

OUCH!

A Havi Biztonsági Tudatosságról szóló hírlevele

Biztonságos virtuális konferencia

Mi az a virtuális konferencia?

Sokunkhoz hasonlóan, az otthoni munkavégzés során valószínűleg Ön is tartotta a kapcsolatot kollégáival olyan virtuális konferencia megoldásokat használva, mint a Zoom, a Slack vagy a Microsoft Teams. Lehet, hogy családtagjai – talán még gyermekei is – ugyanezeket a technológiákat használják a barátokkal való kapcsolattartáshoz vagy a távoktatás során. Függetlenül attól, hogy miért használ távoli kapcsolatot, a következőkben megismerhet néhány olyan lépést, amelyek hozzájárulhatnak a technológiák biztonságos alkalmazásához.

Virtuális konferencián való részvétel

Öt kulcsfontosságú lépés, amennyiben arra készül, hogy részt vegyen egy virtuális konferencián.

1. **Frissítse a szoftvert:** Ügyeljen arra, hogy mindig a konferencia szoftver legújabb verzióját használja. Minél naprakészebb egy szoftver, Ön annál nagyobb biztonságban lesz. Engedélyezze az automatikus frissítést, és lépjen ki a programból ha készen van, így a következő újraindításkor a program leellenőrzi a legújabb frissítéseket.
2. **Audió / Videó beállítások konfigurálása:** Ha kapcsolódik egy megbeszéléshez, a beállításokban némítsa le a mikrofont és kapcsolja ki a kamerát, és csak akkor engedélyezze őket, amikor azokra szükség van. Amikor nem használja a számítógép webkameráját, fontolja meg annak eltakarását, hogy megóvja magánéletét. Ne feledje: ha a kamera be van kapcsolva, mindenki láthatja mit csinál, még ha éppen nem is beszél.
3. **Kétszer is ellenőrizze le mi van a háttérben:** Ha engedélyezni szeretné webkameráját, ügyeljen arra, hogy mi van Ön mögött. Ügyeljen arra, hogy hívás közben ne legyen látható személyes vagy bizalmas információ. Néhány videokonferencia szoftver lehetővé teszi a homályosítást vagy a virtuális háttér használatát, így az emberek nem látják, valójában mi van Ön mögött.
4. **Ne ossza meg meghívóját:** A meghívó az Ön személyes belépője a megbeszélésre. Még akkor is, ha egy megbízható munkatársnak van szüksége a linkre, sokkal jobb megoldás, ha a konferencia szervezőjétől kér egy saját meghívót.
5. **Ne rögzítsen:** Ne készítsen képernyőképeket vagy rögzítse a konferenciahívást engedély nélkül. Véletlenül megoszthat nagyon érzékeny információkat, ha ezek a képernyőképek vagy felvételek nyilvánossá válnak.

Virtuális konferencia szervezése

Ha virtuális konferenciát rendez, akkor íme néhány további lépés, amelyet meg kell tennie.

1. **Használjon jelszót:** A konferencia biztonságának védelme, valamint annak ellenőrzése érdekében, hogy kik csatlakozhatnak, használjon jelszót a megbeszéléshez. Ilyen módon csak a konferencia jelszával rendelkezők csatlakozhatnak az eseményhez.
2. **Tekintse át a résztvevőket:** Vizsgálja meg, kik csatlakoznak az eseményhez. Ha van valaki, akit nem ismer vagy nem tud azonosítani, kérje meg, hogy azonosítsa magát. Ha bármilyen aggálya van, vagy valaki durván és zavaróan viselkedik, távolítsa el őt a konferenciabeszélgetésből. Számos megoldás lehetőséget kínál arra, hogy a konferencia annak kezdete után zárolásra kerüljön, így senki más nem csatlakozhat, hacsak Ön be nem engedi őket. Egy másik lehetőség az, hogy a résztvevőket először egy virtuális váróterembe helyezi, így jóváhagyhatja, ki csatlakozik a híváshoz.
3. **Tájékoztassa a résztvevőket, ha rögzíti a megbeszélést:** Ha rögzíteni kívánja az eseményt (és van engedélye a felvétel készítésre), mindenképpen időben tájékoztasson minden résztvevőt.
4. **A képernyő megosztása:** Ha megosztja számítógépe képernyőjét, akkor mindenképpen zárjon be minden más alkalmazást, és távolítsa el minden érzékeny fájlt a számítógép asztaláról. Tiltsa le az előugró értesítéseket is. Ez segít abban, hogy a számítógép képernyőjének megosztásával véletlenül se osszon meg érzékeny vagy zavaró információkat. Egy másik lehetőség, ha csak a megmutatni kívánt programot osztja meg a teljes számítógép képernyő helyett.

Ezek a technológiák fantasztikus eszközök, és sok szempontból reprezentálják a jövőt, hogyan fogunk másokkal együttműködni, dolgozni és kommunikálni. Ezek az egyszerű lépések biztosítják a hosszútávú biztonságos felhasználást.

A szerzőről

Lodrina Cherne vezető biztonsági képviselő a [Cybereasonnél](#), aki védi az embereket és információkat a mai nyitott és összekapcsolt világban. A SANS Intézetnél [Windows digitális nyomelemzést](#) oktat, valamint közreműködik a [ThisWeekin4n6](#) blog vezetésében. Kövesd a Twitteren: [@hexplates](#).



Források

Egyszerű jelszókezelés: <https://www.sans.org/security-awareness-training/resources/making-passwords-simple>

Jelszókezelők: <https://www.sans.org/security-awareness-training/resources/password-managers-0>

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)

OUCH! A Sans Security Awareness részleg által közzétett és a [Creative Commons BY-NC-ND 4.0](#) licenz alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra. Szerkesztette: Walter Scrivens, Phil Hoffman, Alan Wagoner, Cheryl Conley