



Školení z oblasti bezpečnosti IT systémů a problematiky kyberšikany

V současné době se organizace připravují na zavedení GDPR (General Data Protection Regulation, obecné nařízení o ochraně osobních údajů). Zároveň se ve zvýšené míře objevují útoky na informační systémy, nerespektování pravidel práce v těchto systémech a další negativní jevy v této oblasti. Vzrůstá také množství projevů kyberšikany na školách všeho typu a s tím souvisejících negativních jevů.

Toto právně bezpečnostní školení má za cíl důrazně seznámit žáky s jednotlivými projevy porušování pravidel vnitřních řádů organizací a především na skutkové podstaty jejich jednání v oblasti IT bezpečnosti, kyberšikany v návaznosti na trestně právní podstatu těchto skutků i nekompromisní požadavky na sankce s tímto jednáním spojené i zásadní následky tohoto jednání. Se zavedením GDPR se ve všech státech EU v prostředí bezpečnosti ICT, sociálních sítí i samotném školním prostředí významně mění a zintenzivňuje boj se všemi těmito projevy jednání a chování v návaznosti na možné důsledky porušování školního řádu, vnitřních předpisů i trestně právních norem, kterou doposud mnozí ani nepovažují za zjistitelnou a nyní i zcela zásadně postižitelnou.

1/ OBLAST BEZPEČNOSTI IT SYSTÉMŮ

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

1. Kdo **překone bezpečnostní opatření** a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.
2. **Kdo získá přístup k počítačovému systému nebo k nosiči informací a**
 - a. neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
 - b. data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
 - c. padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
 - d. neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.
3. Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
 - a. v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo
 - b. v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.
4. Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,
 - a. spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
 - b. způsobí-li takovým činem značnou škodu,
 - c. způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,
 - d. získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo
 - e. způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.
5. Odnětím svobody na tři léta až osm let bude pachatel potrestán,
 - a. způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo
 - b. získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.



§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

1. Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává
 - a. zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
 - b. počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.
2. Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,
 - a. spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
 - b. získá-li takovým činem pro sebe nebo pro jiného značný prospěch.
3. Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.

1/ OBLAST KYBERŠIKANY

Šikana je jakékoli chování, jehož záměrem je ublížit, ohrozit, ponižovat nebo zastrašovat jiného člověka či skupinu lidí. Kyberšikana (též kybernetická šikana, počítačová šikana či cyberbullying) je specifický druh šikany, který využívá informační a komunikační technologie, elektronické prostředky, jako jsou mobilní telefony, e-maily, pagery, internet, blogy a podobně. Kybernetická šikana má stejný cíl jako klasická fyzická šikana: ublížení a ponížení oběti. Na rozdíl od klasické šikany tváří v tvář, nabízí kyberšikana agresorům nejenom jiné nástroje ubližování, ale specifika virtuální reality obměňují charakter celého procesu šikanování, včetně rolí agresora a oběti.

Mezi projevy kyberšikany patří:

- 1) **Publikování ponižujících záznamů nebo fotografií** (např. v rámci webových stránek, MMS zpráv).
- 2) **Ponižování a pomlouvání** (*denigration*) (v rámci sociálních sítí, blogů nebo jiných webových stránek).
- 3) **Krádež identity** (*impersonation*), **zneužití cizí identity ke kyberšikaně nebo dalšímu sociálně patologickému jednání** (např. zcizení elektronického účtu).
- 4) **Ztrapňování pomocí falešných profilů** (např. v rámci sociálních sítí, blogů nebo jiných webových stránek).
- 5) **Provokování a napadání uživatelů v online komunikaci** (*flaming/bashing*) (především v rámci veřejných chatů a diskuzí).
- 6) **Zveřejňování cizích tajemství s cílem poškodit oběť** (*outing*) (např. v rámci sociálních sítí, blogů nebo jiných webových stránek, pomocí SMS zpráv apod.).
- 7) **Vyloučení z virtuální komunity** (*exclusion*) (např. ze skupiny přátel v rámci sociální sítě).
- 8) **Obtěžování** (*harassment*) (např. opakovaným prozváněním, voláním nebo psaním zpráv).
- 9) **Napomáhání** všem druhům kyberšikany, které jsou uvedeny v bodech 1-8.



Pro řešení problémů s kyberšikanou existuje řada dokumentů:

- Listina základních práv EU**
- Úmluva o právech dítěte**
- Školský zákon**
- Občanský zákoník**
- Zákon o ochraně osobních údajů**
- Zákon o sociálně-právní ochraně dětí**
- Trestní zákoník**
- Přestupkový zákon**
- Zákon o soudnictví ve věcech mládeže**
- Metodický pokyn ministerstva školství k prevenci a řešení šikanování mezi žáky**

Přehled paragrafů, podle kterých lze klasifikovat kyberšikanu

Trestní zákoník (Zákon 40/2009 Sb.)

§ 144	Účast na sebevraždě	až 12 let
§ 175	Vydírání	až 16 let
§ 180	Neoprávněné nakládání s osobními údaji	až 8 let
§ 181	Poškození cizích práv	až 5 let
§ 182	Porušení tajemství dopravovaných zpráv	až 10 let
§ 183	Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí	až 8 let
§ 184	Pomluva	až 2 roky
§ 191	Šíření pornografie	až 5 let
§ 192	Výroba a jiné nakládání s dětskou pornografií	až 8 let
§ 209	Podvod	až 10 let
§ 230	Neoprávněný přístup k počítačovému systému a nosiči informací	až 8 let
§ 231	Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	až 5 let
§ 232	Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti	až 2 roky
§ 352	Násilí proti skupině obyvatelů a proti jednotlivci	až 3 roky
§ 353	Nebezpečné vyhrožování	až 3 roky
§ 354	Nebezpečné pronásledování	až 3 roky
§ 356	Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod	až 3 roky
§ 357	Šíření poplašné zprávy	až 8 let

Na základě nařízení orgánů MŠMT, školských poradenských zařízení a především metodických pokynů orgánů činných v trestním řízení v oblasti porušování norem v prostředí IT bezpečnosti a jakýchkoliv projevů kyberšikan, budou školy všech stupňů opakovaně prokazatelně proškolovat všechny žáky a zaměstnance a současně v součinnosti s těmito institucemi co nejzásadněji a nejefektivněji hlásit a tvrdě postihovat aktuální i budoucí projevy porušování bezpečnosti IT prostředí a kyberšikan.

Projevy tohoto negativního jednání nebo zvláště závažné činnosti směřující k porušování výše uvedených vnitřních i vnějších právních norem, mají školy pravomoc v prostředí „školní odpovědnosti“ postihovat institutem správního rozhodnutí nejvyššího sankčního dopadu, tj. vyloučení ze školy, případně postoupení k řešení orgánům činných v trestním řízení /oddělením kyberbezpečnosti policie ČR/.

Tyto instituce budou dle aktuální právní úpravy používat všech dostupných prostředků k zajištění ochrany dat, informačních systémů, IT systémů a ochraně žáků i učitelů před všemi projevy kyberšikan.



Svým podpisem stvrzuji, že jsem byl prokazatelně seznámen s projevy porušování norem v oblasti bezpečnosti IT systémů, kyberšikany a možnými sankcemi v důsledku jejich porušení.

- I. § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
- II. § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- III. Zákon 40/2009 Sb - klasifikace projevů kyberšikany a s akcí s tím spojených

třída:	jméno	příjmení	podpis
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			

Ve Frýdku-Místku:2021

Školení provedl/a:

Mgr. Radan Nachmilner
ředitel SŠINFOTECH, s.r.o.



SŠ INFOTECH
Střední škola informačních
technologií s.r.o., Frýdek-Místek