



Spoločnosť Zoom bola založená v roku 2011 a je jedným z popredných svetových poskytovateľov softvéru pre videokonferencie. Zoom disponuje množstvom funkcií, ako napríklad videokonferencie a zvukové konferencie, má k dispozícii chat, zdieľanie obrazovky, možnosť nahrávania, zdieľania a vyhľadávania obsahu. Používatelia môžu zahájiť svoje vlastné schôdzky alebo sa môžu pripojiť k schôdzkam založeným ostatnými. Aplikáciu je možné používať na počítačoch, notebookoch, tabletoch a smartfónoch, pričom si ju zadarmo môžete stiahnuť v obchode s aplikáciami priamo vo Vašich zariadeniach.

ZOOM BOMBING

„Zoom bombing“ je termín, ktorý charakterizuje a popisuje neoprávnené osoby pripájajúce sa k zoomovým stretnutiam bez pozvania a prezentujú pornografické alebo nevhodné videá. Neoprávnená osoba môže vstúpiť na schôdzku, ak pozná ID schôdzky, ktoré nie je posilnené heslom. Preventívne opatrenia a ochrana súkromia sú prostriedkami, ktoré sú nápomocné pri ochrane detí od sexuálneho alebo iného nevhodného obsahu.

RIZIKO PHISHINGU

Nárast popularity programu Zoom viedol k nárastu hackerských operácií a phishingových kampaní, ktoré účastníkom odporúčajú kliknúť na odkazy a pripojiť sa k tomu, o čom sa domnievajú, že sú legitímne schôdzky v aplikácii Zoom, ale v skutočnosti sú podvodné. Cieľom týchto podvodov je získať citlivé informácie, ako sú napríklad prihlasovacie údaje používateľa, heslá alebo informácie o kreditnej karte.

OCHRANA SÚKROMIA

V závislosti od toho, ako bola aplikácia nastavená, môže program Zoom ponúkať veľmi málo súkromia. V mnohých prípadoch môžu hostitelia schôdzky vidieť podrobné informácie o každom účastníkovi vrátane jeho celého mena, telefónne čísla a možno aj údaje o polohe. Tým existuje potenciálne riziko odcudzenia súkromných alebo osobných informácií aj v závislosti od toho, kde je počítač s kamerou umiestnený a čo je vidieť na pozadí.

NAHRÁVANIE

Jednou z funkcií Zoom je možnosť nahrávať živé stretnutia. Prioritne môže nahrávanie stretnutia povoliť iba hostiteľ schôdzky, ale aj ostatní členovia schôdze, ak im hostiteľ dá prístup. Nahrávky je možné ukladať do zariadenia a následne je možné ich sťahovať a zdieľať bez akýchkoľvek obmedzení. To znamená, že videá, zvukové nahrávky a prepisy záznamov môžu byť zdieľané na internete alebo medzi používateľmi bez Vášho súhlasu.

SÚKROMNÉ SCHÔDZKY V MENŠÍCH SKUPINÁCH

Zoom umožňuje skupinu rozdeliť do „Breakout rooms“, čo sú súkromné skupiny mimo hlavného stretnutia na Zoom. Hostiteľ môže ľubovoľne rozdeliť účastníkov pôvodnej schôdze na samostatné zasadnutia. To dáva možnosť hovoriť súkromne mimo hlavnej skupiny s ostatnými používateľmi.

RIZIKÁ ŽIVÉHO VYSIELANIA

Zoom podporuje živé vysielanie. To znamená, že nevyhnutne so sebou nesie niekoľko s tým súvisiacich rizík. V kontrolovanom prostredí ich bude pravdepodobne minimum (napr. v učebni v rámci dištančnej výučby). Obsah nie je vždy moderovaný a deti, ktoré používajú aplikáciu bez dozoru alebo s obmedzeným nastavením zabezpečenia, môžu byť vystavené vyššiemu riziku nevhodného materiálu. Medzi ďalšie riziká môže patriť sťahovanie škodlivých odkazov, zdieľanie osobných údajov alebo nadviazanie kontaktu s cudzou osobou.

NAHLÁSIŤ NEVHODNÝ OBSAH

Ako rodič a učiteľ môžete výrazne podporiť deti a žiakov k tomu, aby hovorili otvorene a s dôverou o tom, čo videli, počuli a cítili sa v tom nepríjemne alebo rozrušene. Okrem toho, že je tu priestor, aby sa obrátili na Vás, môžu nevhodný obsah nahlásiť. Hlásiť môžu nežiaduce aktivity, obťažovanie a kyber útoky priamo pomocou funkcie v Zoome.

ID A HESLÁ SÚKROMNÝCH SCHÔDZI POUŽÍVATEĽOV

Vždy je lepšie zostaviť schôdzku s náhodným identifikačným číslom vygenerovaným programom Zoom ako s použitím osobného čísla. Je ťažšie odhaliteľné a je menej pravdepodobné, že dôjde k hacknutiu. Dajte si pozor na zdieľanie ID schôdzky s niekým, koho nepoznáte a vždy nastavte funkciu hesla, ktorá umožní ostatným ľuďom prihlásiť sa.

CHRÁŇTE SVOJE OSOBNÉ ÚDAJE

Je dôležité, aby ste sa s dieťaťom porozprávali o zdieľaní osobných informácií v aplikácii Zoom. Patria sem heslá, ich adresa, telefónne číslo atď. Vytvorte účet dieťaťa pod falošným menom alebo pseudonymom a vždy nastavte vlastné pozadie, ktoré pomôže skryť podrobnosti vo Vašej domácnosti. Zoom umožňuje zapnúť virtuálne pozadia a zvoliť si vlastný obrázok, ktorý sa zobrazí za Vami alebo Vaším dieťaťom.

POZOR NA PHISHINGOVÉ E-MAILY

Zakaždým, keď Vy alebo Vaše dieťa získate odkaz na pripojenie, overte si, či pochádza z oficiálnej platformy a nie je podvodný. Medzi znaky phishingového e-mailu patrí napríklad nerozpoznatelná e-mailová adresa, neoficiálny názov domény. Samotný e-mail by mohol tiež byť zle napísaný alebo obsahovať podozrivé prílohy.

VYPNITE NEPOTREBNÉ FUNKCIE

Existuje niekoľko funkcií, ktoré môžete vypnúť, aby boli zážitky a stretnutia bezpečnejšie. Napríklad deaktivácia možnosti prenosu súborov alebo zapojenie sa do súkromných chatov, môže pomôcť znížiť riziko príjmu škodlivých príloh alebo falošných správ. Okrem toho môžete vypnúť kameru a mikrofón, ak ich nepotrebujete na stretnutí používať.

VYUŽITE FUNKCIU VIRTUÁLNEJ ČAKÁRNE

Funkcia čakárne v aplikácii Zoom znamená, že ktokoľvek, kto sa chce pripojiť do schôdzky v Zoome naživo, musí „počkať“, kým ho hostiteľ preverí a povolí mu prístup do stretnutia. Je to predvolená funkcia a pridáva ďalšiu možnosť ochrany a zabezpečenia.

UDRŽUJTE SVOJU VERZIU AKTUALIZOVANÚ

Je dôležité používať najnovšiu dostupnú verziu Zoom a vždy, keď je dostupná nová aktualizácia, tak ju použite. Tieto aktualizácie zvyčajne slúžia na posilnenie bezpečnostných dier, aby ste boli viac v bezpečí.

HOSTITEĽ A KONTROLA SÚKROMIA

Ak je Vaše dieťa súčasťou väčšej skupinovej schôdzky, je dôležité zabezpečiť, aby hostiteľ dodržiaval Zmluvné podmienky spoločnosti Zoom. Patrí sem aj skutočnosť, že získal povolenie všetkých používateľov na zaznamenávanie relácie. Hostiteľ by mal tiež nastaviť zdieľanie obrazovky na „iba hostiteľa“ a zakázať „prenos súborov,“ aby bol živý prenos v bezpečí.

Odkaz rodičom a učiteľom

Získajte informácie o aplikácii Zoom a bezpečnostných možnostiach, ktoré aplikácia ponúka. Hovorte so svojimi deťmi/žiakmi o možnostiach ochrany, budte pri Vašich deťoch/žiakoch, zaujímajte sa a rozprávajte sa o ich online živote. Ak „urobia chybu“ – majú na ňu právo, keďže nemajú toľko skúseností ako Vy – sprevádzajte ich, vytvorte im bezpečný a otvorený priestor, v ktorom môžu otvorene hovoriť a požiadať o pomoc. Podporte ich v tom, aby neprijímali a neotvárali podozrivé správy, maily a linky. Naučte sa spolu, aké informácie je bezpečné zdieľať, kde a ako. Ak sa Vám dieťa zdôverí, že narazilo na niečo, čo v ňom vyvoláva znepokojenie, oceňte to, rozprávajte sa o tom a riešte to spolu ak máte pocit, že sa s Vami o tom rozprávať nechce, povedzte mu, že existuje miesto, kde pomoc získa a nebude v tom osamote.

- SME TU -

www.ipcko.sk

www.stalosato.sk

www.krizovalinkapomoci.sk

www.dobralinka.sk

0800 500 333

Viac nájdete na

WWW.STALOSATO.SK

[#STOPONLINEGROOMINGU](https://twitter.com/STOPONLINEGROOMINGU)

[#ZALEZINATEBE](https://twitter.com/ZALEZINATEBE)

[#DEJESATO](https://twitter.com/DEJESATO)

[#POMOCEXISTUJE](https://twitter.com/POMOCEXISTUJE)

Tento poster pre Vás vytvorili
psychológovia z IPČko.sk.

Inšpirované: nationalonlinesafety.com



STALOSATO.SK



IPČko.sk
Internetová polícia pre mladých



Register domény .sk