Küberturvalisus

Ülikooli küberturvalisus algab ülikooli iga liikme käitumisest.
Praegusel pingelisel ajal tuleb meil kõigil olla valmis nii erinevateks küberpettusteks kui ka küberrünnakuteks.
Peamised soovitused turvalisuse tagamiseks on:

- Ära ava e-kirjades ja SMS sõnumites olevaid tundmatuid linke ning manuseid. Kahtluse korral küsi alati enne Arvutiabi kaudu nõu.
- Ära usu ähvardavaid ja kiiret tegutsemist nõudvaid kirju, sõnumeid või telefonikõnesid tundmatutelt saatjatelt. Tea, et peale saatja e-posti aadressi saab tänapäeval võltsida ka helistaja telefoninumbrit.
- Ära anna tundmatule helistajale või tundmatule isikule juurdepääsu oma arvutile. Ära kunagi sisesta oma digiallkirja PIN koode, kui Sa pole ise seda tegevust algatanud.
- Kasuta eri keskkondades alati erinevaid paroole ning muuda neid paroole kohe, kui on kahtlus, et see on teatavaks saanud või lekkinud. Kasuta oma konto kaitsmiseks alati kaheastmelist autentimist, kui see on võimalik.
- Veendu, et kasutad oma arvutis usaldusväärset ja ajakohast tarkvara ning kõik turvauuendused on paigaldatud.
- Tekkinud küberintsidendist teavita Arvutiabi kohe esimesel võimalusel.

Allpool toodud juhenditest leiad veel üksikajalikumaid näpunäiteid

In English

Juhised

Küberturbe intsident on soovimatu või ootamatu infoturvasündmus, mis võib:

- kahjustada organisatsiooni tegevust
- ohustada andmete turvalisust

Teavita intsidendist esimesel võimalusel, võttes ITO-ga telefonitsi ühendust alljärgnevas järjestuses:

1. arvutiabi, 737 5500
2. infoturbejuht Risto Rahu, 5305 5032
3. taristutalituse juhataja Erkki Kukk, 521 3503

Ole kursis infosüsteemide kasutamist ja infoturvet reguleerivate eeskirjadega:

- infoturbe materjalid siseveebis: https://siseveeb.ut.ee/et/tugiteenused/infoturve
- ülikooli IT eeskirjad, vt https://siseveeb.ut.ee/et/tugitegevused/dokumendid-ja-juhendid-4

Täiendavat nõu eeskirjade kohta küsi vajadusel arvutiabi kaudu või infoturbejuhi käest

Riigi Infosüsteemi Amet on avaldanud soovitused turvalisemaks arvutikasutuseks

- vaata soovitusi veebiportaalis https://www.itvaatlik.ee/

Andmete turvalisuse tagamine on oluline ja sõltub eelkõige sinust:

- ole teadlik tööülesannete tõttu sinu kätte usaldatud andmetest ja taga nende kaitse
- hoia ülikooli andmeid vaid ülikooli serverites ja infosüsteemides
- kui tööülesande täitmiseks antud andmeid enam vaja ei ole, kustuta need oma tööarvutist

Tartu Ülikoolis saab andmekaitse teemal abi andmekaitse peaspetsialistilt Terje Mäesalult:

- telefon 737 5119
- e-post terje.maesalu@ut.ee

Tööarvuti turvalisuse tagamiseks järgi juhiseid:

- arvuti juurest lahkumisel lukusta ekraan, Windowsi arvuti puhul kasuta klahvikombinatsiooni win + L
- veendu, et tööarvutis on kasutusel ja toimib turvatarkvara (Windows Defender) ning arvutis oleva tarkvara puhul on paigaldatud selle uusimad versioonid ning aktiveeritud automaatne uuendamine. Vajaduse korral küsi nõu arvutiabist.
- kasuta arvutis töötamisel alati vaid tavakasutaja (standard user) õiguseid. Privilegeeritud (administraatori) õiguste kasutamine peab olema lühiajaline, näiteks vaid tarkvara uuendamine ajaks. Vajaduse korral küsi nõu arvutiabist.
- sülearvuti puhul väldi avatud (krüpteerimata) wifi-ühenduse kasutamist või kui see pole võimalik, kasuta mobiilset andmesidet või VPN-ühendust
- kui töötad kohas, kus arvuti ekraanil toimuvat võivad näha võõrad isikud, soovitame kasutada privaatsust suurendavat ekraanifiltrit
- kasuta sülearvutis ja nutiseadmes võimalusel alati andmete (ketta) krüpteerimist. Nii väldid andmete leket seadme kadumise või varguse korral.
- ära jäta oma sülearvutit väljaspool tööruume lukustamata ruumi või järelevalveta.
- kui seade varastatakse, anna sellest kohe arvutiabile teada ja vaheta esimesel võimalusel oma konto parool
- kui tekib kahtlus, et oled käivitanud pahavara sisaldada võinud programmi või avanud pahavara sisaldanud dokumendi (ebaharilik veateade, häirivad reklaamid vms), võta arvutiabiga **kohe** ühendust

Veendu, et isiklik arvuti kasutab turvalist ja ajakohast tarkvara, vajadusel uuenda tarkvara.

Soovitused:

- jälgi oma isikliku arvuti või nutiseadme paremaks turvamiseks vt Riigi Infosüsteemi Ameti soovitusi
- paigalda tarkvara ainult ametlikust kanalist, näiteks tootja veebilehe või operatsioonisüsteemi rakenduste poe kaudu,
- kasuta ka isiklikus arvutis töötamisel alati vaid tavakasutaja (standard user) õiguseid. Privilegeeritud (administraatori) õiguste kasutamine peab olema lühiajaline, näiteks vaid tarkvara uuendamine ajaks.
- kasuta tööalase info töötlemiseks eelkõige TÜ poolt pakutavaid veebipõhiseid (pilvepõhiseid) tarkvaralahendusi
- ära hoia tööalast infot isiklikus seadmes kauem, kui on vajalik kaugtöö tegemiseks

Tartu Ülikooli põhiline e-posti lahendus on pilvepõhine Microsoft Exchange Online.
Kõik ülikooli liikmed saavad teenust kasutada veebipõhiselt või arvutisse paigaldatava tarkvara kaudu.

Soovitused:

- kasuta teadus- ja õppetöös alati vaid ülikooli e-posti aadressi. Ära suuna ülikooli e-posti edasi oma isiklikule e-posti aadressile.
- kirja saatmisel ole adressaatide valikul hoolikas – kontrolli üle, kas kõik saajad peavad olema kaasatud (eriti kirjadele vastamisel!) ja kas saajate e-posti aadressid on õiged
- kui saad kirja tundmatult isikult või ettevõttelt, ole kirja manuste ja kirjas olevate veebilinkide avamisel ettevaatlik ning vajaduse korral küsi nõu arvutiabist
- kui saad kirja, milles nõutakse parooli uuendamist või muud kohest kiiret tegutsemist, suhtu sellesse ettevaatlikult ja küsi vajaduse korral nõu arvutiabist.
- kui oled avanud kahtlase veebilingi või oled sisestanud oma andmeid kahtlasele veebilehele, võta arvutiabiga **kohe** ühendust
- oma e-posti konto kaitsmiseks aktiveeri kaheastmeline autentimine (2FA) (vt Kaheastmelise autentimise aktiveerimine)

Tartu Ülikool on oma liikmetele videoloengute ja videokoosolekute läbiviimise jaoks hankinud mitu tarkvaralahendust, sh Bigbluebutton, Panopto, Microsoft Teams ja Zoom.

Kõik ülikooli liikmed saavad neid teenuseid kasutada oma ülikooli konto kaudu.

Eelista alati ülikooli poolt pakutud videokoosoleku lahendusi. Arvesta, et osad tasuta videokoosolekute teenused sisaldavad reklaame või edastatakse isikuandmeid (müügiks) kolmandatele isikutele.

Turvalisuse tagamise soovitused:

- kui plaanitav videokoosolek käsitleb tundlikku infot, mille avalikuks tulek tekitaks ülikoolile märkimisväärset kahju, hinda võimalikke riske ning vajadusel konsulteeri enne koosoleku korraldamist arvutiabiga.
- arvesta tundliku info jagamisel sellega, et osalejad saavad videokoosolekut lihtsasti salvestada või teha sellest ekraanipilte.
- võimaluse korral pea oma videokoosolekuid ja -loenguid privaatsena. Näiteks luba juurdepääsu vaid isikutele, kellel on Tartu Ülikooli kasutajatunnus ja ära luba võõrastel oma koosoleku või loenguga liituda
- ära jaga veebilinke oma privaatsetele koosolekutele või loengutele sotsiaalmeedia kanalite kaudu, kasuta sellise info levitamiseks vaid ülikooli e-posti ja sisemisi veebikanaleid
- kui koosolek toimub laiemas osalejate ringis, kontrolli, kes saavad koosolekuga liituda ning kellele on antud õigus ekraanipilti jagada
- uuri, kuidas saab koosolekult eemaldada võõraid või ka ekslikult üh endunud isikuid ning vajaduse korral loe juhendeid või küsi nõu arvutiabist
- paigalda videokoosoleku tarkvara ainult ametlikust kanalist (tootja veebilehe või operatsioonisüsteemi rakenduste poe kaudu), kui kahtled tarkvara ehtsuses, võta ühendust arvutiabiga
- veendu, et kasutad videokoosoleku tarkvara kõige uuemat versiooni
- kõigi infoturbeprobleemide ja -küsimuste tekkimisel võta **kohe** ühendust arvutiabiga, dokumenteeri võimalikult täpselt intsidendi sisu ja selle toimumise aeg ning võimaluse korral tee koosolekul juhtunust ekraanipilt (kuvatõmmis)

Ülikooli konto parooli loomise reegleid on kirjeldatud arvutiabi paroolide vahetamise infolehel.

Soovitused:

- parooli saab turvaliselt muuta iseteeninduskeskkonnas https://parool.ut.ee
- kui on vaja parooli arvutis meeles pidada, kasuta turvalist paroolihalduse tarkvara. Vt ka juhised veebilehel Paroolihaldurid
- muuda parooli korrapäraselt **(vähemalt korra kahe aasta jooksul)** ja vaheta see kohe välja, kui on tekkinud kahtlus, et see on kõrvalistele isikutele teatavaks saanud
- konto lekkimise kohta saad oma kasutajatunnuse põhjal teha päringu veebilehel https://haveibeenpwned.com/

Kui näed tööruumis kahtlast isikut, siis uuri, kes ta on ja kelle juurde ta soovib minna. Vajaduse korral anna oma kahtlusest teada valvekeskuse telefonil +372 737 5111.
Oma küberturbealase teadlikkuse tõstmiseks:

- tee läbi ülikooli küberhügieeni veebikoolitus: https://cyberhygiene.ut.ee/
- tee läbi Riigi infosüsteemi ameti küberkaitsekursus kõigile - https://www.itvaatlik.ee/test/
- loe lisamaterjale lehelt https://itvaatlik.ee/
- Vaata lisaks: Alo Peetsi loeng teemal Küberturvalisus – kuidas kaitsta ennast levinud ohtude vastu?

- Pahavara ja arvutiviirused
- Andmekaitse
- Andmete õngitsemine
- Rämpspost
- Kontrolli oma infoturbe teadmisi