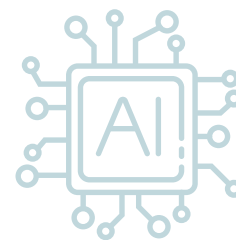




TEHISINTELLEKT JA TURVALISUS



Aine: Informaatika

Teema: Tehisintellekti (*artificial intelligence* - AI) turvalisus



Tunnikava on mõeldud õpilastele **alates 10. klassist**, kuid seda on võimalik kohandada (lihtsustada) ka teema käsitlemiseks nooremate õpilastega.

EESMÄRK:

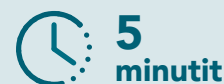
- Tutvustada õpilastele tehisintellekti turvalisuse põhimõtteid.
- Teha õpilased teadlikuks tehisintellekti tehnoloogiaga seotud võimalikest ohtudest ja väljakutsetest.
- Anda õpilastele põhiteadmised ja praktilised oskused end digimaailmas kaitsta.

MATERJALID:

1. Esitlus
2. Tahvel ja markerid
3. Internetiühendusega seadmed praktiliseks ülesandeks (vajadusel)
4. Töölehed praktilise ülesande jaoks (valikuline)

Tunnikava on koostanud Birgy Lorenz, küberkaitse vanemteadur Tallinna Tehnikaülikooli IT Kolledžis, projekti Targalt internetis raames.

1. Sissejuhatus



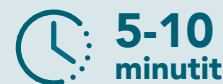
- a. Tervita õpilasi ja loo positiivne õpikeskkond.
- b. Alusta küsimusega, kas õpilased on kuulnud tehisintellektist ja mida nad selle kohta teavad.
- c. Selgita lühidalt, et tehisintellekt on võimas tehnoloogia, mida kasutatakse mitmesugustes rakendustes, kuid sellega kaasnevad ka turvalisusega seotud väljakutsed.

2. Tehisintellekti turvalisuse mõistmine



- Esita lihtne ja õpilastele sobiv selgitus tehisintellekti turvalisuse kohta, keskendudes sellele, kuidas tehisintellekt võib olla haavatav rünnakutele ja väärkasutusele.
- Arutage võimalikke tehisintellekti turvalisuse probleeme, nagu andmete privaatsus, eelarvamuslikud algoritmid ja tehisintellekti võimalik manipuleerimine.

3. Tehisintellekti turvalisuse riskide tuvastamine



- Kaasa õpilased arutellu erinevate tehisintellekti rakenduste üle, mida nad kasutavad või millega kokku puutuvad, näiteks virtuaalsed assistendid, mängud või haridusvahendid.
- Palu õpilastel tuvastada nende tehisintellekti rakenduste võimalikud turvariskid.
- Kirjuta õpilaste vastused tahvlile ja arutlege iga riski üle lühidalt.

4. Praktiline ülesanne: Turvariskide märkamine



- Jaga õpilased väikestesse gruppidesse.
- Anna igale grupile arvuti/tahvel (vajadusel) või töölehed tehisintellekti rakendustega seotud stsenaariumidega.
- Juhenda neid stsenaariume analüüsima ja võimalikke turvariske või haavatavusi tuvastama.
- Julgusta õpilasi oma gruppides arutlema.
- Palu igal grupil esitada oma leiud klassile ja arutada välja pakutud lahendusi või ennetavaid meetmeid.

5. Kokkuvõte ja olulised mõtted



- Tee lühike kokkuvõte tunnis käsitletud põhipunktidest.
- Rõhuta digitaalse ohutuse ja turvalisuse olulisust tehisintellekti või ükskõik millise tehnoloogia kasutamisel.
- Julgusta õpilasi olema ettevaatlikud isikuandmete jagamisel ja kui nad satuvad turvalisusprobleemiga silmitsi, otsima abi usaldusväärselt täiskasvanutelt.

6. Küsimused ja tagasiside



- Anna õpilastele aega küsimuste esitamiseks, mis neil tehisintellekti turvalisuse kohta võivad tekkinud olla.
- Kogu õpilastelt tagasisidet nende õpikogemuse kohta.