Zaštita privatnosti na internetu

Tema: Savjeti za sigurno korištenje interneta

Dobna skupina: 8. razred

Ciljevi
ikt A.3.3. Učenik aktivno sudjeluje u oblikovanju vlastitoga sigurnog digitalnog okružja.
ikt B.3.1. Učenik samostalno komunicira s poznatim osobama u sigurnome digitalnom okružju.
ikt B.3.2. Učenik samostalno surađuje s poznatim osobama u sigurnome digitalnom okružju.

Potrebni materijali: pripremljena power-point prezentacija *Sigurnost na internetu*, Wordwall kviz *Oblici elektroničkog nasilja*, infografika *Savjeti za sigurnost na internetu*

Izvor: *Obitelj i izazovi novih medija.* 2016. Društvo za komunikacijsku i medijsku kulturu. Zagreb

Scenarij radionice

Uvodna aktivnost (10 minuta)

Započnite radionicu igrom zagrijavanja. Recite neka ustanu/dignu ruku svi koji....

- Igraju igrice na računalu
- Koji imaju facebook
- Koji su govorili istinu koliko imaju godina kada su otvarali facebook ili neku drugu društvenu mrežu
- Koji dijele osobne informacije na društvenim mrežama
- Koji rado dijele osobne fotografije na internetu

Pitanja

- Ima li vaš razred razredna pravila?
- Kako i zašto su donesena?
- Čemu pravila služe?
- Što mislite bi li bilo dobro da nema pravila? Zašto?
- Pitajte jesu li čuli za pravila ponašanja na internetu?

Recite učenicima da je današnja tema *Savjeti za korištenje interneta* te da će danas naučiti kako se koristiti internetom na siguran način.

Pitajte učenike:
Na što trebamo obratiti pažnju kada se služimo internetom?
Kako se trebamo ponašati na internetu?

Kroz potpitanja i raspravu vodite ih zaključcima kako trebamo uvažavati druge, čuvati svoju privatnost i biti sigurni.

Središnja aktivnost (30 minuta)

Učenicima prikažite prezentaciju ***Sigurnost na internetu***. Uz prezentaciju objasnite ***savjete za sigurno korištenje interneta***:

- Ne dijelite svoje fotografije i osobne fotografije putem Interneta – lako ih je zloupotrijebiti
- Ne dijelite svoje lozinke i čuvajte svoje profile na društvenim mrežama privatnima
- Nemojte putem mreža dogovarati sastanke s ljudima koje ne poznajete osobno ili bez dopuštenja odrasle osobe od povjerenja.
- Obavijestite odraslu osobu ako se osjećate neugodno zbog bilo čega što vidite na internetu.
- Ponajprije zbog vlastite sigurnosti, a zatim i sigurnosti samog uređaja provjerite izvore informacija.

Učenicima objasnite pojam ***digitalnih tragova*** (sve informacije koje ostavljamo služeći se internetom). Mogu biti pasivni i aktivni, kao i pozitivni i negativni.

Uz prezentaciju učenicima objasnite kakvim se ***opasnostima*** izlažu ukoliko se ne budu pridržavali navedenih savjeta. Postoje dvije vrste napada – izravni i napad preko posrednika. Za razliku od izravnog napada, kod napada preko posrednika, osoba napada drugu osobu preko treće osobe, najčešće njezinog profila na društvenim mrežama, a da ta osoba toga nije ni svjesna. Učenike upoznajte s različitim vrstama elektroničkog nasilja: spam, phishing, sexting, happy slapping, grooming, cyber uhođenje, flaming,…

Tijekom objašnjavanja poželjno je navoditi stvarne primjere opasnosti ukoliko ih poznajete i upitati učenike jesu li oni upoznati s nekim od navedenih vrsta nasilja, te ukoliko jesu u kojem obliku (svjedok, žrtva i /ili zlostavljač).

Na kraju power point prezentacije je Wordwall kviz *Oblici elektroničkog nasilja* putem kojeg ćete s učenicima provjeriti koliko su zapamtili i utvrditi naučeno.

Završna aktivnost (5 minuta)

Ponovite o čemu ste danas razgovarali.
Učenicima podijelite infografiku *Savjeti za sigurnost na internetu*. Oni je nose kući kako bi mogli objasniti roditeljima o čemu su u školi razgovarali i zajedno s njima još jednom raspraviti o sigurnosti na internetu.