Online výuka a její bezpečnost

SŠIPF

Jaroslav Tihlařík

Povinná distanční výuka

- Novela školského zákona byla publikována ve Sbírce zákonů pod číslem 349 a nabyla účinnosti 25. 8. 2020.

- Distanční výuka je **pro žáky povinnou** součástí školní docházky.
- **Škola je povinna** žákům a studentům poskytovat vzdělávání distančním způsobem v případě znemožnění jejich osobní přítomnosti ve škole.

Distanční výuka / Online výuka

- **Distanční** vzdělávání je multimediální **forma řízeného studia**, kde hlavní **odpovědnost za průběh a výsledky vzdělávání spočívá na studujících**, kteří jsou odděleni od vyučujících (konzultantů).

Distanční výuka / Online výuka

- **Online** výuku lze definovat jako **synchronní distanční výuku**.
- **Online** výuka může být chápana také jako forma **prezenčního** studia, při které je vyžadována osobní přítomnost žáků při výuce **skrze moderní komunikační technologie** (např. videokonference). Tuto formu studia lze také označit jako denní studium, přesněji: online denní forma vzdělávání.

Přechod na distanční / online výuku

- Přechod na distanční výuku byl problematický ve všech státech světa.
- Neřízené, rychlé a živelné.
- Teprve následně řešena bezpečnost.

Výběr prostředí pro online výuku

- Microsoft Teams
- Google for Education (Classroom, Meet, Calendar, …)

- Zvolte si vždy pouze jednu platformu!

- **Roztříštěnost způsobuje chaos.**

Hesla (passwod)? Raději fráze (passphrase)!

- Základem bezpečného pohybu v online prostoru je bezpečné heslo, které by mělo splňovat několik zásad.
  - Unikátnost
  - Délka hesla
  - Složení hesla
- Ideální heslo je takové, které nikdo v okolí neodhadne, nebo takové, které nedává nikomu jinému smysl.
- Tip: Používejte aplikace pro **správu hesel**.

Soukromí učitelů a žáků

- **Důsledně oddělujete** soukromou a profesní identitu.
- Důležité školní dokumenty posílejte pouze přes služební e-mailovou schránku.
- Používejte vždy školní e-mailovou adresu.
- Pro komunikaci učitelů s žáky si ve škole nastavte jednu komunikační platformu.

GDPR

- Vždy při nahrávání online hodiny myslete také na ochranu osobních údajů.
- Nezveřejňujte videa mimo zvolený systém výuky.
- Využívejte oficiální školní účty.

- Bohužel nelze zamezit sekundárnímu nahrávání na straně žáků.

Rizika

- Nezabezpečená videokonferenční místnost
  - skrytí pozorovatelé
  - škodliví herci
- Sdílené prostředí
  - prostor pro kyberšikanu
- Zvyšuje se riziko otevření přílohy mailu obsahující škodlivý kód (malware).

Kyberšikana

Terčem se mohou stát nejen žáci, ale velmi lehce také učitelé!

Doporučení:

- nezveřejňujte žádná videa,
- hodnocení práce žáků, dělejte individuálně, ne před celou třídou,
- oddělte prostředí pro odevzdání prací žáků.

Pozor na Phishing!

- Typicky se může jednat o rozeslání e-mailů nebo zpráv, které vyzývají k zadání osobních údajů na falešnou stránku. Tato stránka může být velmi podobná stránce oficiální, může např. napodobovat přihlašovací okno MS Teams (Bakaláři, …).
- Uživatel zadá své přihlašovací jméno a heslo, čímž prozradí své přihlašovací údaje, a umožní přístup ke svému účtu.

Doporučení

- Zlepšit zabezpečení zařízení a síťové infrastruktury.
- Jednotná platforma od velkých společností (MS, Google)
- Metoda jednoho administrátora (většinou sci-fi)
- Metodika online výuky
- Školení učitelů.

Děkuji za pozornost …