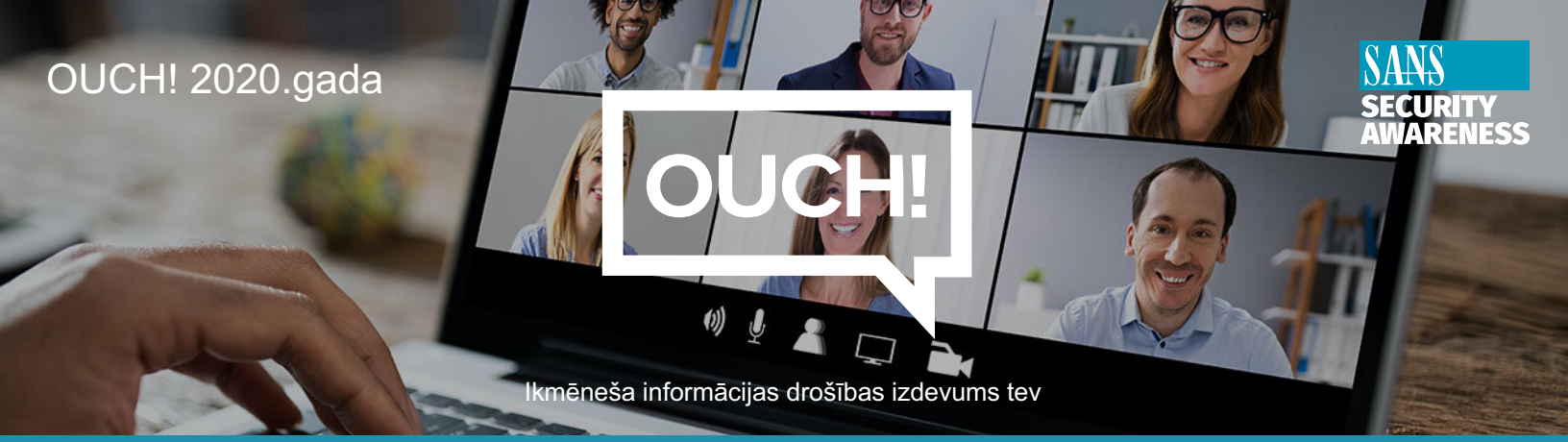
OUCH! 2020.gada



SANS SECURITY AWARENESS

Ikmēneša informācijas drošības izdevums tev

Drošas virtuālās konferences

Kas ir virtuālā konference?

Tā kā daudzi no mums šodien strādā no mājām, visticamāk, arī saziņa ar kolēģiem notiek attālināti, izmantojot virtuālo konferenču risinājumus, piemēram, Zoom, Slack vai Microsoft Teams. Jūsu ģimenes locekļi, iespējams, arī jūsu bērni, lieto šīs pašas tehnoloģijas, lai mācītos attālināti vai sazinātos ar draugiem. Neatkarīgi no tā, kāpēc izmantojat virtuālos saziņas rīkus, tālāk uzskaitītas būtiskākās lietas, kas jāievēro, lai izmantotu šīs tehnoloģijas droši.

Dalība virtuālajā konferencē

Ja jūs plānojat piedalīties virtuālajā sanāksmē, lūk 5 svarīgākie ieteikumi:

1. **Programmatūras atjaunināšana**: Pārliecinieties, vai vienmēr izmantojat jaunāko konferenču programmatūras versiju. Jo jaunāka un aktuālāka būs jūsu programmatūra, jo drošāks būsiet. Aktivizējiet programmatūras uzstādījumos automātisko atjaunināšanu. Kad esat beidzis tikšanos, izejiet no programmas, lai nākamajā pieslēgšanās reizē tā varētu automātiski meklēt un uzstādīt pēdējos atjauninājumus.
2. **Konfigurējiet audio / video uzstādījumus**: Iestatiet pēc noklusējuma izslēgtu mikrofonu un video, pieslēdzoties sapulcei; aktivizējiet tos tikai tad, kad vēlaties. Lai nodrošinātu konfidencialitāti, apsveriet iespēju aizklāt jūsu datora vai citas iekārtas kameru, kamēr nepiedalāties sanāksmēs. Atcerieties: ja kamera ir ieslēgta, ikviens var redzēt, ko jūs darāt, pat ja nerunājat.
3. **Divreiz pārliecināties par to, kas ir jums aiz muguras**: Ja vēlaties ieslēgt datora kameru, apskatieties, kas atrodas jums aiz muguras. Pārliecinieties, ka aiz jums nav redzama kāda jūsu personīgā vai cita sensitīva informācija. Dažas video konferenču programmatūras ļauj aizmiglot vai izmantot virtuālu fonu, līdz ar to pārējie nevar redzēt, kas atrodas aiz jums.
4. **Nedalieties ar jūsu ielūgumu**: Ielūguma saite pasākumam ir jūsu personīgā ieejas biļete. Pat ja uzticamam kolēģim ir nepieciešama ielūguma saite, ir drošāk, ja pats kolēģis to lūgs konferences organizatoriem.
5. **Neierakstiet pasākumu**: Bez atļaujas neveiciet konferences ierakstu un netaisiet ekrānšāviņus. Ja šie ekrānšāviņi vai ieraksti kļūs publiski, jūs nejauši būsiet dalījies, iespējams, ar ļoti sensitīvu informāciju.

Virtuālo konferenču organizēšana

Ja plānojat organizēsit virtuālu konferenci, lūk daži papildu ieteikumi.

1. **Nepieciešama parole**: Lai aizsargātu jūsu konferences konfidencialitāti un drošību, un kontrolētu, kurš var pievienoties, aizsargājiet sapulci ar paroli. Tā pasākumam varēs pievienoties tikai tie cilvēki, kuriem ir konferences parole.
2. **Pārbaudiet dalībniekus**: Pārbaudiet cilvēkus, kuri vēlas pievienoties jūsu pasākumam. Ja ir kāds, kuru jūs nepazīstat vai nevarat identificēt, pieprasiet personai apliecināt savu identitāti. Ja jums ir kādas bažas vai kāds izturas nepieklājīgi vai traucējoši, izraidiet šo dalībnieku no konferences. Daudzi risinājumi piedāvā iespēju slēgt konferenci, tiklīdz tā ir sākusies, līdz ar to neviens nevar pievienoties, ja vien jūs tos neielaižat. Vēl ir iespēja sākotnēji novietot konferences viesus virtuālā uzgaidāmajā telpā, lai jūs varētu apstiprināt, kurš pievienojas zvanam.
3. **Pasākuma ierakstīšana**: Ja plānojat pasākumu ierakstīt (un jums ir atļauja to darīt), pirms konferences noteikti informējiet visus.
4. **Dalīšanās ar ekrānu**: Ja plānojat kādā brīdī dalīties (koplietot) datora ekrānu, pirms tam noteikti aizveriet visas pārējās programmas un no datora ekrāna noņemiet visus sensitīvos failus. Atslēdziet arī visu uznirstošo paziņojumu parādīšanos. Tas palīdzēs nodrošināt, ka, daloties ar datora ekrāna saturu, jūs netīšām neparādīsiet arī sensitīvu vai apkaunojošu informāciju. Vēl iesakām apsvērt iespēju dalīties tikai ar to programmu, kuru vēlaties parādīt, nevis visu datora ekrānu.

Mūsdienu tehnoloģijas ir fantastisks līdzeklis un daudzējādā ziņā ieskicē arī mūsu nākotni, kā mēs strādāsim, sadarbosimies un sazināsimies ar citiem. Šīs vienkāršās darbības ilgtermiņā nodrošinās jūsu drošību.

Viesredaktors

Lodrina Cherne ir Galvenā drošības eksperte-advokāte Cybereason, kura aizsargā visus cilvēkus un informāciju mūsdienu plašajā interneta pasaulē. Viņa arī pasniedz Windows forensics SANS Institūtā un līdzdarbojas blogā ThisWeekin4n6. Jūs varat sekot viņai Twitter @hexplates.

Resursi

Kā padarīt paroles vieglāk iegaumējamas: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Paroļu pārvaldnieki: https://www.sans.org/security-awareness-training/resources/password-managers-0

Tulkojums: CERT.LV