

ZOOM

A ZOOM céget 2011-ben alapították és mára a videokonferenciákhoz szükséges szoftverfejlesztők között a világ élvonalába tartozik. A ZOOM sok funkciót képes ellátni, közvetíthet videokonferenciát, audiokonferenciát, ezenkívül csevegőt működtet, képernyőmegosztást, felvételt készítést, megosztást és tartalomböngészést is biztosít. A felhasználók a ZOOM segítségével saját találkozókat indíthatnak vagy bekapcsolódhatnak mások által létrehozott találkozóba is. Ez az applikáció számítógépen, notebookon, táblagépen vagy okostelefonon is működik, ráadásul a webáruházon keresztül ingyenesen letölthető közvetlenül a felhasználó gépére.

ZOOM BOMBING

Ez a kifejezés olyan illetéktelen személyeket jelöl, akik a zoomos találkozókhoz meghívás nélkül kapcsolódnak és azokon pornográf és nem oda illő videókat mutatnak be. A találkozókra bejuthatnak illetéktelen személyek is, ha ismerik a rendezvény azonosítóját (ID), amennyiben ez nincs jelszóval védve. Az anonimitás és az egyéb megelőző intézkedések megóvják a gyermekeket a szexuális, ill. a számukra nem megfelelő tartalomhoz való hozzáfutástól.

A PHISHING KOCKÁZATA

A ZOOM program népszerűségének növekedése hacker- és phishing támadások sokaságát idézte elő, mely utóbbi a látogatóknak olyan linkeket kínál, amelyről a látogató azt feltételezi, hogy valós találkozóhoz kapcsolódik, miközben mégsem. Ezen csalások célja érzékeny információk, pl. felhasználónevek vagy jelszavak, ill. hitelkártya-információk gyűjtése.

A MAGÁNSZFÉRA VÉDELME

Az alkalmazás beállításától függően a Zoom program minimális anonimitást biztosíthat. Sok esetben a találkozók szervezői aprólékos információkat is megtudhatnak a találkozók résztvevőiről, mint pl. az egész nevüket, telefonszámukat, sőt esetenként még tartózkodási helyüket is. Ezek birtokában fennáll a magánjellegű vagy személyes információk eltulajdonításának kockázata is, attól függően, hol van a webkamerás számítógép elhelyezve és mi látható a háttérben.

FELVÉTEL

A Zoom egyik funkciója az élő találkozók rögzítése. A találkozók felvételére elsődlegesen csak a találkozó házigazdája jogosult, de az ő engedélye után ugyanezt megtehetik a résztvevők is. A felvétel a gépbe elmenthető, utána korlátozás nélkül letölthető és megosztható. Ez azt jelenti, hogy a videók, a hanganyagok és a jegyzetek az interneten, ill. a felhasználók között szabadon megoszthatók az Ön engedélye nélkül is.

KISEBB CSOPORTOK TALÁLKOZÓI

A Zoom lehetővé teszi, hogy a kisebb csoportok "különtermekbe" vonulhassanak el a fő, közös találkozón kívül. A résztvevőket a házigazda tetszés szerint beoszthatja ezekbe a külön csoportos megbeszélésekre. Ez lehetőséget kínál arra, hogy a fő csoporton belül néhány felhasználó egymás között is beszélgethessen.

AZ ÉLŐ ADÁS KOCKÁZATAI

A Zoom élő sugárzást is lehetővé tesz. Ez azt jelenti, hogy ez természetszerűleg néhány kockázattal jár. Ellenőrzött környezetben ezek a kockázatok valószínűleg minimálisak (pl. a távoktatás tantermeiben). A tartalom nem mindig felülvizsgált, és azok a gyermekek, akik az applikációt felügyelet nélkül vagy laza biztonsági megkötésekkel használják, nagyobb valószínűséggel találkozhatnak koruknak nem megfelelő tartalommal. További rizikó lehet pl. káros utalások letöltése, személyi adatok megosztása vagy ismeretlen személyekkel való kapcsolatteremtés.

A HELYTELEN TARTALOM BEJELENTÉSE

Mint szülő vagy tanár Ön sokat tehet azért, hogy a gyermekek és tanulók nyíltan és bizalommal beszéljenek arról, amit láttak, hallottak és ami kellemetlenül érintette vagy felzaklatta őket. Azon túl, hogy Önnek erről beszámolnak, a helytelen tartalmat maguk is jelenthetik. A bejelenthető tartalmak közé tartoznak pl. a nemkívánatos aktivitások, a zaklatás és a kibertámadások, amelyek a Zoom programban található funkció segítségével közvetlenül bejelenthetők.

AZONOSÍTÓ ADATOK ÉS JELSZAVAK

A találkozót mindig sokkal célszerűbb egy véletlenszerűen, a program által generált azonosító számmal indítani, mintsem egy személyes számmal. Az előbbi nehezebben nyomozható ki és ezáltal az esetleges hackelés is kevésbé valószínű. Ügyeljen, hogy a találkozó azonosító számát ne ossza meg ismeretlen személlyel, és mindig adjon meg jelszót, amely lehetővé teszi, hogy a meghívottak bejelentkezhessenek.

VÉDJE SZEMÉLYI ADATAIT

Fontos, hogy beszélgessen el a gyermekkel a személyi adatok megosztásának veszélyeiről a Zoom applikációban. Ide tartoznak a jelszók, a lakcím, a telefonszám, stb. Hamis név alatt hozzon létre fiókot a gyermek számára és mindig használjon saját hátteret, amellyel elrejtheti a képeket a háztartásáról. A Zoom lehetővé teszi virtuális háttér vagy saját kép használatát háttérként, amely az Ön vagy gyermeke mögött jelenik meg a monitoron.

VIGYÁZZON A PHISHING E-MAILEKRE

Minden egyes alkalommal, amikor Ön vagy gyermeke meghívást kap egy online találkozóra, győződjön meg arról, hogy az a hivatalos oldalról jött és nem csalás. A phishing e-mail egyik jól felismerhető jele a szokatlan, esetleges e-mail cím, vagy a nem hivatalos doménnév. Az e-mail maga is tartalmazhat hibákat vagy gyanús mellékleteket.

KAPCSOLJA KI A

SZÜKSÉGTelen FUNKCIÓKAT

Van néhány funkció, melyeket ajánlott kikapcsolni a nagyobb biztonság érdekében. Például, a fájlok küldésének és magánbeszélgetések lehetőségének deaktiválásával kisebb lesz a kockázata annak, hogy a gyermek ártó mellékleteket vagy hamis üzeneteket kap. Ezenkívül ki lehet kapcsolni a kamerát és a mikrofont, ha ezekre nincs szükség a találkozó alatt.

HASZNÁLJA A VIRTUÁLIS VÁRÓTEREM FUNKCIÓT

A virtuális váróterem a Zoom-ban azt jelenti, hogy mindenkinek, aki a találkozóhoz csatlakozni szeretne, meg kell várnia, amíg a "házigazda" leellenőrzi a kilétét és beengedi. Ez egy előre beállítható funkció, amely újabb biztonságvédelmi és ellenőrző réteget biztosít.

LEGYEN AZ ALKALMAZÁS MINDIG AKTUÁLIS

Fontos az alkalmazás legújabb elérhető verzióját használni. Az újítások általában biztonsági hézagokat tömnek be, ezzel erősítve az applikáció biztonságos használatát.

HÁZIGAZDA

ÉS A MAGÁNSZFÉRA ELLENŐRZÉSE

Ha gyermeke egy nagyobb csoportos online találkozón vesz részt, szükséges biztosítani, hogy a házigazda betartsa a Zoom felhasználási feltételeit. Ide tartozik az is, hogy minden résztvevő beleegyezett a találkozó rögzítésébe. A házigazdának le kellene tiltania a többi résztvevő általi képernyő-megosztást és fájlküldést, így növelve az élő adás biztonságát.

ÜZENET SZÜLŐKNEK ÉS TANÁROKNAK

- Gyűjtsenek be információkat a Zoom applikációról és biztonsági beállításairól.
- Beszéljenek a gyerekekkel / diákokkal a védekezési lehetőségekről.
- Töltsenek időt a gyerekekkel / diákokkal, érdeklődjének online életükről.
- Ha "hibáznak", és erre joguk van, mert nem rendelkeznek az Önök tapasztalataival, segítsék őket, legyenek nyitottak, hogy bármikor megkereshessék Önöket és segítséget kérjenek.
- Vigyázzanak rájuk, hogy ne fogadjanak és ne nyissanak meg gyanús üzeneteket, postát vagy linkeket.
- Együtt tanulják meg, hogy mely információkat lehet biztonságosan megosztani, és mikor és hogyan.
- Ha a gyermek azzal szólítja meg, hogy olyasmire akadt az online térben, ami aggodalommal tölti el, értékelje, hogy megkereste Önt, beszélgessenek el róla és együtt keressék a megoldást.
- Ha úgy érzi, hogy Önnel nem akar erről beszélni, ajánlja fel neki, hogy felhívhat olyan vonalat, melyeken keresztül segítséget kaphat:

WWW.IPCO.SK

WWW.STALOSATO.SK

WWW.KRIZOVALINKAPOMOCI.SK

WWW.DOBALINKA.SK

0800 500 333

Magyarul:

Felvidéki Lelki Elsősegély Telefonszolgálat

0918 500 333 (Orange)

0904 500 338 (T-Mobile)

Kék vonal (MO): <https://kek-vonal.hu/>

WWW.STALOSATO.SK

#STOPONLINEGROOMING

#ZALEZINATEBE

#DEJESATO

#POMOCEXISTUJE

EZT A RÖPLAPOT AZ IPCO.SK

PSZICHOLOGUSAI ÁLLÍTOTTAK ÖSSZE.

ITT INSPIRÁLODTUNK: NATIONALONLINE SAFETY.COM

