Kümme soovitust Zoomi videokonverentsi turvaliseks kasutamiseks

6 aastat tagasi - 22.04.2020 Autor: AM

Ülemaailmselt levinud sotsiaalse distantseerumise ja karantiini tõttu väga paljudes riikides hakkasid inimesed kiiresti otsima tõhusaid vahendeid üle interneti suhtlemiseks. Üheks populaarseimaks vahendiks on saanud varem vähetuntud Zoom, ent kasutamise kiire kasvuga ilmnesid ruttu ka selle videokonverentsitarkvara turvavead. Ettevõte tegeles töökoormuse tohutu tõusuga sujuvalt ja reageeris kiiresti ka paljudele leitud puudustele. Ent nagu iga teenuse puhul, ei lahenda koodi uuendamine päris kõiki kaebusi. Siin on kümme soovitust, mida pakub välja küberturvalisuse ettevõte Kaspersky Zoomi kasutamiseks. Enamik neist kehtivad ka muude videokõneplatvormide kasutamisel.

1. Kaitse oma kontot

Zoomi konto on nagu iga tavaline konto ja selle seadistamisel peaksid kasutama konto kaitse põhialuseid. Kasuta tugevat ja ainulaadset salasõna ning kaitse oma kontot kahefaasilise autentimisega, mis muudab konto raskemini häkitavaks ja paremini kaitstuks isegi andmete lekke korral (ehkki seda pole seni juhtunud).

On veel üks Zoomile iseloomulik omapära: pärast registreerumist saad lisaks kasutajanimele ja salasõnale ka isikliku ID (Personal Meeting ID). Võimalusel väldi selle avalikustamist. Kuna Zoom pakub võimalust luua sinu Personal Meeting ID-ga (PMI) avalikke koosolekuid, on ID lekitamine üsna lihtne. Kui jagad oma PMI-d avalikult, võib igaüks liituda sinu hostitud kohtumisega, nii et jaga seda teavet ettevaatlikkusega.

2. Kasuta Zoomi registreerimisel oma töökoha meiliaadressi

Zoomis esineva tõrke tõttu arvab teenus sama domeeniga meiliaadresside osas välja arvatud juhul, kui tegemist on tõesti tavalise domeeniga nagu @ gmail.com või @ yahoo.com, et need kuuluvad ühele ja samale ettevõttele ning jagab kontaktandmeid iga grupi liikmega. Näiteks juhtus selline asi kasutajatega, kes kasutasid registreerimisel meiliaadressi lõpuga @yandex.kz, mis on Kasahstani avalik e-posti teenus ning sama võib juhtuda uuesti ka teiste väiksemate avalike

e-posti teenuse pakkujatega.

Seega registreeri end Zoomis töö meiliaadressiga. Ametikoha kontaktandmete jagamine päris-elu kolleegidega ei tohiks olla probleem. Kui sul pole töö meiliaadressi, kasuta oma isiklike kontaktandmete privaatsuse hoidmiseks tuntud üldkasutatavat domeeni, näiteks Gmail.com.

3. Ära lange võlts-Zoomi rakenduste võrku

Kaspersky turbeuurija Denis Parinov avastas, et tänavu märtsis kolmekordistus populaarsete videokõneteenuste (Webex, GoToMeeting, Zoom ja teised) nimesid sisaldavate pahatahtlike failide arv võrreldes eelmise aasta kuude lõikes välja võetud numbritega.

Tõenäoliselt tähendab see, et kurjategijad on hakkanud ära kasutama Zoomi ja teiste sarnaste platvormide populaarsust, maskeerides pahavara videokonverentsiklientideks.

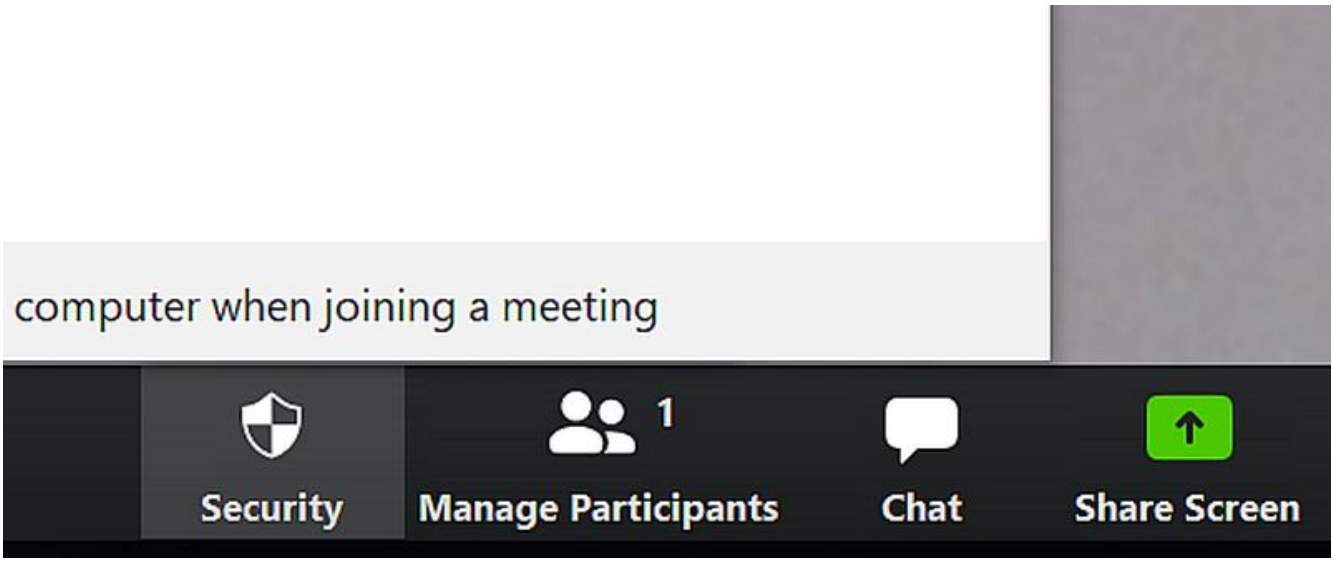
Zoomi turvaliseks allalaadimiseks Maci ja PC jaoks on soovitatav kasutada Zoomi ametlikku veebilehte zoom.us ning mobiilversiooni kasutamiseks külastada App Store'i või Google Play´d.

4. Ära kasuta videokõne linkide jagamiseks sotsiaalmeediat

Mõnikord on sul kindlasti soov korraldada avalikke üritusi ning paljudes asukohtades on veebis toimuvad sündmused ainus võimalik viis avaliku ürituse korraldamiseks. Just seetõttu meelitab Zoom üha enam inimesi. Ent isegi kui sinu üritus on tõepoolest kõikidele avatud, peaksid vältima lingi jagamist sotsiaalmeedias. Vastasel juhul on tõenäoline, et trollid võivad sinu üritust häkkida ning postitada sinna solvavat sisu - nähtus, mida nimetatakse nüüd *zoombombing´*uks.

5. Kaitse igat kohtumist salasõnaga

Salasõna seadistamine on endiselt parim viis tagamaks, et kohtumisel osaleksid ainult soovitud inimesed. Zoom muutis hiljaaegu salasõnaga kaitse vaikimisi valikuks, mis on hea samm. Nagu ka ürituse lingid, ei tohiks koosoleku paroolid kunagi ilmuda sotsiaalmeediasse ega muudesse avalikesse kanalitesse või on kõik sinu pingutused olnud ilmaasjata.



6. Kasuta *Waiting Room´*i

Üks seade, mis tagab sulle suurema kontrolli kohtumise üle, on *Waiting Room* - hiljuti muudetud vaikimisi seadeks - osalejad ootavad "ooteruumis", kuni *host* kiidab igaühe neist heaks. See annab sulle võimalust kontrollida kohtumisel osalejaid. Samuti saad selle abil soovimatu inimese koosolekult välja visata ning suunata ta ooteruumi. Soovitame jätta antud valiku märgituks.

7. Pööra tähelepanu ekraanijagamisfunktsioonidele

Iga tavaline videokõnerakendus pakub ekraani jagamist ehk osalejatele võimalust jagada omavahel ekraane. Zoom pole erand. Mõned sätted, millel tasub silma peal hoida:

- Ekraani jagamise võimalus ainult *host*ile või kõikidele osalejatele?
- Kas lasta mitmel osalejal jagada ekraani samaaegselt?

8. Võimalusel tööta veebiliideses

Erinevad Zoomi kliendirakendused on esile toonud mitmeid vigu. Mõni versioon lubab häkkeritel juurdepääsu seadme kaamerale ja mikrofonile, teised lubavad lisada nõusolekata kasutajaid. Zoom lahendas nii eelnimetatud kui ka muud sarnased probleemid kiiresti ning lõpetas kasutajaandmete jagamise Facebooki ja LinkdIN´iga. Kuna oht on siiski siiani võimalik, soovitame võimalusel rakenduse seadmesse installimise asemel kasutada Zoomi veebiliidest. Veebiliides asub brauseri liivakastis ja tal puuduvad installitud rakenduse õigused, piirates sedasi võimaliku kahju ulatust.

Võib juhtuda, et kui soovid kasutada veebiliidest, on Zoom juba installija alla laadinud ning koosolekuga liitumiseks pole paraku muud võimalust kui installimine. Sel juhul saad vähemalt piirata seadmete arvu, kuhu Zoom installitakse. Vali seade, millel puudub isiklik teave. See kõlab mõnevõrra paranoiliselt, ent parem karta kui kahetseda.

9. Veendu, et kasutad kõige uuemat Zoomi versiooni

Rakenduste uuendamine kohe pärast uue versiooni ilmumist on alati hea mõte - enamikul juhtudest sisaldavad uuendused eelmises versioonis leitud tõsiste turbevigade parandusi. Zoom pole erand - tõenäoliselt tegeleb uuem versioon teatud probleemide lahendamisega ja programmi turvalisuse parandamisega.

10. Ole kindel, mida lased inimestel kuulda või näha

See kehtib kõikide videokonverentsiteenuste kohta. Enne kõne alustamist mõtle, mida inimesed näevad või kuulevad. Isegi kui oled kodus täiesti üksi, eeldavad ekraani teisel poolel olevad kaaslased, et oled täielikult riides. Tavapärane hoolitsetud välimus on ilmselt hea mõte.

Sama kehtib ka sinu ekraani kohta, kui plaanid seda jagada. Sulge kõik veebiaknad, mida sa ei taha jagada teistega, olgu selleks siis üllatuskingituse ostmine või uue töökoha otsing, millest ülemus midagi teadma ei pea.

Eneseisolatsioon võib olla igav ja üksildane. Ent kujuta ette, kui see kõik oleks juhtunud enne lairibaühendust, videokonverentse ja muid kaugtöö võimalusi? Hea, et eksisteerivad Zoom´i taolised rakendused ja neid saab turvaliselt kasutada.

- Lahendused
- Turvalisus

Pilt

