Noortele ja vanematele: 7 põhitõde sotsiaalmeedia turvaliseks kasutamiseks

2. august 2017 - 14:23 Autor: AM

Nutiseadmed koos kõikjal saadaoleva ülikiire mobiilse internetiga on meie igapäevaelu märgatavalt lihtsustanud - taskusse mahtuva abilise nõul saame valida ilmale sobivaima riietuse, tellida paari näpuvajutusega lõunasöögi kontorisse või hoida end sõprade-tuttavate tegemistega sotsiaalmeedia vahendusel jooksvalt kursis.

Just see viimane – sotsiaalvõrgustike kasutamine – on kõige levinum ajaveetmise viis. Elisa tooteturunduse osakonna juht Mailiis Ploomann tuletab meelde põhitõed, kuidas sotsiaalmeedias targalt ja turvaliselt käituda ja meie ümber toimunut ja nähtut jagada, ilma et peaks kartma selle kurjade silmade ette jõudmist.

Elisa kasutusstatistika näitab, et telefonis leiduvate populaarseimate rakenduste esikaheksast koguni kuus on erinevad sotsiaalmeedia kanalid. Facebook, Twitter, Instagram, Snapchat, Pinterest ja veel mitmed sarnased rakendused on pea iga nutikasutaja seadmes.

Kuid unustada ei tohi, et sotsiaalmeedia kanalid on ka omamoodi osa avalikust ruumist. Kõik Facebookis, Twitteris, Instagramis jagatu jätab sinust maha digitaalse jalajälje ning jääb internetti tõenäoliselt igaveseks. Seetõttu on ülimalt oluline mõelda hoolikalt läbi, kellega, mida ja kuidas sotsiaalmeedia vahendusel jagada.

Kellega jagada Facebooki puhkuse-postitust ja asukohta?

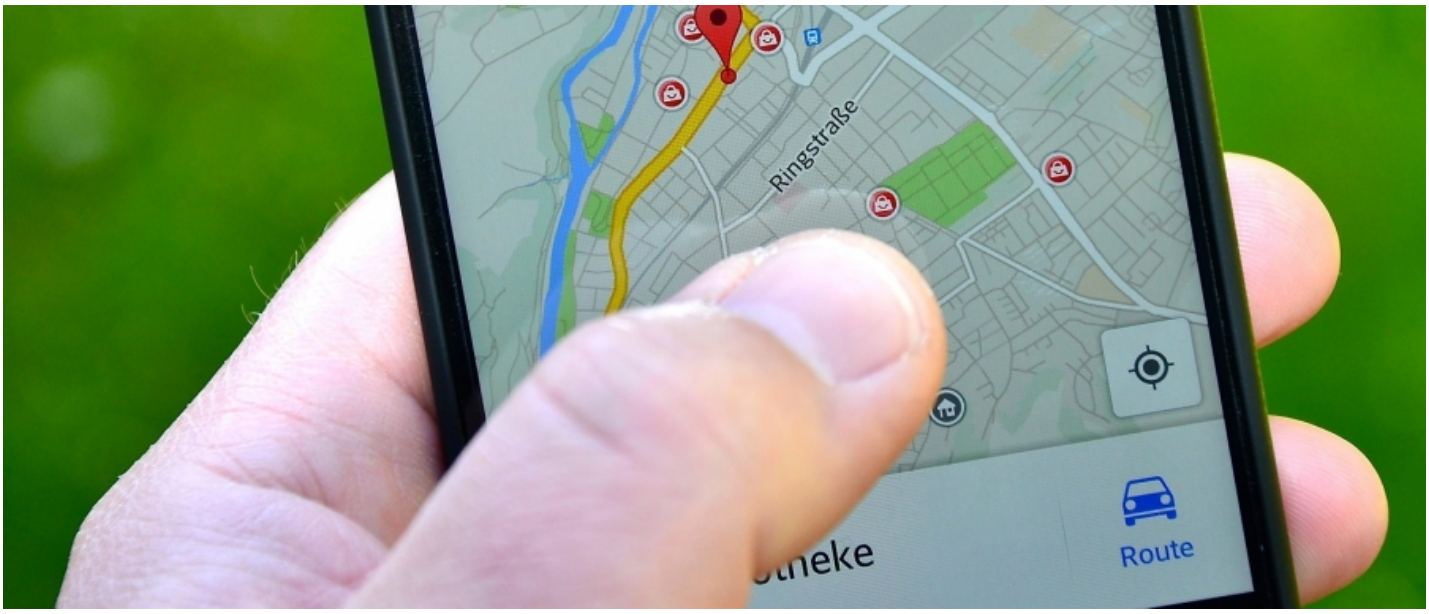


Foto: (CC) Tobias Albers-Heinemann / Pixabay

Pea kõik allalaaditavad sotsiaalmeedia rakendused kasutavad GPS-i, mis jälgib, kus sa parasjagu asud. Kuigi enamjaolt näevad seda infot sinu lähemad sõbrad (sõltuvalt sellest, kuidas oled Facebookis info avaldamise seadistanud), võib see pahatihti jõuda inimesteni, kes saavad seda kurjasti ära kasutada.

Praeguste muutlike suveilmadega on paljud eestlased otsustanud päikest hoopis välismaale otsima minna ning muidugi on tore türkiissinise mere ja rannaliiva muljeid sõpradele Facebookis muljetada. Kuna aga varasemast on kindlasti kontol pilte kodust koos kodu asukohaga, siis oma postitusi kogu avalikkuse või ka kõigi mitmesaja sõbra või sõbra-sõbraga jagades võid tahtmatult muutuda maiuspalaks kõige lihtlabasemale vargale – perekond on kaks nädalat Hispaanias reisil ning kodu tühi ja valveta.

Isegi ainult sõpradega meeleolukaid pilte-videoid jagades tasub olla pigem ettevaatlik, sest pahatahtlikud häkkerid võivad sinu andmeteni jõuda ka läbi su sõprade – kui nende telefon kaob või varastatakse, turvamata avalikku wifi-võrku kasutades häkitakse nende seadmesse sisse jm.

Samuti võiksid oma konto privaatseks või vaid vähestele sõpradele nähtavaks teha Endomondot jt sarnaseid rakendusi kasutavad spordiharrastajad, kes näiteks regulaarselt igal õhtul samal ajal ja samas kohas jooksutiiru teevad. Selline informatsioon on tundlik, kuna näiteks iga päev otse koduuksest alguse saanud jooksutiir võimaldab jällegi positsioneerida sinu kodu täpse aadressi ning anda kurjategijale orienteeruva ajavahemiku, mil sinu kodu ja vara valveta on. Samuti tuleb arvestada ka riskiga, et võid mõnele halbade kavatsustega inimesele anda ette täpse marsruudi, kus sa parasjagu üksi ja kõrvaklapid peas metsa vahel sõrgid.

Ka kohtingul säilita valvsus

Eriliselt tähelepanelik tuleb olla erinevaid kohtingusaite kasutades, kuna seal alustad suhtlemist sisuliselt võõra inimesega, mistõttu ei saa kunagi sajaprotsendiliselt tema tegelikes eesmärkides kindel olla. Eestis, nagu ka mujal maailmas, on kõige kasutatavamaks kohtingusaidiks Tinder, ent selle kategooria alla kuuluvad ka kõige tavalisemad jututoad. Nende rakenduste kasutamisel kehtib kuni uue tutvuse osas kindluse saamiseni kuldne reegel – “mida vähem, seda parem”. Tinderi puhul peaks veel meeles pidada, et rakendus põhineb GPS-funktsioonil, mis võimaldab samuti sinu asukohta kergesti positsioneerida.

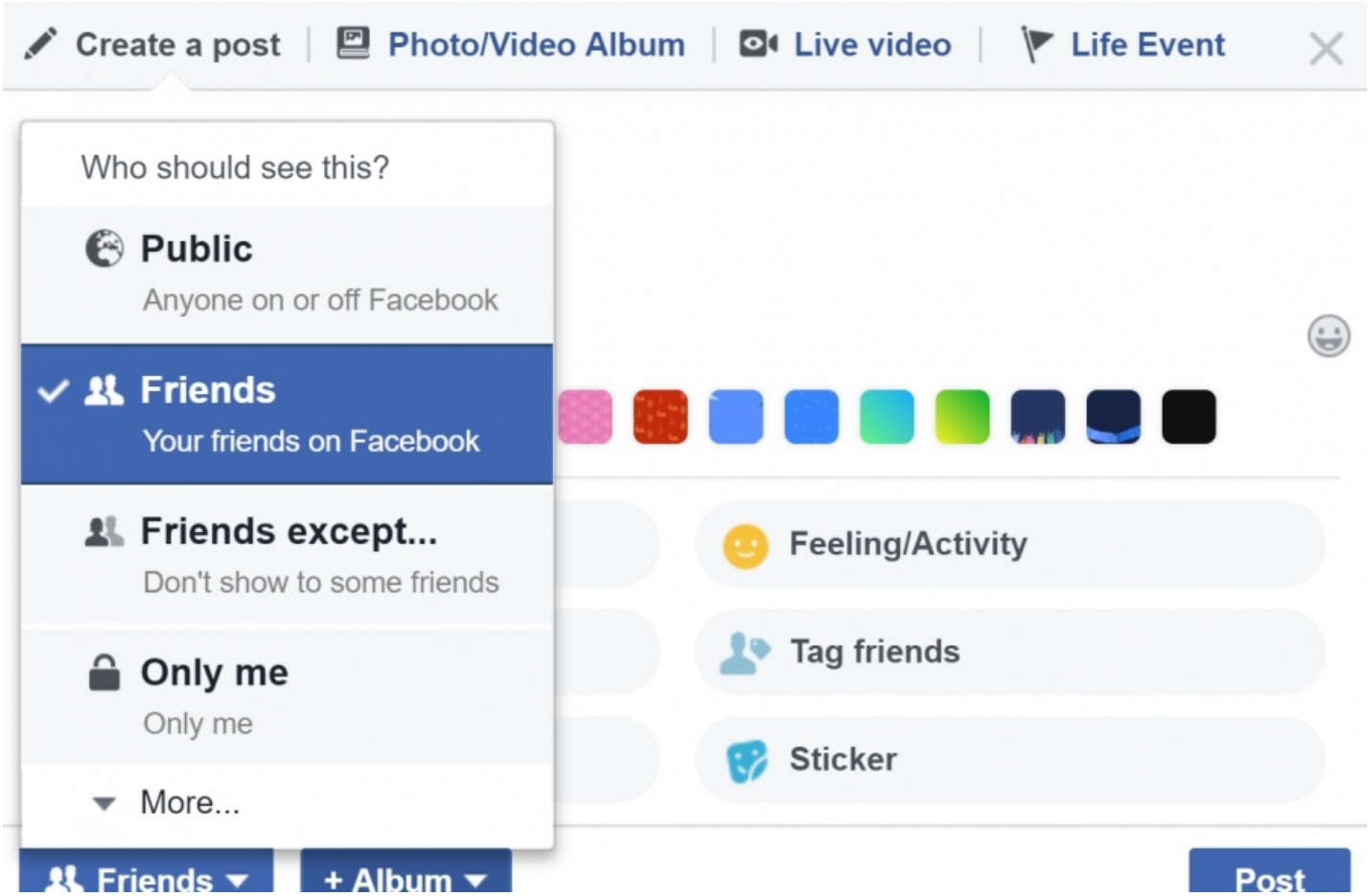
Turvalised paroolid

Kui sul on konto mitmes erinevas keskkonnas alates Facebookist ja lõpetades näiteks Snapchatiga, siis olgu see kui tülikas tahes – kasuta alati erinevates keskkondades erinevaid paroole. Muidugi on kümnekonna või ka enama parooli meelespidamine keeruline, siin on lahenduseks näiteks muutes hästi meeles olevas salasõnas iga kord midagi õige pisut – lisades mõne tähe, numbri või sümboli.

Parool ei tohi kunagi olla lihtne, nagu “parool”, “tere12345” või “qwerty”. Heas paroolis võiks olla suur- ja väiketähti, sümboleid ja numbreid.

Kõige olulisem on, et sinu Facebooki parool oleks teistest eristuv ja väga turvaline, kuna ilmselt kasutavad paljud meist Facebooki poolt pakutavat autentimisvõimalust mitmesugustel teistel veebikülgedel või teenusepakkujate juures – olgu näiteks muusikateenus Spotify, broneerimiskeskkond Booking.com või ka kodumaine e-pood Hansapost. Juhul kui kasutad liiga lihtsasti äraarvatavat salasõna või satub see võõraste silmade alla, ei ähvarda oht mitte ainult sinu Facebooki konto andmeid, vaid ka paljusid teisi sulle olulisi keskkondi ja kaudselt isegi ka rahakotti.

Määra ise, kellega millist infot jagad



Veendumaks, et sinu poolt jagatud informatsioon ei jõua valede inimesteni, vaata üle kõik oma sotsiaalmeedia kontode privaatsussätted. Eestlaste seas kõige populaarsem sotsiaalmeedia rakendus Facebook võimaldab sul ise määrata, milline postitus on nähtav kõigile ning milline ainult sinu sõpradele. Samuti pakub Facebook võimalust grupeerida kõiki oma sõpru. Näiteks saad teha eraldi grupi oma perele, lähimatele sõpradele, tuttavatele või kolleegidele. Vastavalt postituse sisule saad valida, milline grupp nendest sinu postitust näevad.

Eestlaste seas samuti populaarsetes rakendustes Twitter ja Instagram ei saa küll selekteerida oma auditooriumi postituste kaupa, ent võimaldab muuta oma konto privaatseks ning seejärel ligipääsu ise jagades. Selle tulemusena saad ise manuaalselt valida, kes sinu postitusi näeb ja kes mitte.

Kas ma tahan, et ema seda näeks?

Ehkki sotsiaalmeedia kanalite privaatsussätted annavad võimaluse määrata oma postituste privaatsust, siis on mitmesugust informatsiooni, mida tasuks sotsiaalvõrgustikes pigem üldse mitte jagada.

Enne igat postitust mõtle korraks – kas võiksin seda näidata oma emale, töökaaslasele, ülemusele? Kui vastus on eitav, siis pigem ära postita. Sest isegi kui sa pärast selle postituse eemaldad või kustutad, võis keegi vahepeal su postitusest juba ekraanitõmmise teha.

Isiklike andmete kaitse

Sarnaseid rusikareegleid on veel. Ära kunagi jaga oma isikukoodi, detailset sünnikohta, koduaadressi. Isegi väikesed infokillud võivad aidata kaasa sinu identiteedivargusele. Samuti võid sattuda häkkerite poolt koostatud e-maili listi, mille tulemusena võid hakata saama e-kirju, mis sisaldavad pahavaralisi linke või manuseid.

Sama kehtib ka kõikide sinu kontode paroolide, sh krediitkaardi kontonumbrite ja PIN-koodide, paroolikaartide ja ID-kaardi informatsiooni kohta. Kuigi see soovitus võib tunduda elementaarsena ja ilmselt justkui pähekulununa, on tegelikult väga palju inimesi, kes niivõrd tundlikku informatsiooni jätkuvalt sotsiaalmeedias jagavad. Twitteris on hoiatusena tehtud isegi enam kui 18 500 jälgijaga eraldi konto, kus on näha inimeste poolt ise jagatud pangakaartide fotod koos nimede, kontonumbrite ja sageli ka turvakoodidega. Õnneks on sel kontol olevad postitused peamiselt väljamaised, kuid hoiatava näitena on see siiski väga kõnekas.

Sama kehtib ka ostetud kontserdi-, kino- või teatripiletite kohta, eriti kui need sisaldavad näiteks QR-koodi. Vilunud häkkerid või ka mõni pahatahtlik juhututtav oskavad sellega hõlpsalt üritusele enne sind sisse pääseda, mille tulemusena jääb sul kultuurielamus saamata. Kui sa tahad tõesti nii väga oma ostetud piletiga teiste ees eputada, kata pildistades käe või sõrmega kood või murra pilet just selle koha pealt pooleks.

Räägi sellest kõigest lapsega

Viimane ja kõige eelneva valguses isegi ehk kõige tähtsam nõuanne on kõiki neid soovitusi jagada oma lapse või lastega. Kui teie peres on ka lastel nutiseadmete ja erinevate sotsiaalvõrgustike kasutamine juba lubatud ja näiteks teie teismeline poeg-tütar on alustamas erinevate sotsiaalmeediakanalite kasutamist, siis seda olulisem on tähelepanu kõigele turvalisusega seonduvale.

Üks väga oluline täiendav märkus puudutab mitmesuguseid lastele ja noortele suunatud mänge-keskkondi, nagu näiteks Growtopia. Ehkki lapsevanema silmis ei pruugi see nii olla, siis ka sarnased mängud toimivad omamoodi sotsiaalmeediana, kus kaasmängijatega võidakse teadmatusest jagada turvalisusriske tekitavat tundlikku infot.

Seetõttu tasub igal lapsevanemal kõik eelnevad nõuanded ühiselt läbi arutada ja ühiselt erinevate rakenduste-mängudega tutvuda, et lapsevanemana olla rakenduse sisuga kursis ning hinnata võimalikke ohukohti.