ABC teadmised küberhügieenist nii ema, isa kui ülemuse seisukohalt

Küberhügieen ei erine tavahügieenist: leia endale sobivad tooted, mis puhastavad ja kaitsevad, kasuta ja vaheta neid regulaarselt ning pea rutiinist kinni.

Hoia seadmed ja kontod kaitstuna

Kõik nutiseadmed, arvutist telefonini, peavad olema varustatud paroolide ning viirusetõrjeprogrammidega. Kõige lihtsam viis enda andmete kaitsmiseks on seada salasõnad kõikidele seadmetele, olenemata sellest kas nendega surfatakse Internetis ja/või nad on Interneti teel juhitavad või seadistatavad. Samuti on kohustuslikud viirusetõrjeprogrammid. Oma seadmete salasõnad ja muud vajalikud sisselogimistunnused peavad olema hoitud selliselt, et need ei saaks teatavaks kolmandetele isikutele. Salasõnu tuleks vahetada regulaarselt. Kui kahtlustad, et need on kellelegi teatavaks saanud või et kellelgi on lubamatu ligipääs seadmele või kontole, tuleb vastavad autentimiseks vajalikud tunnused välja vahetada viivitamatult.

Võõras või avalikus seadmes (näiteks tehnikapoes väljapandud telefonis või tahvelarvutis) oma e-posti või sotsiaalmeediakontole sisselogimine ei pruugi olla hea mõte. Esiteks kiputakse võõras seadmes käituma ikka sellise rutiini kohaselt nagu oma isiklikus seadmes ja nii unustatakse end vastavalt kontolt välja logida või laetakse võõrasse seadmesse alla infot, mida allalaadija tegelikkuses teistega jagada ei tahtnud. Teiseks võib võõras seade salvestada Sinu kontode paroolid ja siis ei ole ka välja logimisest suurt kasu, sest kolmandate isikute kontrollimatu ligipääs kontole on tagatud.

Tööandjana peaksid

Töötajad ja tööandjad peaksid läbi mõtlema, kas ja kuidas on andmed kaitstud siis, kui töötaja ühel päeval enam tööle ei tule. Kui teatud süsteemidele on ligipääs ainult ühel töötajal ja temaga midagi juhtuma peaks, siis võib tööandjale tekkida suur kahju tegemata töö ja kaotsi läinud andmete osas. Eeltoodut aitab vältida see, kui tööandja on läbi mõelnud tööprotsessid, töötajatega sõlminud konfidentsiaalsuskokkulepped ning on töötajaid üheselt ja selgelt instrueeritud seadmete ja andmetega töötama. Tööandja peab arvestama asjaoluga, et kui töötaja rikub isikuandmete töötlemisel kehtivaid või kehtima hakkavaid õigusakte, siis vastutab tööandja töötaja rikkumise ja võimaliku tekitatud kahju eest. Küsimus ei ole alati mitte isikuandmete väärtöötlemises vaid mh tööandja äri- ja tootmissaladuse ning konfidentsiaalse teabe hoidmises kui ka näiteks ettevõtte maines.

Noorema põlvkonna inimesed tunnevad end sotsiaalmeedia vestluslahenduste, kui ka muude peamiselt isikulikuks otstarbeks loodud infovahetuse platvormide, kasutamises ääretult mugavalt ning unustavad, et teatud infot ei või nimetatud vahendite kaudu edastada ja/või sinna talletada. Eriti, kui tööandja ei ole nimetatud kanalit määratlenud ametlikuks suhtluskanaliks. Töötaja isiklikku Facebooki vestlusesse või telefoni salvestatud info jääbki sinna ning tööandjal ei ole hiljem võimalust seda sealt kustuda või kontrollida, et info, failid vms oleks kustutatud.

Peale selle tuleb arvestada, et tööandjal puudub ülevaade, millistes lepingulistes suhetes on töötaja oma teenusepakkujaga, kelle lahendust ta kasutab. Pahatihti puudub kasutajatel kontroll, kas, millises mahus ja mis perioodil platvormil salvestatud info säilitatakse. Ettevõtetel, avaliku sektori asutusetel ja ka mittetulundusühingutel on kohustus töödelda kõiki isikuandmeid turvaliselt ja vajadusel anda andmesubjektile ülevaade hoiustatud andmetest. Seda isegi juhul kui jutt käib vaid e-kirjadest ja telefoninumbritest.

Mida alaealine Internetis teeb? Mida lapsevanem lapsest postitada tohib?

Lapsevanem või eestkostja on see isik, kes vastutab lapse turvalisuse eest. Kui alaealine on teinud kohatuid postitusi või saatnud endast seksuaalse sisuga pilte ja/või videoid, võime põhjendatult küsida, kus sellel ajal lapsevanema silmad olid. Lapsevanema kui täiskasvanu kohustus on selgitada alaealisele nutiseadme kasutamisega seotud riske ja ohtusid. Lapsevanem peaks esmalt endale selgeks tegema millised võimalused ühe või teise seadme või kontoga kaasnevad ja siis otsustama, kas tema laps üldse peaks olema seotud nende ohtudega.

Alaealistega seotud postituste tegemine (isegi nende vanemate või eestkostjate poolt) on samuti isikuandmete töötlemine ja esmajärjekorras peavad kaitstud olema lapse huvid. Arvestada tuleb, et positust ei saa reeglina kunagi lõpuni kustutada või olematuks teha. Sotsiaalmeedias olevate piltide vaatajaskond laieneb kordades kui seda pilti on like'itud või jagatud. Igaüks, kelle ekraanile pilt tuleb, saab seda alla laadida. Lähisõpradele mõeldud väikelapse pilt muutub hetkega perverdile kättesaadavaks. Isegi kui lapse või lapsevanemani ei jõua mitte kunagi info, et väikese inimese pilti haige inimene korduvalt väärkasutab, siis lapse igapäeva elu saab suure hoobi, kui eakaaslased leiavad, et üks või teine postitus on aasimist vääriv. Kõige mõistlikum ja õiguspärasem on lapse pilte sotsiaalmeediasse mitte postitada.

Kolmandatel isikutel ei ole õigust teha lapse nimel kontosid ilma lapsevanema või eestkostja vastavasisulise nõusolekuta. Ka haridusasutustel on kohustus küsida andmesubjektidelt nõusolekut, kas andmete edastamine kolmandatele isikutele on lubatud või mitte. Lapse isikuandmete edastamine kolmandatele isikutele on tõenäoliselt vastuolus kehtiva õigusega. Seejuures on kindlasti lubamatu, et kool loob lastele kontod, mille kõigi võimalustega kool ise kursis pole ning väiksed kasutajad hakkavad koolitunnis kasutamiseks mõeldud kontot kasutama selleks, et teha enda jaoks ohtliku sisuga postitusi. IT-õpe üldhariduskoolides peab vastama kehtivale õigusele ning olema ohtusid ennetava sisuga.

Tee seoses oma seadmete, sotsiaalmeedia, kontode, e-posti ning ID-kaardiga tarku otsuseid

Inimesed ei teadvusta, et teise isiku arvuti, tahvelarvuti, mobiil, e-post, ja privaatvestluse keskkonnad ei ole kolmandatele isikutele lugemiseks või kasutamiseks. Sõnumisaladuse rikkumine on nt olukord, kus teise isiku mobiiltelefonis olevat infot (salaja) loetakse. Põhjendatud ei ole see ka olukorras, kus lugeja vabandab, et lähisuhtes ei peaks olema saladusi vms. Seadmetele peavad olema seatud kasutajanimed ja salasõnad. Kellelgi ei ole õigust küsida Sinult Sinu seadme, konto vms autentimiseks vajalikke tunnuseid. Ära luba kedagi oma kontole või seadmesse luusima.

Harvad ei ole ka olukorrad, kus perekonnaliige on kuritarvitanud ID-kaarti, mis on koos koodidega lihtsasti kättesaadavad või ilusti teiste dokumentidega sahtlisse tallele pandud. ID-kaardi peamised (kodused) väärkasutamised on seotud kaardi omaniku pangakontol oleva raha ülekandmisega, väikelaenude võtmisega, käenduslepingute sõlmimisega või Interneti hasartmängude mängimisega. ID-kaart on oluline dokument, mida tuleb samamoodi hoida nagu oma reisipassi. Arvestada tuleb, et erinevalt reisipassist, saab ID-kaardiga sõlmida tehinguid, mida kaardi omanik teha ei ole tahtnud. Sellised tehingud on küll tühised, aga tõendamiskoormis on kaardi omanikul, sest näiteks panga töötajal on võimatu kindlaks teha, et tänane elektrooniline dokument on sõlmitud kellegi teise poolt kui digikonteineris näha olev nimi seda arvata lubab. Tehingu tühistamisele ei aita kaasa ohvri häbitundest tingitud passiivsus, mis ei lase ohvril võimalikult kiiresti (kohe peale teadasaamist) politseisse ja tehingu teise osapoole poole pöörduda. Mida kauem viivitatakse vastava informatsiooni edastamisega, seda keerulisem on politseil uurimist teostada.

Arvestada tuleb, et süüteod aeguvad ning tsiviiltehingud jäävad kehtima kui isik, kelle nimel tehingud tehti, seda õigel ajal ei vaidlusta.

KATRIN SARAP
VANDEADVOKAAT, PARTNER

(+372) 66 76 440
KATRIN.SARAP@NJORDLAW.EE

LIISI JÜRGEN
VANDEADVOKAAT, PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE