Úloha **č. 11**

HESLA – jak vytvořit bezpečné heslo

Tato úloha je vhodná pro 5.-7. ročník ZŠ / Návrh úlohy vypracovala Veronika Veseloušová

KYBERBEZPEČNOST

SOUKROMÍ NA INTERNETU

Setkali jste se někdy s podezřelou zprávou, zvláštním profilem nebo odkazem, na který jste raději neklikli? Přemýšleli jste, proč je na internetu důležité dávat pozor na to, co otevíráme, sdílíme a komu věříme?

Vytváření představy:
Představte si, že vám přijde zpráva: „Klikni sem, jinak ti zablokujeme účet." nebo vám někdo cizí napíše: „Pošli mi svou fotku a telefonní číslo.". Na internetu nevidíme vždy, kdo je na druhé straně. Proto je důležité znát základní pravidla bezpečného chování online, umět poznat riziko a vědět, jak správně reagovat.

Kyberbezpečnost znamená chránit sebe, své údaje, zařízení i své účty při používání internetu, aplikací a digitálních technologií.

POMŮCKY

- Tablety nebo počítače (/mobily)
- Tužka, propiska.

CÍLE

Badatelsky objevit, jaké základní pojmy souvisejí s kyberbezpečností, jak rozpoznat rizikové situace v online prostředí, které informace patří mezi osobní údaje a proč je důležité je chránit, jak správně reagovat na podezřelé zprávy, odkazy a profily a jak přemýšlet o vlastní digitální stopě a bezpečném chování na internetu.

K ZAMYŠLENÍ

Než začnete vyplňovat pracovní list, zamyslete se:

- Co všechno o sobě člověk může nechtěně prozradit na internetu?
- Jak poznáme, že je zpráva nebo profil podezřelý?
- Proč není dobré jednat na internetu ve spěchu nebo v panice?

Pamatujte:
Na internetu není všechno pravda, ne každý je tím, za koho se vydává, a ne každý odkaz je bezpečný.

POSTUP

1 Nejprve si zopakujte základní pojmy z oblasti kyberbezpečnosti. Přiřaďte pojmy pod tabulkou k vysvětlení.

POJMY	VYSVĚTLENÍ
	Škodlivý program, který může poškodit zařízení nebo ukrást data.
	Podvodná zpráva, která se snaží vylákat kliknutí, údaje nebo peníze.
	Nepravdivá poplašná zpráva, která se šíří dál.
	Záměrné ubližování přes internet.
	Informace, podle kterých lze poznat konkrétního člověka.
	Stopy po tom, co na internetu dělám.
	Účet, který se tváří jako někdo jiný nebo není skutečný.
	Kontrola, jestli je informace pravdivá.

Kyberšikana, Osobní údaje, Digitální stopa, Phishing, Hoax, Fake profil, Malware, Ověřování informací

2 Zaměřte na osobní údaje a rozlište, co je bezpečné sdílet a co ne.

ROZHODNĚTE ANO / NE

Jméno a příjmení .....
Přezdívka, která nikoho neprozradí .....
Fotka obličeje .....
Název školy + třída .....
Adresa bydliště .....
Fotka vysvědčení .....
Číslo telefonu .....
„Jsem teď doma sám / sama.“ .....

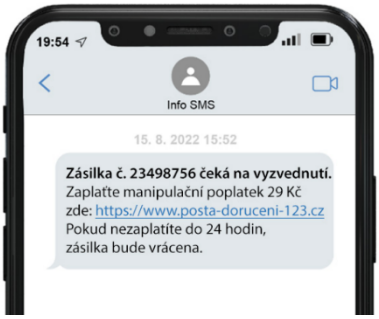
** kromě přezdívky, která nikoho neprozradí je vše nebezpečné.*

3 Vyhodnoťte modelové situace s podezřelými zprávami a odkazy.

Vyber správnou reakci

U každé situace zakroužkujte, co je nejlepší udělat, poté v rámci diskuze rozeberte.

A) SMS:
„Doručení balíku se nezdařilo. Klikni a potvrď adresu: https://www.posta-doruceni-123.cz“

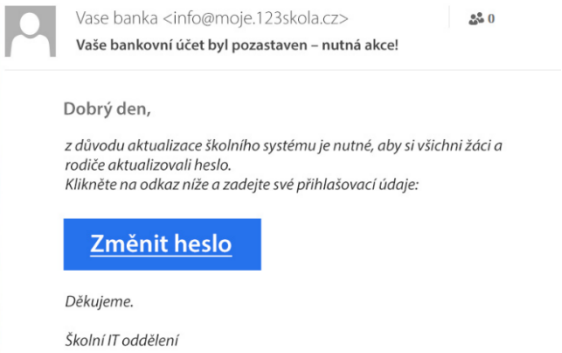


a) Kliknu hned, ať o balík nepřijdu
b) Zeptám se kamaráda, jestli mu to taky přišlo
c) Neklikám, ověřím u dopravce v oficiální aplikaci, na oficiálním webu nebo u rodiče

B) Zpráva v chatu:
„Tady je tvoje fotka 😳 → bit.ly/něco“

a) Otevřu odkaz, ať vím, co je na fotce
b) Neotevírám, ptám se odesílatele, co to je, a raději ověřím jinak
c) Přepošlu to do skupiny, aby to viděli ostatní

C) E-mail:
„Váš účet byl zablokován. Změňte heslo: …“



a) Nejednám v panice, zkontroluji adresu odesílatele a ověřím vše přes oficiální web
b) Okamžitě kliknu, aby se účet nezablokoval
c) Pošlu zpět své údaje, aby mi pomohli

4 Zamyslete se nad tím, jak poznat fake profil.

5 Uvědomte si, co znamená digitální stopa a proč je důležité přemýšlet před sdílením. Výsledek ověřte s umělou inteligencí.

6 Nakonec zkuste formulovat vlastní bezpečnou reakci v situaci, kdy by mohl být někdo online zraňován.

7 Prodiskutujte všechny body a společně si z nich vytvořte alespoň 5 důležitých bodů pro bezpečné chování online.

CO VŠECHNO O VÁS PROZRADÍ VÁŠ MOBIL/PC?

Zde se můžete podívat, co jsme schopni zjistit o vašem mobilním zařízení (/vás) bez toho, aniž byste nám dali váš souhlas. Otevřete si web: https://selfcheck.tegram.cz/ (nebo na QR kódu) a přesvědčte se sami.

SHRNUTÍ

Zjistili jsme, že bezpečné chování na internetu znamená přemýšlet, co sdílíme, komu věříme a na co klikáme. Naučili jsme se poznat podezřelé zprávy, falešné profily i rizika spojená s osobními údaji a digitální stopou.

Poznámka pro učitele: Úloha je vhodná jako úvod do tématu kyberbezpečnosti. Lze na ni navázat například tématy: silná hesla a zabezpečení účtů, ověřování informací a fake news, bezpečné chování na sociálních sítích, kyberšikana a pomoc v rizikové situaci.