

# Teams

Teams view je platforma poskytujúca priestor na vytváranie online spolupráce pre študentov alebo profesionálov prostredníctvom audiovizuálnych komunikačných kanálov (audio, video, správy – chat). Aplikácia ponúka priestor na stretnutie „jeden na jedného,“ ale aj na skupinové stretnutia s kapacitou až pre 10 000 ľudí naraz.

## ZVEREJŇOVANIE OSOBNÝCH ÚDAJOV

Tak ako aj pri iných sociálnych sieťach, tak aj tu sa môžu vyskytnúť situácie, v ktorých nedôveryhodná osoba žiada zdieľanie osobných, citlivých údajov (telefónne číslo, dátum narodenia, adresa, prístupové heslá atď.) Pri úniku takýchto informácií nedôveryhodnej osobe samozrejme rastie pravdepodobnosť stretnutia s „online vreckárom“.

## GYDIERANIE, OBŤAŽOVANIE A MANIPULÁCIA

Zo skúseností vieme, že riziko vydierania, obťažovania a manipulácie narastá v komunikácii vo forme chatu, ktorou Teams takisto disponuje, či už v podobe súkromných správ alebo v skupinových konverzáciách. V takýchto situáciách sa môže dieťa ocitnúť v kontakte s negatívnymi komentármi, ktoré sa týkajú jeho osoby. Za tento prejav môže tzv. disinhibičný efekt, ktorý má za následok to, že v online prostredí sme otvorenejší a ľahšie sa nám hovorí o veciach, ktoré by v bežnej komunikácii v takejto otvorenej podobe neodznali (pozitívne aj negatívne).

## NEVHODNÁ KOMUNIKÁCIA NA CHATOCH

Vzhľadom na dostupnosť funkcie posielania súkromných správ, aj v rámci skupinovej práce, sa deti môžu dostať do situácie, v ktorej zdieľajú nevhodný obsah. Nakoľko sa s Teams pracuje väčšinou v školskom prostredí, je dôležité, aby vedeli rozpoznať, ktoré informácie do chatu v danej situácii patria a ktoré nie.

## RIZIKO HACKINGU

Ako každá aplikácia, aj Teams môže byť terčom hackerov a môže predstavovať riziko úniku citlivých informácií a osobných údajov. V brandži je známy tzv. „A man in the middle attack,“ v ktorej sa do komunikácie dvoch ľudí nepozorovane pripojí tretia osoba, ktorá všetky zdieľané údaje vidí, počuje a môže s nimi nelegálne zaobchádzať.

## RIZIKO VÍRUSOV

Používanie online aplikácií a platforiem prináša so sebou automaticky riziko vystavenia sa počítačovému vírusu. V takejto situácii sa dá spozorovať slabší výkon počítača (tabletu, telefónu), chybovosť alebo absencia dát, uniknutie citlivých informácií/súborov a pod.

## RIZIKO LIVE STREAMINGU

Ako aj ostatné aplikácie disponujúce možnosťou komunikovať aj cez video, tak aj Teams poskytuje funkciu live-streamov. Napriek tomu, že v školskom prostredí sú riziká live-streamu redukované na minimum, live-stream je často necenzurovaný a teda počas neho môže dieťa prísť do kontaktu s nejakým nevhodným obsahom.

# Užitočné rady pre zvýšenie bezpečnosti

## BLOKOVANIE UŽÍVATEĽOV

Ak dieťa dostane na Teams správy s nevhodným obsahom alebo ak sa v nejakej inej forme ocitne v situácii ako obeť online zneužívania, kontakty, od ktorých tieto útoky smerujú zablokujte v nastaveniach aplikácie. Za užitočné považujeme takisto blokovanie kontaktov, ktoré nezobrazujú svoju vlastnú identitu. Dieťa tým pádom nebude komunikovať s niekým, koho nepozná.

## OCHRANA OSOBNÝCH ÚDAJOV

Vnímame ako prospešné, ak s dieťaťom komunikujete o dôležitosti zachovania citlivých osobných údajov v bezpečí. Veríme, že deti by mali dávať minimum informácií pri vytváraní účtu na akejkoľvek sociálnej sieti vrátane Teams. Zároveň je však pre ne rovnako dôležité rozoznať riziko, ak si od nich osobné údaje pýta niekto iný a uvedomiť si potenciálnu hrozbu.

## POZADIE NA OBRAZOVKE

Pre zvýšenie ochrany súkromia a citlivých údajov počas video hovoru alebo live-streamu odporúčame pridať efekty pozadia, ktoré sú k dispozícii v aplikácii. Jedným z efektov je tzv. „Blur background,“ ktorého úlohou je rozmazať pozadie okolo dieťaťa, aby tak druhé strany nevideli prostredie, v ktorom sa nachádza. Pozadie taktiež môžete nahradiť aj úplne inou fotografiou alebo obrázkom.

## AKTUALIZÁCIA POČÍTAČOVEJ BEZPEČNOSTI

Pri inštalovaní a následnom využívaní aplikácie Teams sa skúste uistiť, že sú všetky zložky bezpečnosti a ochrany systému aktualizované (antivírusy a pod.) s cieľom minimalizácie kyber útoku.

## VYPÍNANIE AUDIA A VIDEO

Za užitočné považujeme vypínanie audia a aj videa počas skupinovej komunikácie na Teams (v prípade, ak nemáte slovo). Takto viete eliminovať zvuky, poprípade rozhovory obsahujúce citlivé informácie, ktoré narúšajú pracovný proces v skupine a zároveň zvyšovať bezpečnosť súkromia detí počas využívania aplikácie.

## Odkaz rodičom a učiteľom

Získajte informácie o aplikácii Microsoft Teams a bezpečnostných možnostiach, ktoré aplikácia ponúka, hovorte so svojimi deťmi/žiakmi o možnostiach ochrany, buďte pri Vašich deťoch/žiakoch, zaujímajte sa a rozprávajte sa o ich online živote ak „urobia chybu“ – majú na ňu právo, keďže nemajú také skúsenosti 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 získá a nebude v tom osamote.

- SME TU -

[WWW.IPCO.SK](http://WWW.IPCO.SK)

[WWW.STALOSATO.SK](http://WWW.STALOSATO.SK)

[WWW.KRIZOVALINKAPOMOCI.SK](http://WWW.KRIZOVALINKAPOMOCI.SK)

[WWW.DOBRALINKA.SK](http://WWW.DOBRALINKA.SK)

0800 500 333.

Viac nájdete na

[WWW.STALOSATO.SK](http://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](http://nationalonlinesafety.com)



STALOSATO.SK

