E-Bezpečí 2020, 5(2): Page 33-35. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=2034

UČITELÉ, POZOR! ŽÁCI ZVOU DO ONLINE VÝUKY DALŠÍ UŽIVATELE, KTEŘÍ PAK VÝUKU NARUŠUJÍ, SVÉ TROLLOVÁNÍ NAHRÁVAJÍ A STREAMUJÍ ZÁZNAMY HODIN… TŘEBA NA TWITCHI NEBO TIKTOKU.

Kamil KOPECKÝ

S přechodem škol na distanční formu vzdělávání - především pak na online synchronní výuku - se v online světě opětovně objevují rizikové fenomény spojené s únikem osobních údajů do online světa (nahrávky vyučovacích hodin bez souhlasu učitele a jejich sdílení prostřednictvím sociálních sítí, trollování online výuky změnami profilové fotografie, spamováním na zeď, sdílením odkazů na nevhodný obsah apod.), nově se pak objevují situace, kdy se do online výuky připojí další osoba, která začne výuku narušovat. Žáci totiž sdílejí své přihlašovací údaje do online výuky (např. ID číslo a PIN pro přístup do systému Zoom, kód pro přístup ke konkrétní videokonferenci atd.) s dalšími osobami, které pak mohou výuku sabotovat.

Pro učitele to znamená především to, že by měli omezit plánování vzdělávacích aktivit pomocí rozesílání identifikačních přístupů ke vzdělávacím lekcím svým žákům. Ty je totiž velmi snadné přeposlat dalším kamarádům, kteří mají v oblibě např. streamování.

Učitel Daniel Pražák před tímto chováním varuje např. na svém Twitteru:

> Tak jsem zachytil, že nějací borci lákají z žáků odkazy na online výuku, připojí se tam, trollí učitele, rozloží hodinu a pak to sdílejí online.
>
> K tomu dvě věci:
> 1) Prosím, nebuďte dementi. Škodíte tím nakonec sami sobě.
> 2) Není to náhodou trestný?
>
> A pro autory: Styďte se.
>
> — Daniel Pražák (@daniel_prazak) October 15, 2020

*"Z pohledu trestního práva toto jednání ve většině případů trestné není, **věc se však dá řešit s využitím občanského zákoníku či zákona na ochranu osobních údajů**. Samotný proces je však poměrně komplikovaný, záleží na mnoha faktorech a okolnostech, jaké údaje a informace mohou být zneužity, jakým způsobem atd. Takovéto případy je skutečně důležité řešit individuálně a dle toho vyhledat příslušné porušení zákonného ustanovení,"* uvádí kpt. Pavel Schweiner s Krajského ředitelství policie Olomouckého kraje.

Další právní pohled nabízí Advokátní kancelář SEDLAKOVA LEGA (Řizení školy):
*Ve chvíli, kdy do on-line výuky vstoupí cizí osoba, která narušuje výuku, ponižuje učitele a následně tuto informaci sdílí on-line, **může páchat trestný čin**. Taková nahrávka totiž může být ponižující a může ohrozit společenskou vážnost učitele, což v některých případech může naplnit znaky trestného činu porušení tajemství listin a jiných dokumentů uchovávaných v soukromí dle § 183 trestního zákoníku, za který hrozí trest odnětí svobody až na dvě léta (v případě ohrožení společenské vážnosti). Jednání však musí být významně společensky škodlivé. Vždy je možné obrátit se na Policii ČR, pokud existuje podezření ze spáchání trestného činu a ta má povinnost dané jednání prošetřit.*

*Dále se také může jednat o **přestupek v oblasti občanského soužití dle § 7 odst. 1 písm. a) zákona o některých přestupcích, za který hrozí pokuta až 15 000 Kč**. Učitelé také mají možnost bránit se proti uveřejnění videozáznamu, které byly jinou osobou zachyceny a které mají poškozeného urazit nebo zesměšnit, a to prostřednictvím **žaloby na ochranu osobnosti**.*

Jak z toho ven? Stačí změnit způsob plánování vzdělávacích akcí.

Existuje celá řada způsobů, jak minimalizovat riziko, že se do probíhající vzdělávací akce někdo dostane:

1. **Využívat komplexní uzavřené systémy, ve kterých má každý žák svůj unikátní e-mailový přístup (např. Microsoft Teams, Google Classroom apod.). Ke konkrétní plánované akci se pak dostanou pouze ti, kteří jsou v systému registrováni a přihlášeni (odpadá nutnost sdílet speciální kódy).**
2. **Využívat funkce “předsálí” (např. v systému Zoom, Skype apod.). S aktivovaným předsálím musí studenti po přihlášení k danému videochatu vyčkat, dokud jim učitel nepovolí přístup (neověří si jejich identitu).**
3. **Využívat funkce “uzamknout” (např. v systému Zoom, Discord apod.). Po zahájení hodiny lze videochat uzamknout tak, že se do něj nemůže přihlásit nikdo další.**
4. **Aktivně pracovat s uživatelskými oprávněními v jednotlivých systémech a vhodně nastavovat uživatelská práva a role. V praxi to znamená umět nastavit, jaké aktivity budou mít žáci v průběhu videohodiny povoleny (tj. zda budou moci nahrávat hodinu, pouštět mikrofon (unmute), psát na zeď, sdílet odkazy apod.).**

Co je třeba říci, nahrávání obrazovky počítače (např. s využitím specializovaných programů) nelze nikdy stoprocentně zabránit. Každý student a žák, který ví, jak na to, si může záznam vyučovací hodiny velmi snadno pořídit a rozšířit. Není nutné automaticky předjímat, že by byl záznam z hodiny někdy v budoucnu zneužit, je však třeba s touto možností počítat…

Pro E-Bezpečí
Kamil Kopecký