

KIBERNETIČKA SIGURNOST ZA NASTAVNIKE

Praktične smjernice za sigurnije korištenje interneta i školskih digitalnih sustava

Kao nastavnik radite s osobnim podacima učenika, školskom dokumentacijom i službenim računima. Sigurne digitalne navike zato štite i vas i cijelu školsku zajednicu.

1. Prepoznajte najčešće prijetnje

- Phishing: poruke koje izgledaju kao da dolaze od banke, škole, dostavne službe ili poznate tvrtke i pokušavaju vas navesti da kliknete na poveznicu i unesete podatke.
- Malware: zlonamjerni programi koji mogu oštetiti uređaj, ukrasti podatke ili omogućiti neovlašten pristup sustavu.
- Ransomware: zaključava datoteke i traži otkupninu; često se širi sumnjivim privitcima.
- Spyware: tajno prati lozinke, poruke, podatke o karticama i druge osjetljive informacije.

ZNAKOVI UPOZORENJA: hitnost i pritisak, gramatičke greške, nepoznati pošiljatelj, čudne poveznice, neočekivani zahtjevi za uplatu ili traženje lozinke/PIN-a.

2. Zaštitite službene račune i lozinke

- Koristite snažne lozinke s najmanje 12 znakova, kombinacijom velikih i malih slova, brojeva i posebnih znakova.
- Nemojte koristiti istu lozinku na više različitih računa.
- Uključite dvofaktorsku autentifikaciju (2FA) gdje god je dostupna – putem aplikacije, SMS koda ili sigurnosnog ključa.

3. Posebno pazite na podatke učenika

- Školski sustavi sadrže osobne podatke učenika, podatke djelatnika i financijsku dokumentaciju, zbog čega mogu biti meta napada.
- Za službenu komunikaciju koristite službene komunikacijske kanale.
- Prije otvaranja privitka ili slanja podataka provjerite autentičnost poruke i pošiljatelja.
- Ne dijelite osobne podatke učenika bez potrebe.

4. Sigurna uporaba uređaja i mreža

- Redovito ažurirajte računalo, mobitel, aplikacije i operacijski sustav.
- Ne instalirajte nepoznate aplikacije i koristite antivirusni program.
- Zaključavajte mobitel i druge uređaje kada ih ne koristite.
- Budite oprezni na javnim Wi-Fi mrežama; dokument preporučuje korištenje VPN-a radi zaštite prometa.

5. Što učiniti kada poruka izgleda sumnjivo?

1. Ne klikajte na poveznice i ne otvarajte privitke.
2. Provjerite adresu pošiljatelja i smislenost zahtjeva.
3. Ako se traže lozinka, PIN ili neočekivana uplata, tretirajte poruku kao sumnjivu.
4. Ako sumnja ostaje, prijavite aktivnost školskom administratoru ili se obratite nastavnicima informatike.

KLJUČNO PRAVILO: Ako nešto izgleda čudno – stanite, provjerite i tek tada postupite.

Brzi podsjetnik za svaki radni dan

- Jaka i jedinstvena lozinka.
- Uključena 2FA zaštita.
- Ažurirani uređaji i aplikacije.
- Bez otvaranja sumnjivih privitaka.
- Službeni kanali za školsku komunikaciju.
- Sumnjive aktivnosti prijaviti administratoru.