

Kategoria: Aktualności

Opublikowano: środa, 20, maj 2020 10:39

Małgorzata Orłowska

Odsłony: 1392

---

W czasie trwania pandemii a co za tym idzie podczas pracy zdalnej szczególnie popularne i przydatne stały się narzędzie umożliwiające odbycie wideokonferencji. Dzięki temu możliwe jest wirtualne spotkanie współpracowników i omówienie najważniejszych spraw. Co jednak robić, by mieć pewność, że sposób, w jaki korzystamy z wideokonferencji jest bezpieczny? Urząd Ochrony Danych Osobowych opublikował swoje wytyczne w tej sprawie.

Przed rozpoczęciem wideokonferencji:

1. Zapoznaj się z ogólnymi warunkami lub polityką prywatności programu, z którego chcesz skorzystać
2. Sprawdź, czy Twoje rozmowy będą nagrywane i przechowywane
3. Zweryfikuj, do jakich celów wykorzystywane będą Twoje dane osobowe
4. Sprawdź, o jakie uprawnienia do danych jesteś proszony – lista kontaktów, lokalizacja itp.
5. Do zainstalowania aplikacji na komputerze użyj oficjalnej strony aplikacji z której chcesz skorzystać; w przypadku urządzeń mobilnych wybierz oficjalny sklep – Google Play lub App Store
6. Upewnij się, że osoby postronne nie mają dostępu do Twojego ekranu
7. Sprawdź, czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie
8. Korzystaj z aplikacji webowych, nie desktopowych
9. Zabezpiecz sieć Wi-Fi silnym hasłem
10. Przed udostępnieniem swojego ekranu podczas rozmowy zamknij wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli
11. Przy podłączeniu się do telekonferencji korzystaj z kodów dostępu/PIN-ów
12. Przeskanuj program do telekonferencji systemem antywirusowym lub antymalware-owym

W trakcie korzystania z wideokonferencji:

1. Ogranicz ilość podawania danych osobowych – użyj pseudonimu i służbowego adresu e-mail
2. Użyj innego hasła, niż używane przez Ciebie w innych usługach
3. Nie udostępniaj linków do konferencji w mediach społecznościowych
4. Włącz, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line
5. Zarządzaj opcjami udostępniania ekranu
6. W celu wykonywania rozmów służbowych wykorzystuj dostęp do sieci za pomocą szyfrowanego połączenia VPN
7. Nie udostępniaj dokumentów służbowych, za pomocą czatu, który może być publiczny
8. Jeżeli to możliwe korzystaj z opcji zamazywania tła (tak, żeby rozmówcy nie widzieli Twojego otoczenia)
9. Korzystaj z opcji „poczekalnia” tak, abyś mógł kontrolować osoby uczestniczące w telekonferencji, unikniesz przypadkowych lub niechcianych osób
10. Logując się do telekonferencji, wyłącz mikrofon i kamerę (włączysz je jak będzie to potrzebne)

Po skorzystaniu w wideokonferencji:

1. Wyłącz mikrofon i kamerę
2. Upewnij się, że zakończyłeś spotkanie on-line i zamknąłeś aplikację
3. Sprawdź, czy program do telekonferencji nie działa w tle

Źródło: UODO