

TEAMS

A Teams view olyan felület, amely audiovizuális csatornákon keresztül (audio, videó, hírek, csevegés) teszi lehetővé az online együttműködést diákok vagy szakemberek számára. Az alkalmazásban csak ketten vagy akár tízezren is találkozhatnak egyszerre az online térben.

SZEMÉLYI ADATOK KISZOLGÁLTATÁSA

Csakúgy, mint más közösségi oldalakon, itt is előfordulhat, hogy nem megbízható egyének személyi adatok (telefonszám, születési dátum, cím, bejelentkezési adatok stb.) megosztását fogják kérni tőlünk. Ha ilyen adatok nem megbízható személy birtokába jutnak, megnő az esélye annak, hogy "online zsebtolvajokkal" gyűlik meg a bajunk.

ZSAROLÁS, ZAKLATÁS ÉS MANIPULÁCIÓ

A tapasztalatok azt mutatják, hogy a cseten keresztül történő páros vagy csoportos beszélgetés során, ami a Teams alkalmazásban is lehetséges, növeljük annak az esélyét, hogy zsarolás, zaklatás vagy manipuláció áldozataivá válunk. A gyerekek például negatív kommenteket kaphatnak a személyüket illetően. Erről az online diszinhibíció-effektus (a gátlás gátlása) tehet, melynek következtében az online térben nyitottabbá válunk és könnyebben beszélünk olyan dolgokról, amelyek a hétköznapi beszélgetések során nem

NEM ODA ILLŐ KOMMUNIKÁCIÓ A CSETBEN

A csoportmunka keretében magánüzeneteket is lehet küldeni, melynek következtében a gyerekek gyakran osztanak meg oda nem illő tartalmat. Mivel a Teams általában az oktatást segíti, nagyon fontos, hogy fel tudják ismerni, mely információk illenek az adott helyzetben oda és melyek nem.

A MEGHEKKELES KOCKÁZATA

Csakúgy, mint minden más applikáció, a Teams is kerülhet hackerek célkeresztjébe és így kockázatosabbá válhat az érzékeny és személyi adatok szempontjából. Közismert az ún. "A man in the middle attack", vagyis olyan támadás, mikor két ember beszélgetéséhez észrevétlenül kapcsolódik egy harmadik, aki látja és hallja az összes megosztott információt és ezeket törvénytellenesen felhasználhatja.

A VÍRUSOK KOCKÁZATA

Online applikációk használatával automatikusan növeljük a lehetőségét annak, hogy számítógépes vírus áldozataivá válunk. Ebben az esetben csökken a számítógépünk (tablet, telefon) teljesítménye, hibásak vagy eltűnnek az adataink, adatszivárgás történik (érzékeny adatok/fájlok), stb.

A LIVE STREAMING KOCKÁZATA

Ahogy egyéb alkalmazások része a videón keresztül történő kommunikáció, a Teams is lehetővé teszi live stream-et. Annak ellenére, hogy oktatás közben a live stream-hez kapcsolódó kockázatok minimálisak, a live stream tartalma gyakran nincs ellenőrizve és így a gyermekek káros tartalmakhoz juthatnak.

HASZNOS TANÁCSOK A BIZTONSÁG NÖVELÉSÉRE

FELHASZNÁLÓK BLOKKOLÁSA

Ha a gyermekhez nem megfelelő tartalom jut el vagy online visszaélés áldozatává válik, az alkalmazás beállításában blokkolja a kapcsolatokat, amelyektől a támadások származnak. Hasznos blokkolni azokat a kapcsolatokat is, akik nem tüntetik fel a saját identitásukat. A gyermek így nem kommunikálhat számára ismeretlenekkel.

A SZEMÉLYI ADATOK VÉDELME

Hasznos, ha gyermekükkel elbeszélgetnek az érzékeny személyi adatok védelmének fontosságáról. Azt valljuk, hogy a gyerekeknek a lehető legkevesebb információt kellene megadniuk bármilyen közösségi oldalon való regisztrációnál, a Teams alkalmazást is beleértve. Ezzel együtt fontos, hogy felismerjék a veszélyt, ha valaki a személyi adataikat szeretné elkérni.

A MONITOR HÁTTERE

A magánszféra és személyes adatok védelme érdekében javasoljuk, hogy a videokonferencia vagy live stream közben használják az alkalmazásban található háttéreffektusokat. Ezek egyike az ún. "blur background", amely elmosódó háttérrel fest a gyermek köré és így a körülötte lévő környezet felismerhetetlenné válik. Háttérként használhat képet vagy fényképet is.

A SZÁMÍTÓGÉP BIZTONSÁGI BEÁLLÍTÁSAINAK AKTUALIZÁCIÓJA

A Teams alkalmazás installálásakor és későbbi használata során bizonyosodjon meg arról, hogy gépe biztonsági rendszerei aktuálisak (pl. antivírus program). Minimalizálja így egy lehetséges kibertámadás lehetőségét.

AZ AUDIO ÉS A VIDÉO KIKAPCSOLÁSA

Hasznos az audio és a videó kikapcsolása csoporttalálkozók esetében a Teams alkalmazáson belül (akkor, amikor éppen nem szólal fel). Kizárhatja ezzel a beszűrődő zajokat, esetleg az érzékeny információkat tartalmazó beszélgetéseket, amelyek zavarhatnák a tanítást, és ezzel egyúttal erősíti gyermeke biztonságát az applikáció használata közben.

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, beszélgesse 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.DOBRA LINKA.SK
0800 500 333

Magyarul:
Felvidéki Lelki Elsősegély
Telefonszolgálat
0918 500 333 (Orange)
0904 500 338 (T-Mobile)

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

További információ:
WWW.STALOSATO.SK
#STOPONLINEGROOMING
#ZALEZINATEBE
#DEJESATO
#POMOCEXISTUJE
EZT A RÓPLAPOT AZ IPČKO SK
PSZICHOLÓGUSAI ÁLLÍTOTTAK ÖSSZE.
ITT INSPIRÁLODTUNK: NATIONALONLINE SAFETY.COM

