>

S pozdravom,  
Bezpečnostné oddelenie

*Obrázok 2: Phishingový e-mail*

From: Slovenská pošta <delivery@slovenskaposta.eu>

Subject: **Doručenie balíka bolo pozastavené**

Balík č. SK-2041 sa nepodarilo doručiť.

Uhrad'te doručovací poplatok 1,99 € na potvrdenie adresy: <http://deliver-now.support/pay>

Ak poplatok neuhradíte do 12 h, balík bude vrátený odosielateľovi.

S posdravom  
*Slovenská pošta*

*Obrázok 3: Phisingový e-mail*

From: IT Support Edupage <helpdesk@edubage.sk>

Subject: **Vaše heslo vyprší dnes**

Systém zistil, že vaše heslo vyprší do 30 minút. Ak ho neobnovíte, stratíte prístup do Edupage a k školskej wifi.

Obnoviť heslo: <https://www.edupage.sk/reset>

IT Support

*Obrázok 4: Phisingový e-mail*

From: Finančná správa <info@financnasprava-refund.eu>

Subject: **Máte nárok na vrátenie dane 248,30  
€ – potvrdte účet**

Po prepočte máte nárok na vrátenie dane.  
Zadajte číslo účtu, rodné číslo a dátum  
narodenia pre vyplatenie:

<https://financnasprava-refund.eu/overenie>

Vyplatenie prebehne do 3 pracovných dní.

S pozdravom

Finančná správa

*Obrázok 5: Phisingový e-mail*

# 3 Dokumentácia

## 3.1 Informačný list kurzu Kybernetická hygiena pre stredné školy

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NÁZOV A ADRESA<br/>VZDELÁVACEJ<br/>INŠTITÚCIE:</b> | 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“)                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>NÁZOV KURZU:</b>                                   | Kybernetická hygiena pre stredné školy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>CELKOVÝ ROZSAH:</b>                                | 40 minút na školenie                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>TERMÍNY KURZU:</b>                                 | Kurz je poskytovaný v termínoch dohodnutých s jednotlivými strednými školami.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>FORMA<br/>VZDELÁVANIA:</b>                         | Prednáška, seminár, prípadové štúdie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>METÓDA<br/>VZDELÁVANIA:</b>                        | Prezenčne v priestoroch kompetenčného centra alebo prezenčne na strednej škole.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CIEĽOVÁ SKUPINA:</b>                               | študenti stredných škôl                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>PROFIL ABSOLVENTA:</b>                             | 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. |
| <b>LEKTORI:</b>                                       | 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>VYUČOVACÍ JAZYK:</b>                               | Slovenský jazyk                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>DOKLAD O<br/>ABSOLVOVANÍ KURZU:</b>                | Osvedčenie o účasti na kurze                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## 3.2 Syllabus modulu 2 „Ochrana osobných údajov v kybernetickom priestore“

### 1. Vymedzenie pojmu osobné údaje a ako vzniká digitálna stopa

#### OBSAH

- Definovanie pojmu osobné údaje podľa GDPR a príslušnej slovenskej úpravy ([Európska únia](#))
- Príklady bežne zhromažďovaných údajov v praxi ([NOYB](#))
- Digitálna identita a digitálna stopa: čo všetko o používateľovi zhromažďujú služby a ako sa tieto informácie spájajú ([ČT](#))

**AKTIVITA:** Brainstorming

Prípadové štúdie

Vyhľadávanie a analýza vlastnej digitálnej stopy

### 2. Právny rámec ochrany osobných údajov

#### OBSAH

- Základné zásady Všeobecného nariadenia o ochrane osobných údajov ([Európska Komisia](#))
- Súhlas ako právny základ podľa Všeobecného nariadenia o ochrane osobných údajov ([Európska Komisia](#))
- Práva dotknutej osoby podľa Všeobecného nariadenia o ochrane osobných údajov ([NOYB](#))

#### ODPORÚČANÉ ZDROJE

- Ochrana osobných údajov v kocke ([Európska únia](#))
- Všeobecné nariadenie o ochrane osobných údajov ([Eurlex](#))
- Zákon č. 18/2018 Z.z. o ochrane osobných údajov ([Slovlex](#))

### 3. Riziká zdieľania údajov na sociálnych sieťach

#### OBSAH

- Citlivé osobné údaje ([Európska Komisia](#))

## ODPORÚČANÉ ZDROJE

- Aké informácie Facebook zhromažďuje ([ČT](#))
- Film The Great Hack (dostupné na Netflixe)

### 4. Bezpečné správanie v online priestore

#### OBSAH

- Zásady bezpečného zdieľania a ochrany súkromia ([Bezpečne na internete](#))
- Rozoznávanie podvodných správ a sociálneho inžinierstva ([Tatra Banka](#))

**AKTIVITA:** Analýza emailov

### 5. Praktické nástroje pre ochranu údajov

#### OBSAH

- Dvojfaktorová autentifikácia ([Microsoft](#))
- Ako nastaviť silné heslo a používať správcu hesiel ([Eset](#))
- Anonymizácia a minimalizácia údajov