****

*Õppematerjalid on loodud Euroopa Liidu Euroopa Sotsiaalfondi meetme „Kaasaegse ja uuendusliku õppevara arendamine ja kasutuselevõtt“ (2014-2020.1.03.15-0001) raames.*

**Õpetajale lisalugemiseks III kooliastme õpiku “Infoühiskonna tehnoloogiad” esimese osa kohta**

Õpik: <https://web.htk.tlu.ee/informaatika/infoyhiskond/>

Autorid:

**Birgy Lorenz**, Tallinna Tehnikaülikool, Pelgulinna Gümnaasium, Eesti Informaatikaõpetajate Selts

**Maris Valdmets**, Püünsi Kool, Eesti Informaatikaõpetajate Selts

Maris Valdmets, on loonud õpiku I osa kohta ka [7. klassile töökava.](https://docs.google.com/document/d/1d7Qw8tVQsINvJmnCiS1gBqIYMC09cqSv2T0rmS0Z95E/edit?usp=sharing)

Õpiku esimene osa koosneb kaheksast peatükist ja annab ülevaate infoühiskonnast.

Põhikooli informaatikaõpetusega taotletakse, et õpilane

* mõistab digitehnoloogia tööpõhimõtteid ning valdab peamisi võtteid igapäevases õppetöös infot otsides, töödeldes ja analüüsides ning taasesitades;
* loob, salvestab, taasesitab ja jagab digitehnoloogiliste vahendite abil eesmärgist lähtuvalt digitaalset sisu, järgides privaatsusnõudeid;
* teadvustab ning väldib digitaalses keskkonnas tegutsedes tekkida võivaid riske tervisele, turvalisusele ja isikuandmetele;
* omab õpiteeks ja karjäärivalikuks vajalikke oskusi ja teadmisi.

Õpiku I osa peatükid:

* [Mis on infoühiskond?](https://web.htk.tlu.ee/informaatika/infoyhiskond/chapter/mis-on-infoyhiskond/)
* [Eesti e-riik ja e-teenused](https://web.htk.tlu.ee/informaatika/infoyhiskond/chapter/eesti-e-riik-ja-e-teenused/)
* [Infoühiskonna mängureeglid](https://web.htk.tlu.ee/informaatika/infoyhiskond/chapter/infouhiskonna-mangureeglid/)
* [Isikuandmed ja nende elukaar](https://web.htk.tlu.ee/informaatika/infoyhiskond/chapter/e-teenused-ja-nende-elukaar/)
* [Turvaline käitumine internetis ja küberkuritegevus](https://web.htk.tlu.ee/informaatika/infoyhiskond/chapter/turvaline-kaitumine-internetis-ja-kyberkuritegevus/)
* [Isiklik turvaaudit](https://web.htk.tlu.ee/informaatika/infoyhiskond/chapter/isiklik_turvaaudit/)
* [Enda digipädevuse hindamine](https://web.htk.tlu.ee/informaatika/infoyhiskond/chapter/enda-digipadevuse-hindamine/)
* [Karjäär ja IKT](https://web.htk.tlu.ee/informaatika/infoyhiskond/chapter/karjaar-ja-it/)

**Mis on infoühiskond?**

Peatüki eesmärk on anda ülevaade ühiskonna erinevatest liikidest, digilõhest Eesti ühiskonnas, e-teenustest infoühiskonnas ja teenusedisaini olulisusest e-teenuste loomisel. Ühiskonna erinevate alaliikidega tutvumine loob seose ajaloo ja ühiskonnaõpetusega ning selgitab, mis on ühe või teise ühiskonnaliigi aluseks. Õppijad omandavad mõiste „infoühiskond“ ja „teenusedisain“. Samamoodi saadakse teada ametist teenusedisainer.

Ülesanne Statistikaameti andmebaasiga suunab õppijaid kasutama vabalt kättesaadavat andmebaasi ja arutlema, kas meie kogemus oma peres või kogukonnas on sarnane Eesist teistega. Ülesanne StartUp Estonia andmebaasis suunab õppijaid tutvuma uute ettevõtetega, kes teevad Eestit maailmas tuntuks ja lahendavad erinevaid infoühiskonda saatvaid probleeme.

Mõtteid infoühiskonnast:

* Infoühiskond on ühiskonna mõiste, mis kirjeldab infotehnoloogia mõju ja levikut kogu ühiskonnas. Infoühiskond tähendab ühiskonda, kus informatsioon on muutunud väga oluliseks ressursiks ning tehnoloogia areng on toonud kaasa suured muutused majanduses, kultuuris ja poliitikas. Infoühiskond hõlmab mitmeid erinevaid valdkondi, sealhulgas tehnoloogia, kommunikatsioon, haridus, meedia ja tööhõive. Infoühiskond võimaldab inimestel kiiret ja lihtsat juurdepääsu informatsioonile, suhtlemist kaugel asuvate inimestega ning uusi viise töötamiseks ja teenuste osutamiseks. Infoühiskond on muutnud ka seda, kuidas inimesed suhtlevad ja informatsiooni levitavad. Sotsiaalmeedia ja muud digitaalsed platvormid on muutnud meie suhtlusviise ning võimaldanud kiiremat ja laiemat informatsiooni levikut. Samuti on infoühiskond loonud uusi võimalusi töö tegemiseks kaugtööna ning loonud uusi töökohti infotehnoloogia valdkonnas. Kokkuvõttes võib öelda, et infoühiskond on ühiskond, kus info- ja kommunikatsioonitehnoloogia mõju on laialt levinud ja oluline kõigis eluvaldkondades.
* Digilõhe (inglise keeles *digital divide*) on mõiste, mis kirjeldab digitaalset ebavõrdsust ühiskonnas. See tähendab, et mõned inimesed või grupid omavad suuremat juurdepääsu ja oskusi kasutada infotehnoloogiat ja interneti ressursse, samal ajal kui teised on nende vahendite kasutamises piiratud või üldse ilma nendeta. Digilõhe võib esineda erinevates vormides. Näiteks võib see olla juurdepääsulõhe, kus mõned inimesed ei saa endale lubada või elavad piirkonnas, kus puudub lairiba internetiühendus. Samuti võib digilõhe olla oskuste lõhe, kus mõned inimesed ei ole piisavalt koolitatud või enesekindlad, et kasutada infotehnoloogiat või interneti ressursse tõhusalt. Digilõhe võib tekitada erinevaid probleeme. Näiteks võib see suurendada sotsiaalset ebavõrdsust ja eraldatust, kuna mõned inimesed ei saa kasutada või ei ole kursis digitaalsete teenuste ja ressurssidega. Samuti võib digilõhe piirata majanduslikku arengut, kuna digitaalsed oskused on üha olulisemad tööturul ning ilma nendeta võivad inimesed jääda tööpuudusesse või vähem konkurentsivõimelisteks. Digilõhe vähendamiseks tehakse mitmeid jõupingutusi, nagu näiteks lairiba internetiühenduse laiendamine, infotehnoloogia koolituste pakkumine ja digitaalsete teenuste kättesaadavamaks tegemine. E-teenused on elektroonilised teenused, mida osutatakse infoühiskonnas läbi infotehnoloogia vahendite. E-teenused on sageli kättesaadavad veebipõhiste rakenduste kaudu ning võimaldavad kasutajatel teha mitmesuguseid toiminguid, nagu näiteks tellida kaupu ja teenuseid, saada teavet, maksta arveid või täita dokumente. E-teenused on saanud üha olulisemaks infoühiskonnas, kuna need võimaldavad inimestel mugavalt ja kiiresti saada juurdepääsu erinevatele teenustele ja ressurssidele. E-teenused on samuti oluline vahend ettevõtetele ja organisatsioonidele, kuna need võimaldavad neil pakkuda teenuseid efektiivsemalt ning saavutada suuremat kliendibaasi. E-teenused võivad hõlmata mitmeid erinevaid valdkondi, sealhulgas tervishoid, haridus, pangandus, valitsusasutused ja rohkem. Näiteks võivad tervishoiuteenused hõlmata online-konsultatsioone, elektroonilist retsepti ja patsiendiportaale, kus patsiendid saavad vaadata oma terviseandmeid. Haridusvaldkonnas võivad e-teenused hõlmata online-kursusi, virtuaalseid õppekogukondi ja elektroonilisi õpikuid. Panganduses võivad e-teenused hõlmata mobiilipanga rakendusi, elektroonilist makseteenuseid ja investeerimisplatvorme. E-teenuste arendamine ja kasutuselevõtt võib aidata kaasa infoühiskonna arengule, kuna need võimaldavad inimestel kiiret ja mugavat juurdepääsu erinevatele teenustele ja ressurssidele. Samas on oluline tagada, et e-teenuste kasutamine oleks kättesaadav kõigile ning digilõhe ei tekiks või süveneks.
* Teenusedisain on lähenemisviis teenuste loomiseks ja arendamiseks, mis keskendub kliendi vajadustele ja kogemusele teenuse kasutamisel. Teenusedisain hõlmab mitmeid erinevaid tegevusi ja protsesse, nagu kliendi uurimine, teenuste disainimine ja prototüüpimine ning teenuse juurutamine ja jälgimine. Teenusedisaini eesmärk on luua teenuseid, mis vastavad klientide ootustele ja vajadustele, ning parandada klientide kasutuskogemust teenuste kasutamisel. Selleks võib teenusedisain kasutada erinevaid meetodeid ja vahendeid, nagu näiteks klientide intervjuusid, empaatiakaarte, kliendi teekonna kaardistamist, prototüüpimist ja testimist. Teenusedisaini võib rakendada erinevates valdkondades, sealhulgas panganduses, tervishoius, jaemüügis, transportimises ja rohkem. Näiteks võib teenusedisaini abil disainida pangateenuseid, mis on lihtsad ja mugavad kasutada, või tervishoiuteenuseid, mis võimaldavad patsientidel kiiresti ja tõhusalt juurde pääseda arstiabi. Teenusedisain võib aidata ettevõtetel ja organisatsioonidel luua konkurentsieelist ja paremini teenida klientide vajadusi. Samuti võib see parandada teenuste kvaliteeti ja tõhusust ning vähendada teenuste kasutamisest tulenevat ebamugavust ja stressi.

**Eesti e-riik ja e-teenused**

Peatüki eesmärk on teha ülevaade e-Eesti toimimisest, erinevatest e-teenustest riigis ja sellest, kuidas neid teenuseid kasutada. Õppijad omandavad mõiste „isikutunnistus“. Samamoodi saadakse teada ametist kasutajatoe spetsialist. Video X-teest annab õppijate teada, kui keeruline ja võimas on e-Eesti IT-süsteem. Ülesanded ja küsimused e-teenustest annavad õppijale teada, kuidas kasutada e-teenuseid Eestis nagu ID-kaart, allkirjastamine, bussipileti soetamine või rongiaegade vaatamine. Teenused on samad nii noorele ja vanale, kui oled algaja teemas, siis on üsna loogiline, et omandame ülesandeid sarnases keskkonnas.

Mõtteid Eestist ja e-riigist:

* Eesti on üks maailma juhtivaid riike digitaaltehnoloogia kasutamises ja arendamises. E-Eesti tähendab seda, et Eesti on loonud digitaalse keskkonna, mis võimaldab inimestel ja ettevõtetel mugavalt ja turvaliselt teha toiminguid, nagu näiteks hääletamine, pangandus, tervishoid ja valitsusasutuste teenuste kasutamine. E-Eesti edulugu sai alguse juba 1990-ndate alguses, kui Eesti iseseisvus Venemaalt ja hakkas arendama oma infosüsteeme. Eesti valitsus nägi digitaaltehnoloogia võimalusi juba varakult ning alustas digitaalsete teenuste väljatöötamist juba 2000. aastatel. Täna on Eestis kättesaadavad paljud e-teenused, mis hõlbustavad oluliselt inimeste ja ettevõtete igapäevaelu. E-Eesti lahendused põhinevad avatud ja turvalisel tehnoloogial ning tagavad kasutajate privaatsuse ja andmekaitse. E-Eesti süsteemid on ühtsed ning võimaldavad erinevate teenuste kasutamist ühe kasutajakonto kaudu. Näiteks saab inimene Eesti e-riigi portaalile sisse logida ID-kaardi, mobiil-ID või Smart-ID abil ning seejärel kasutada mitmeid teenuseid, sealhulgas maksuameti teenuseid, tervishoiuteenuseid, hääletamisteenuseid ja palju muud. E-Eesti on muutunud üheks Eesti majanduse alustalaks, aidates kaasa majanduskasvule ja ettevõtluse arengule. Eesti on loonud viljakad tingimused ettevõtluseks, nagu madal bürokraatia, kiire asjaajamine ja madalad kulud, mis võimaldavad ettevõtjatel tõhusalt tegutseda. Lisaks on Eesti kujunenud rahvusvaheliselt tuntud e-riigiks, kus on toimunud palju innovatsiooni ja avatud tehnoloogia arendamist.
* Eesti ID-kaart on ametlik isikutunnistus, mis on välja antud Eesti kodanikele ja elanikele. ID-kaardil on isiku foto, nimi, isikukood ja allkiri ning see on seaduslikult tunnustatud dokument Eestis ja Euroopa Liidus. ID-kaardil on ka mikrokiip, mis sisaldab isikuandmeid ja võimaldab digitaalset autentimist, allkirjastamist ja krüpteerimist. ID-kaarti saab kasutada, näiteks e-teenuste kasutamisel, panganduses, meditsiinis ja reisimisel. ID-kaart võimaldab kasutajal autentida end digitaalselt, allkirjastada dokumente ja krüpteerida andmeid, mis tagab turvalisuse ja privaatsuse. Lisaks sellele, et ID-kaart on isikutunnistus, on see ka rahvusvaheliselt tunnustatud reisidokument, mis võimaldab Eesti kodanikel reisida paljudesse riikidesse viisavabalt või viisat saades. ID-kaardi väljastamine on Eestis tasuta ning seda saab taotleda Eesti kodanikud ja Eestis elavad välismaalased. ID-kaart on oluline osa Eesti e-riigi süsteemist ja on aidanud kaasa Eesti digitaalsete teenuste arengule ja edule.
* E-teenused Eestis jagunevad tõepoolest kolme kategooriasse: riiklikud teenused, kohaliku omavalitsuse teenused ja eraettevõtjate teenused. Kõik need teenused on osa Eesti e-riigi ökosüsteemist, mis on loodud selleks, et muuta kodanike ja ettevõtete elu lihtsamaks, kiiremaks ja mugavamaks. E-teenused on muutunud oluliseks osaks Eesti majandusest ja ühiskonnast, tagades kiire ja tõhusa asjaajamise ning vähendades bürokraatiat ja kulusid. Selgitame neid kategooriaid lähemalt:
	+ Riiklikud teenused: Need on teenused, mida pakuvad Eesti riigi asutused, nagu näiteks maksuamet, terviseamet, politsei- ja piirivalveamet jne. Need teenused hõlmavad näiteks e-maksudeklaratsioonide esitamist, terviseandmete vaatamist ja muutmist, politseile avalduste esitamist jne. Riiklike teenuste kasutamiseks peab inimene esmalt autentima end ID-kaardi, mobiil-ID või Smart-ID abil.
	+ Kohaliku omavalitsuse teenused: Need on teenused, mida pakuvad kohalikud omavalitsused, nagu näiteks linnavalitsused ja vallavalitsused. Need teenused hõlmavad näiteks lapsehoiuteenuste taotlemist, ehituslubade taotlemist, parkimislubade taotlemist jne. Kohalike omavalitsuste e-teenused on kättesaadavad enamikus Eesti omavalitsustes ning neid saab kasutada samamoodi nagu riiklikke teenuseid, autentides ennast ID-kaardi, mobiil-ID või Smart-ID abil.
	+ Eraettevõtjate teenused: Need on teenused, mida pakuvad eraettevõtted, näiteks pangad, kindlustusfirmad, elektroonikakaupluste jne. Need teenused hõlmavad näiteks pangakonto avamist, kindlustuspoliiside ostmist, elektroonikatoodete tellimist jne. Eraettevõtjate teenused on kättesaadavad veebi- ja mobiilirakenduste kaudu ning neid saab kasutada samamoodi nagu riiklikke ja kohaliku omavalitsuse teenuseid, autentides ennast ID-kaardi, mobiil-ID või Smart-ID abil. Kuid eraettevõtjaid on ka välismaal ja ka Eestis, kes pakuvad võimaluse oma teenuseid kasutada ka parooliga või mitmefaktorilise autentimisvõimalusega nt mobiiltelefoniga.

**Infoühiskonna mängureeglid**

Peatüki eesmärk on selgitada, mis on infovabadus, infosõda ja reeglid ühiskonnas. Õppijad omandavad mõiste „infovabadus“. Samamoodi saadakse teada tegelasest nagu häkker ja kräkker. Video kasulikest idiootidest annab õppijate teada, kui oluline on igaühel mõista, mis on internetis sotsiaalse manipulatsiooni taga ning kuidas mitte sattuda teenustõkkerünnaku otsa. Ülesanded ja küsimused e-teenustest annavad õppijale teada erinevatest väljakutsetest internetis toimetamisel. Peatükk on üsna keeruline, seega vastavalt õppijate eelnevatele kogemustele ja oskustele, tuleks õpetajal materjal muuta õppijale lihtsamaks.

Mõtteid infovabadusest:

* Vabadus internetis võib tähendada erinevaid asju, kuid tavaliselt viitab see sellele, et inimesed saavad kasutada internetti ilma piiranguteta ja ilma hirmuta tsensuuri, jälgimise, ebaseadusliku jälgimise ja muude rikkumiste ees. Vabadus internetis on inimeste õigus avaldada oma arvamust, saada teavet, suhelda teiste inimestega ja luua sisu ilma igasuguse hirmuta selle eest, et nende tegevus võib olla keelatud või nende vabadust piirata. Vabadus internetis on seotud ka õigustega nagu privaatsus ja sõnavabadus. See tähendab, et inimestel on õigus säilitada oma privaatsus ja kontrollida, kuidas nende isikuandmeid töödeldakse. Samuti on neil õigus oma arvamust väljendada ilma hirmuta tagakiusamise ees. Paljudes riikides võivad inimesed aga kokku puutuda interneti piiramise ja tsensuuriga, kus valitsused või muud asutused võivad blokeerida juurdepääsu teatud veebisaitidele, jälgida inimeste tegevust või kehtestada muid piiranguid, mis võivad takistada vaba interneti kasutamist. Seega on vabadus internetis oluline väärtus, mida tuleb kaitsta ja säilitada.
* Kui internet on inimõigus, tähendab see, et inimestel peaks olema õigus juurdepääsule internetile ja selle kasutamisele ilma diskrimineerimise ja takistusteta. See hõlmab õigust interneti kasutamisele, sellele ligipääsule, informatsioonile internetis ja sõnavabadusele internetis. Interneti kui inimõiguse tunnustamine tähendab, et valitsused ja muud asutused peaksid tagama, et internet oleks kättesaadav kõigile inimestele, olenemata nende majanduslikust või sotsiaalsest seisundist, ja et selle kasutamine ei oleks diskrimineeriv ega rikkuvaks kuidagi nende õigusi. Interneti kui inimõiguse tunnustamine on oluline ka seetõttu, et internet on muutunud oluliseks meediumiks info jagamiseks, suhtlemiseks, hariduse saamiseks, poliitiliseks kaasamiseks ja majandustegevuseks. Seega on oluline tagada, et kõigil oleks juurdepääs internetile ja sellele, mida see pakub, ning et seda ei saaks kasutada inimeste õiguste rikkumiseks või diskrimineerimiseks.
* Tsensuur piirab inimeste sõnavabadust ja õigust saada teavet ning piirab sellega demokraatia ja inimõiguste olulisi aluseid. Tsensuuri eesmärk on piirata teatud tüüpi teavet või sisu levikut, tavaliselt selleks, et valitsused või muud autoriteedid saaksid kontrollida inimeste arvamusi, tegevusi ja käitumist. Tsensuur võib takistada inimestel väljendada oma arvamust, saada juurdepääsu erinevatele ideedele ja mõtteviisidele ning piirata teatud teemade arutamist. See võib viia ühepoolse teabevahetuse ja arvamuste moonutamiseni ning võib takistada uute ideede ja lahenduste leidmist. Tsensuur võib ka piirata ajakirjandusvabadust, kuna see võib keelata teatud uudiste ja teemade kajastamise, mis võib olla kriitiline või ebamugav võimudele või teatud huvirühmadele. Tsensuur võib olla ka vastuolus inimõiguste, sealhulgas sõnavabaduse ja mõtte-, südametunnistuse- ja veendumusvabadusega. See võib piirata inimeste õigust informatsioonile, mis on vajalik nende valikute ja otsuste tegemiseks. Seega on tsensuur halb, sest see takistab inimeste võimalusi saada teavet ja jagada oma arvamusi ning võib piirata nende vabadust ja demokraatia aluseid.
* Infosõda on tegevus, mille eesmärk on mõjutada ja kontrollida teiste riikide või organisatsioonide infotehnoloogia süsteeme ja kommunikatsioonivõrke. Infosõda hõlmab laias valikus tegevusi, sealhulgas arvutiviiruste levitamist, häkkerite rünnakuid, valeinformatsiooni ja propaganda levitamist, küberväljapealsete konfliktide ja sotsiaalmeedia võrgustike manipulatsiooni. Infosõda on muutunud oluliseks küberruumis, kus riigid ja organisatsioonid võistlevad strateegilise teabe, majandusliku konkurentsi ja poliitilise mõju saavutamise eesmärgil. Infosõda võib olla ka riikide vahelise konflikti lahendamise osa, kus infosõja eesmärk on teise riigi või organisatsiooni võimete ja ressursside nõrgestamine või hävitamine. Infosõda võib olla ohtlik, kuna see võib kahjustada olulisi infotehnoloogia süsteeme, põhjustada majanduslikku kahju, häirida ühiskondlikku stabiilsust ja ohustada rahvuslikku julgeolekut. Seetõttu on infosõda saanud tähelepanu rahvusvaheliste julgeolekuorganisatsioonide ja valitsuste poolt, kes töötavad välja meetmeid ja poliitikaid, et kaitsta oma infotehnoloogia süsteeme ja riiklikke huve infosõja eest.
* Internetis kehtivad samad seadused ja reeglid nagu ka väljaspool seda. Kuid Interneti eripära tõttu võib olla keeruline jälitada ja kaitsta inimeste õigusi ja turvalisust, seega on Internetis kehtestatud mitmeid reegleid ja eeskirju, mida tuleb järgida. Need on vaid mõned näited Interneti reeglitest. Oluline on meeles pidada, et Interneti kasutamisel on kaasas vastutus ning et teatud tegevused võivad olla ebaseaduslikud või kahjustada teisi inimesi. Seetõttu on oluline järgida Interneti reegleid ja käituda vastutustundlikult, et kaitsta enda ja teiste inimeste õigusi ja turvalisust Internetis. Mõned näited interneti reeglitest on järgmised:
	+ Autoriõiguste järgimine: Internetis levitatakse palju sisu, sealhulgas fotosid, videoid, tekste jne, mis on autorikaitsega kaitstud. Seetõttu peavad inimesed järgima autorikaitse seadusi ja nõudeid, kui nad soovivad kasutada või jagada autorikaitsega kaitstud materjale.
	+ Privaatsuse ja andmekaitse kaitse: Internetis on isikuandmete kaitse väga oluline. Seda teevad andmekaitse seadused ja reeglid, mis kehtestavad standardid, mida peab järgima, kui kogutakse, töödeldakse ja salvestatakse isikuandmeid.
	+ Interneti turvalisus: Interneti turvalisuse tagamine on oluline, et kaitsta inimesi Internetis pettuste ja rünnakute eest. Seda teevad küberjulgeoleku seadused ja standardid, mis kehtestavad turvanõuded ja kaitsemeetmed.
	+ Netikett: Netikett on interneti hea tava kogum, mis hõlmab viisakuse ja käitumise reegleid, kui kasutatakse Internetti ja suheldakse teiste inimestega. Netikett nõuab, et inimesed käituksid Internetis viisakalt ja austaksid teisi inimesi ning nende õigusi.
* "Häkkerid" ja "kräkkerid" on kaks erinevat terminit, mis sageli segamini ajatakse, kuid millel on erinev tähendus. Häkkerid on inimesed, kes kasutavad oma teadmisi ja oskusi tarkvara või riistvara arendamiseks ning IT-süsteemide parandamiseks ja täiustamiseks. Häkkerid võivad töötada nii turvasektoris kui ka tarkvaraarendajatena ning nad kasutavad oma oskusi, et leida uusi ja innovatiivseid lahendusi probleemidele. Häkkerid on sageli motiveeritud teadmiste omandamisest ja nende jagamisest teiste huvilistega, et aidata kaasa tehnoloogia arengule. Kräkkerid on aga inimesed, kes kasutavad oma oskusi kuritegelikeks eesmärkideks, näiteks andmete varastamiseks, andmebaaside häkkimiseks või teiste inimeste süsteemidesse sissetungimiseks ja nende privaatsuse rikkumiseks. Kräkkerid võivad olla seotud organiseeritud kuritegevusega ja nende eesmärk on sageli raha teenida või tekitada kahju ettevõtetele või isikutele. Seega võib öelda, et häkkerid ja kräkkerid erinevad selle poolest, et häkkerid kasutavad oma oskusi positiivseteks eesmärkideks, samal ajal kui kräkkerid kasutavad oma oskusi kuritegelikeks eesmärkideks. Oluline on meeles pidada, et häkkimine ei ole automaatselt kuritegu, kuid kräkkimine on seda kindlasti.

**Isikuandmed ja nende elukaar**

Peatüki eesmärk on teha ülevaade andmete elukaarest, mis on isikuandmed, mis on digiprügi ja kuidas lahendada isikuandmetega seonduvaid juhtumeid. Õppijad omandavad mõiste „andmeleke“. Samamoodi saadakse teada ametist nagu andmekaitsespetsialist. Videod annavad õppijate teada, kui oluline on igaühel kaitsta oma andmeid. Ülesanded ja küsimused puudutavad seekord andmete käitlemist ja hävitamist kui ka digiprügi vähendamise võimalusi.

Mõtteid andmetest:

* Andmete elukaar (inglise keeles *data lifecycle*) viitab andmete läbimisele kogu elutsükli jooksul, alates nende loomisest või kogumisest kuni nende säilitamise, kasutamise, jagamise ja lõpuks hävitamiseni. Andmete elukaare kontseptsioon hõlmab kogu protsessi, mida andmed läbivad oma eksistentsi jooksul, ning on oluline andmekaitse, andmeanalüüsi ja andmete haldamise seisukohalt. Andmete elukaar võib varieeruda sõltuvalt andmete tüübist ja kasutusotstarbest, kuid tavaliselt sisaldab see järgmisi etappe: Kogumine ja loomine: andmed kogutakse või loovad kas inimesed, seadmed või muud allikad; Töötlemine ja salvestamine: andmed salvestatakse ja töödeldakse, et neid saaks kasutada analüüsi, haldamise või mõne muu eesmärgi jaoks; Kasutamine ja jagamine: andmed jagatakse ja kasutatakse erinevates kontekstides ja otstarvetes; Säilitamine ja arhiveerimine: andmed säilitatakse nende kasuliku eluea jooksul vastavalt seadusandlikele, regulatiivsetele ja eetilistele nõuetele; Kustutamine või hävitamine: andmed kustutatakse või hävitatakse pärast nende kasuliku eluea lõppemist või vastavalt seadusandlikele, regulatiivsetele ja eetilistele nõuetele. Andmete elukaar on oluline kontseptsioon andmete haldamiseks ja kaitseks, sest see aitab mõista, kuidas andmeid kogutakse, töödeldakse ja jagatakse, ning võimaldab välja töötada andmekaitsestrateegiaid, mis tagavad andmete turvalisuse ja privaatsuse igal etapil.
* Konfidentsiaalsus-ligipääsetavus-terviklikkus on infoturbe põhiprintsiibid, mis tagavad andmete turvalisuse ja konfidentsiaalsuse ning väldivad nende tahtmatut või volitamata kasutamist. Selgitame neid printsiipe lähemalt: konfidentsiaalsus: see tähendab, et teatud andmeid peab nägema ainult see inimene või organisatsioon, kellel on selleks õigused. Konfidentsiaalsus on oluline eriti tundlike või isiklike andmete nagu terviseandmete, finantsteabe või ärisaladuste puhul. Andmete konfidentsiaalsuse tagamine hoiab ära nende lekkimise, varguse või muu volitamata juurdepääsu. Ligipääsetavus: see tähendab, et andmete muutmiseks või töötlemiseks peab olema selleks luba või õigus. Ligipääsetavus on oluline, et tagada, et andmed on ajakohased, täpsed ja sobivad kasutuseesmärgiks. Kui andmeid saavad muuta või töödelda ainult need inimesed või süsteemid, kellel on selleks õigused, välditakse teadmatut andmete rikkumist või moonutamist. Terviklikkus: see tähendab, et andmed peavad olema õiged ja täpsed. Terviklikkuse tagamine hoiab ära andmete tahtmatu või pahatahtliku muutmise või moonutamise. Andmete terviklikkuse tagamiseks kasutatakse tavaliselt mitmesuguseid meetodeid, nagu krüpteerimine, digitaalallkirjad ja logimine, mis võimaldavad andmete muutmist tuvastada ja takistada.
* Isikuandmete kaitse on vajalik selleks, et kaitsta inimeste privaatsust ja isikuandmeid, mis on sageli tundlikud ja kergesti väärkasutatavad. Isikuandmete hulka võivad kuuluda näiteks nimi, aadress, sünniaeg, sotsiaalkindlustuse number, terviseandmed, pangaandmed, tööandjaga seotud andmed jne. Isikuandmete kaitse on oluline järgmistel põhjustel: Privaatsuse kaitse: Inimesed peaksid saama oma isikuandmeid hoida privaatsena ja otsustama, kuidas nende andmeid kasutatakse, kellele neid jagatakse ja millist teavet nende kohta avaldatakse. Isikuandmete kaitse tagab, et isikuandmeid ei kasutata volitamata viisil, et kaitsta inimeste eraelu. Identiteedivarguse ennetamine: Isikuandmete kaitsmine on oluline identiteedivarguse ja pettuste ennetamisel. Kui isikuandmed satuvad volitamata isikute kätte, võivad need kasutada andmeid kuritegelike eesmärkide saavutamiseks, sealhulgas võltsimiseks, pettusteks ja identiteedivarguseks. Turvalisus ja usaldusväärsus: Isikuandmete kaitse on oluline, et tagada nende andmete turvalisus ja usaldusväärsus. Kui inimesed teavad, et nende isikuandmeid kaitstakse, suureneb nende usaldus organisatsioonide ja asutuste vastu, mis koguvad ja töötlevad nende isikuandmeid. Seadusandluse nõuded: Isikuandmete kaitse on ka seadusega nõutav. Enamik riike on kehtestanud seadused ja määrused, mis reguleerivad isikuandmete kogumist, töötlemist ja jagamist. Isikuandmete kaitse tagamine on vajalik, et organisatsioonid järgiksid seadusandluse nõudeid ja vältida trahve või muid õiguslikke tagajärgi.
* Digifailide prügi arvutis võib koosneda erinevatest andmetest, mida enam ei kasutata või millel pole enam mingit praktilist väärtust. See võib hõlmata erinevaid faile, kaustu, programme, pilte, videoid, helifaile ja muud digitaalset sisu, mis on teie arvutisse kogunenud. Digifailide prügi arvutis võib mõjutada teie arvuti jõudlust ja mälu kasutamist, samuti võib see muuta teie arvuti vähem turvaliseks, kuna seal võib olla tundlikke andmeid, mida on võimalik taastada. Seega on oluline regulaarselt korrastada oma arvuti digifailide prügi ja kustutada kõik andmed, mida te enam ei vaja. Digiprügi on elektroonilise jäätme, nagu vananenud elektroonikaseadmed, kasutamiskõlbmatud arvutid, printerid, mobiiltelefonid, elektroonilised mänguasjad, kõlarid, telerid, jne., mis vajavad taaskasutamist või korralikku utiliseerimist. Digiprügi on tõsine keskkonnaprobleem, sest kui seda ei käidelda korralikult, võib see kahjustada keskkonda, tervist ja loodusvarasid. Seetõttu on oluline tegeleda digiprügiga mitmel põhjusel: Keskkonnakaitse: Digiprügi sisaldab sageli mürgiseid ja ohtlikke kemikaale, mis võivad kahjustada keskkonda, sealhulgas pinnast, vett ja õhku. Kui digiprügi utiliseeritakse valesti, võivad need kemikaalid sattuda keskkonda ja põhjustada tõsiseid keskkonnaprobleeme. Tervisekaitse: Digiprügis leiduvad ohtlikud ained võivad kahjustada inimeste tervist, kui neid ei käidelda korralikult. Nende hulka kuuluvad raskmetallid, nagu plii, elavhõbe ja kroom, mis võivad põhjustada tõsiseid terviseprobleeme, sealhulgas mürgistust ja vähki. Ressursitõhusus: Digiprügi sisaldab sageli kasulikke materjale, nagu metallid, plastid ja klaas, mis saab ringlusse võtta ja taaskasutada. Kui digiprügi ei töödelda korralikult, raisatakse väärtuslikke ressursse ja suurendatakse prügilatesse ladestamise mõju. Juriidilised nõuded: Paljud riigid on kehtestanud seadused ja määrused, mis reguleerivad digiprügi käitlemist ja utiliseerimist. Need õigusaktid võivad sisaldada nõudeid digiprügi käitlemiseks, et vältida keskkonna- ja terviseprobleeme ning võimalikke õiguslikke tagajärgi. Seega on digiprügi käitlemine oluline, et kaitsta keskkonda, tagada tervisekaitse, vältida ressursside raiskamist ning järgida seadusandlust.

**Turvaline käitumine internetis ja küberkuritegevus**

Peatüki eesmärk on anda ülevaade turvalisest käitumisest internetis, privaatsusseadetest ja keskkondadest ja küberkuritegevuse liikidest kui ka küberturvalisusega seotud ametitest. Õppijad omandavad mõiste „küberkuritegu“. Samamoodi saadakse teada erinevatest küberturvalisuse valdkonna ametinimedest. Videod erinevatest küberkuritegudest annavad õppijate teada, millist liiki pettuseid internetis ja arvutitega tehakse. Ülesanded ja küsimused aitavad mõista, milliseid erinevaid juhtumeid tuleb digitaalses ohutuses ja küberkuritegudena ette.

Mõtteid turvalisest käitumisest ja küberturvalisuse valdonnast:

* Turvaline käitumine internetis hõlmab mitmeid olulisi meetmeid, et kaitsta ennast ja oma andmeid võimalike ohtude eest. Mõned peamised turvalise käitumise viisid internetis on järgmised: Tugevate paroolide kasutamine: Kasutage tugevaid ja erinevaid paroole erinevate kontode jaoks ning muutke neid regulaarselt. Kaheastmeline autentimine: Aktiveerige kaheastmeline autentimine oma kontode jaoks, mis nõuab teie identiteedi kinnitamist ka muul viisil, lisaks paroolile. Turvapäeviku hoidmine: Kirjutage üles oma paroolid, et vältida unustamist. Oluline on aga hoida turvapäevik turvalises kohas. Kahtlaste linkide ja manuste vältimine: Ärge avage kahtlasi linke või manuseid, mis võivad sisaldada pahavara või ründeid. Usaldusväärsete allikate kasutamine: Kui külastate veebisaite või allalaadite faile, veenduge, et need oleksid usaldusväärsed ja turvalised. Tarkvara ajakohastamine: Hoidke oma tarkvara ja operatsioonisüsteemid ajakohastatud, et vältida turvaaugude ärakasutamist. Privaatsuse säilitamine: Olge ettevaatlik, millist teavet jagate oma sotsiaalmeedia kontodel või teistel avalikel veebisaitidel. VPN-i kasutamine: Kasutage virtuaalset privaatvõrku (VPN), et oma internetiühenduse turvalisust tõsta. Kahtlase tegevuse teatamine: Kui märkate midagi kahtlast, teavitage sellest asjakohaseid ametiasutusi või teenusepakkujaid. Need on mõned peamised meetmed, mis aitavad tagada turvalise käitumise internetis. Kuid pidage meeles, et interneti turvalisus on pidev protsess ja nõuab tähelepanu ning valmisolekut uuendusteks ja kohandusteks vastavalt muutuvatele ohtudele ja riskidele.
* Privaatsusseaded on seadistused, mis võimaldavad teil kontrollida, millist teavet jagate oma seadme ja veebilehtedega. Selleks saate määrata, milliseid andmeid teie veebilehitseja ja teie seade veebilehtedega jagavad, näiteks küpsised, asukohaandmed või teie sirvimisajalugu. Samuti saate määrata, millist teavet jagate oma sotsiaalmeedia kontodega, nagu profiilteave või postitused. Kasutusleping on leping, mis reguleerib õigussuhteid teenusepakkuja ja teenuse kasutaja vahel. See määratleb teenuse kasutamise tingimused, sh teenuse kasutamise eesmärgid, piirangud ja vastutuse. Kasutusleping võib sisaldada ka privaatsustingimusi, mis reguleerivad isikuandmete kogumist, töötlemist ja kaitset. Kasutusleping on leping, millele kasutaja nõustumisega kinnitab, et ta aktsepteerib teenusepakkuja tingimusi ja kohustub neid järgima. Lisaks on oluline jälgida ja tutvuda veebilehtede privaatsuspoliitikaga ning veenduda, et need vastavad teie privaatsuse ja turvalisuse vajadustele. Veenduge, et jagate oma isikuandmeid ainult usaldusväärsete organisatsioonidega ja ärge jagage tundlikku teavet, nagu sotsiaalkindlustuse number või krediitkaardiandmed, avalikult või e-kirjade või tekstisõnumite kaudu. Üldiselt on oluline olla teadlik ja tähelepanelik, millist teavet te internetis jagate ja kellega te seda jagate, et tagada oma privaatsuse ja turvalisuse kaitse.
* Küberturvalisus on muutunud tänapäeva infoühiskonnas väga oluliseks, kuna küberkuritegevus ja andmelekete oht on suurenenud. Seetõttu on vaja inimesi tööle küberturvalisuse valdkonda, et tagada organisatsioonide ja inimeste isikuandmete, rahaliste vahendite ja intellektuaalomandi turvalisus. Küberturvalisuse spetsialistid aitavad organisatsioonidel ennetada küberohtusid, kaitsta organisatsiooni ja klientide andmeid, tuvastada ründeid ja nendele reageerida ning parandada turvalisust. Töötades küberturvalisuse valdkonnas, saavad spetsialistid anda oma panuse nii avaliku kui ka erasektori organisatsioonide andmekaitse ja turvalisuse tagamisse. Lisaks on küberturvalisuse valdkond väga kiiresti arenev, seega on vaja inimesi, kes oleksid kursis uusimate tehnoloogiate ja meetoditega ning saaksid tagada organisatsioonide turvalisuse ja andmekaitse ka tulevikus. Küberturvalisuse valdkonnas on mitmeid erinevaid võimalusi töötamiseks.
* Pettused internetis põhjustavad aastas miljardeid eurosid kahju kogu maailmas. Kahju võib olla finantsiline, kuid ka mittemateriaalne, näiteks pettuse ohvri maine võib kannatada. Mõned näited pettustest ja nende kahju: Identiteedivargused: selle tulemusena võib kahju olla rahaline, kuna varas saab juurdepääsu ohvri rahalistele vahenditele ja kontodele. Lisaks võib identiteedivargus mõjutada ohvri krediidi ajalugu ja raskendada tulevikus laenude saamist. Pettused e-kaubanduses: petturid võivad müüa võltsitud või olematuid kaupu, nii et ohvrid kaotavad raha. Võib esineda ka pettuseid tagasimaksete tegemisel või laekumiste esitamisel. Küberkuritegevus: küberkurjategijad võivad kasutada ohvrite arvuteid või mobiiliseadmeid andmete kaevandamiseks või häkkimiseks, näiteks tundlike dokumentide varastamiseks või hävitamiseks. See võib kaasa tuua tõsiseid tagajärgi ettevõtetele ja organisatsioonidele. Pettused sotsiaalmeedias: petturid võivad teeselda, et nad on kellegi teise, et koguda isikuandmeid või raha. Nad võivad luua võltsitud kontosid, mis näevad välja autentsed, et petta usaldusväärseid inimesi. Pettused seotud tööga: petturid võivad kasutada tööotsingu saidid, et petta inimesi nende raha, isikuandmete või muude teabe saamiseks. Võib esineda ka pettuseid seoses töölepingutega. Kokkuvõtvalt võib öelda, et pettused internetis on laialt levinud ja võivad põhjustada suurt kahju nii isiklikul kui ka ettevõtte tasandil. Seetõttu on oluline olla teadlik pettuste ohtudest ning järgida küberhügieeni parimaid tavasid, et vältida pettuste ohvriks langemist. Pettused internetis võivad võtta mitmeid erinevaid vorme ning kahjustada inimeste rahalist seisundit, isikuandmete turvalisust ja üldist usaldust interneti vastu. Petturitega võitlemiseks on oluline olla teadlik ja valvas, kontrollida saadetud e-kirju ja veebisaite ning jagada isikuandmeid ainult usaldusväärsetele organisatsioonidele. Kui te arvate, et olete sattunud pettuse ohvriks, peaksite sellest teavitama politseid või vastavat küberkuritegevuse üksust.

**Isiklik turvaaudit**

Peatüki eesmärk on teha ülevaade kuidas viia läbi isiklik turvaaudit oma kodus. Õppijad omandavad mõiste „turvaaudit“. Samamoodi saadakse teada ametist infoturbejuht. Ülesanded ja küsimused aitavad õppijal viia läbi oma kodune turvaaudit.

Mõtteid kodusest turvaauditist:

* Kodune turvaaudit on protsess, kus kodukasutajad kontrollivad oma koduseadmete (näiteks arvuti, nutitelefoni, nutiteleri, nutikodu seadmete) turvalisust, et tagada nende kaitse küberrünnakute ja andmepüügi eest. Kodune turvaaudit hõlmab tavaliselt tarkvara ja seadmete turvaseadete läbivaatamist, tarkvara uuendamist, tugevate paroolide kasutamist, tundlike andmete krüpteerimist, pahavara skannimist ja võrgu turvaseadete kontrollimist. Kodune turvaaudit võib aidata kasutajatel avastada turvariske ja võtta meetmeid nende kõrvaldamiseks enne, kui need muutuvad tõsisteks probleemideks.
* Koduse turvaauditi läbiviimine võib olla lihtne protsess, kuid see võib varieeruda vastavalt seadmetele ja tehnoloogiale, mida kasutatakse. Need on mõned põhilised sammud, mida saate järgida, et tagada oma koduseadmete turvalisus. Lisaks sellele võite kaaluda ka tugevama tulemüüri seadistamist, VPN kasutamist või võrguliikluse monitoorimist, et tagada võrguliikluse turvalisus. Siin on mõned sammud, mida saate järgida, et oma koduseadmete turvalisust parandada:
	+ Kontrollige oma seadmete tarkvara uuendusi: Veenduge, et teie arvuti, nutitelefon, nutiteler ja muud nutikodu seadmed oleksid kõige värskema tarkvaraga. Enamikul seadmetel on automaatne uuendusfunktsioon, mis võimaldab tarkvara regulaarselt värskendada.
	+ Looge tugevad paroolid: Kasutage tugevaid ja unikaalseid paroole, mida on raske arvutada või pahatahtlikult ära arvata. Paroolide loomisel kasutage erinevaid sümbolite kombinatsioone, suuri ja väikseid tähti ning numbreid.
	+ Krüpteerige tundlikud andmed: Krüpteerimine on protsess, kus andmed kodeeritakse nii, et neid saab lugeda ainult siis, kui neid dekrüpteeritakse. Tundlike andmete, nagu pangakontode ja sotsiaalkindlustuse numbrid, krüpteerimine aitab tagada, et need andmed ei ole kättesaadavad ega häkitavad.
	+ Skannige pahavara: Pahavara skannimine aitab tuvastada ja eemaldada pahatahtlikke programme, mis võivad olla teie seadmetele kahjulikud. Kui teie seadmel ei ole pahavara skannerit, siis võite kaaluda sellise tarkvara installimist.
	+ Lülitage välja võrgu jagamine: Kui kasutate võrku, võib see olla turvarisk, kui jagate võrku teiste seadmetega, mis võivad olla häkkinud. Veenduge, et võrgu jagamine oleks välja lülitatud või turvatud vastavalt vajadusele.

**Enda digipädevuse hindamine**

Peatüki eesmärk on selgitada digipädevuse hindamist. Õppijad omandavad mõiste „digipädevus“. Ülesanne puudutab enda digipädevuse hindamist.

Mõtteid digipädevuse hindamisest:

* Digipädevuse omandamine koolis on oluline mitmel põhjusel. Esiteks on digipädevus tänapäeva tööturul üha olulisemaks muutunud ning selle valdkonna oskuste omandamine võib avada uusi võimalusi tööturul. Paljud töökohad eeldavad tänapäeval juba digitaalsete oskuste valdamist ning tulevikus saavad need oskused ilmselt veelgi olulisemaks. Teiseks on digipädevus oluline ka igapäevaelus toimetulekuks. Digitaalne maailm on meie igapäevaelu lahutamatu osa ning digitaalsete oskuste olemasolu võimaldab hõlpsamat suhtlemist, tööd, õppimist ning muud igapäevaelus vajalikku. Kolmandaks on digipädevus oluline ka turvalisuse seisukohalt. Digipädevus annab vajalikud teadmised ja oskused, et hoida end turvaliselt ja kaitsta ennast ning teisi internetis levivate ohtude ja pettuste eest. Seetõttu on digipädevuse omandamine koolis oluline, et noored saaksid vajalikud oskused ja teadmised, mis on vajalikud tulevikuks ning mis aitavad neil nii igapäevaelus kui ka tööturul edukamalt toime tulla.
* Digipädevuse hindamiseks on mitmeid lähenemisviise, sõltuvalt sellest, millist aspekti soovitakse hinnata. Kokkuvõttes võib öelda, et digipädevuse hindamine on oluline, et mõista inimeste teadmisi ja oskusi digimaailmas ning tagada nende sobivus erinevatele töökohtadele ja ühiskonnas toimimisele laiemalt. Siin on mõned võimalused:
	+ Enesehindamine: Inimesed saavad ise hinnata oma digipädevust läbi enesehindamise küsimustiku või testi, mis aitab mõõta nende teadmisi, oskusi ja hoiakuid erinevates digivaldkondades.
	+ Välise hindaja hindamine: See võib hõlmata nii individuaalseid hindajaid kui ka organisatsioone, mis hindavad digipädevust konkreetsetes valdkondades. Näiteks võivad tööandjad kasutada hindamistööriistu, et hinnata töötajate digipädevusi ja teadmisi, et tagada nende sobivus konkreetsele ametikohale.
	+ Standarditud hindamine: Standarditud hindamisvahendid võivad hõlmata standardiseeritud teste või eksameid, mis hindavad üldist digipädevust või spetsiifilisi oskusi nagu programmeerimine, andmeanalüüs jne.
	+ Portfoolio hindamine: See hõlmab isiku tööde ja projektide kogumit, mis näitab nende digipädevust ja võimaldab hinnata nende töö kvaliteeti.

**Karjäär ja IKT**

Peatüki eesmärk on teha ülevaade milliseid IKT oskuseid on vaja erinevates ametites, milliseid oskuseid on vaja IT-valdkonna ametites, kuidas planeerida oma õppimist ja karjääri ehk oskuste omandamist. Samamoodi saadakse teada erinevatest valdkondade vajadustest IT osas ja kes on talent IT-sektoris. Video IT-spetsialisti ametist annab õppijate teada, millised on ootused antud ameti ja selle õppimise suhtes. Samaoodi kutsub üles noori IT-ga tegelema ja ka ise talendiks saama. Ülesanded ja küsimused aitavad avastada erinevaid IKT-ameteid ja nende ülesandeid.

Mõtteid karjäärist ITK valdkonnaga seonduvalt:

* IKT karjäär oluline, kuna see pakub mitmeid võimalusi, aitab kaasa ühiskonna arengule ning tagab ka edaspidi tööjõu järele nõudluse. IKT (infotehnoloogia ja kommunikatsioonitehnoloogia) karjäär on oluline mitmel põhjusel: Tööjõuturg: IKT sektor on üks kiiremini kasvavaid tööstusharusid ja seal on suur nõudlus tööjõu järele. IKT karjäär võimaldab saada hea palga ning pakub võimalust pidevalt enda oskusi täiendada ja edasi areneda. Innovatsioon: IKT on innovatsiooni eestvedaja, kus on palju võimalusi uute tehnoloogiate loomiseks ja rakendamiseks. IKT karjäär võimaldab panustada uute ja põnevate lahenduste loomisesse ning aidata kaasa ühiskonna arengule. Vajalik oskus: IKT oskus on muutunud tänapäeva ühiskonnas oluliseks oskuseks. IKT kasutamine on muutunud praktiliselt kõigis eluvaldkondades ning seetõttu on vajalik, et inimestel oleksid piisavad digioskused. Mitmekülgsus: IKT karjäär võimaldab valida erinevate erialade vahel ning seega on võimalik leida endale sobivaim valdkond. Lisaks pakub IKT karjäär võimalust töötada erinevates sektorites ja erinevates organisatsioonides.
* IT töötajaid on vaja ka teistes sektorites, sest tänapäeval kasutatakse igas valdkonnas arvutipõhiseid lahendusi ning digitaalne tehnoloogia on integreeritud paljudesse protsessidesse. Näiteks kasutatakse IT-lahendusi tervishoius, logistikas, finantssektoris ja paljudes teistes valdkondades. IT-töötajad on vajalikud, et luua ja hallata uusi lahendusi ning tagada nende sujuv töö. Seega on IT-teadmised ja -oskused üha enam nõutud kõigis valdkondades ning võimaldavad inimestel paremini mõista ja rakendada digitaalseid töövahendeid oma igapäevatöös.
* IT sektori töötajate arv on viimastel aastatel oluliselt kasvanud, sest digitaalne tehnoloogia on muutunud üha olulisemaks ja integreeritumaks meie igapäevaelusse. Paljud ettevõtted ja organisatsioonid on hakanud rohkem kasutama IT-lahendusi oma tegevuse optimeerimiseks ja konkurentsivõime suurendamiseks. Samuti on tehnoloogia areng võimaldanud uute ja innovaatiliste ettevõtete tekke, mis vajavad enda meeskonda IT-spetsialiste. Statistika näitab, et IT-sektori töökohtade arv kasvab jätkuvalt üle kogu maailma. Näiteks Euroopa Liidus ennustatakse, et 2020. aastaks vajab 90% töökohtadest vähemalt keskmist digitaalset pädevust ning 40% töökohtadest vajab kõrgemat digitaalset pädevust. Samuti ennustatakse, et IT-sektori töötajate nõudlus kasvab ka tulevikus ning see on üks kiiremini kasvavaid tööstusharusid. Seetõttu on IT-alased oskused ja teadmised üha enam nõutud ning IT-sektori töötajate arvu kasv on tõenäoliselt jätkuv.