

BEZPIECZEŃSTWO W SIECI W TRAKCIE ZDALNEJ NAUKI

INFORMACJE DOTYCZĄCE BEZPIECZNYCH ZACHOWAŃ W SIECI W CZASIE ZDALNEJ NAUKI



1. Korzystaj z oprogramowania antywirusowego.
2. Uważaj na e-maile otrzymane od nieznanych Ci osób. Nigdy nie otwieraj podejrzanych załączników i nie korzystaj z linków przesłanych przez obcą osobę! Mogą na przykład zawierać wirusy. Najlepiej od razu kasuj maile od nieznanomych.
3. Ostrożnie pobieraj pliki z sieci.
4. Unikaj klikania w nieznane linki i załączniki w wiadomościach e-mail.
5. Nigdy nie podawaj na swojej stronie adresu domowego, numeru telefonu, informacji o rodzicach, itp. Bez zgody rodziców nie publikuj też na niej zdjęć swoich, rodziny ani nikogo innego, kto nie wyrazi na to zgody.
6. Chroń swoje konta na serwisach społecznościowych.
7. Stosuj trudne do odgadnięcia hasła, które są kombinacją liter i cyfr.
8. Czytaj regulaminy.
9. Sprawdzaj, czy strona, do której się logujesz, ma zabezpieczenie SSL.
10. Pamiętaj, że osoba po drugiej stronie nie musi być tym, za kogo się podaje.

- Rozmawiaj z rodzicami o Internecie. Informuj ich o wszystkich stronach, które Cię niepokoją. Pokazuj im również strony, które Cię interesują i które często odwiedzasz.
- Nie bądź wulgarny, stosuj się do zasad ortografii i interpunkcji.
- Nie wysyłaj tzw. łańcuszków szczęścia.
- Nie wysyłaj e-maili do wielu osób jednocześnie z jawnymi adresami – stosuj kopię ukrytą.
- Nie wysyłaj niepotrzebnych wiadomości SPAM.
- Traktuj innych tak, jak chcesz, żeby oni traktowali Ciebie.
- Jeżeli wiadomość, którą otrzymałeś jest wulgarna lub niepokojąca, nie odpowiadaj na nią. Pokaż ją swoim rodzicom lub innej zaufanej osobie dorosłej.

PAMIĘTAJ!

Mimo, że komunikacja w Internecie przebiega inaczej niż w realnym życiu, nie oznacza to, że masz prawo być niekulturalny. Dlatego bez względu na to czy kogoś znasz, czy nie, zawsze zachowuj się według obowiązujących zasad.

Dobre praktyki pomagające zachować bezpieczeństwo danych podczas lekcji online

20 zasad bezpieczeństwa, o których powinni pamiętać zarówno szkolni administratorzy, jak i nauczyciele oraz uczniowie, przygotowując się do lekcji online, aby chronić swoje dane:

- Na bieżąco aktualizuj systemy operacyjne.
- Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware.
- Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware.
- Pobieraj oprogramowanie wyłącznie ze stron producentów.
- Nie otwieraj załączników z nieznanymi źródłami dostarczanych poprzez korespondencję elektroniczną.
- Nie zapamiętuj haseł w aplikacjach webowych.

- Nie zapisuj haseł na kartkach.
- Nie używaj tych samych haseł w różnych systemach informatycznych.
- Zabezpieczaj serwery plików czy inne zasoby sieciowe.
- Zabezpieczaj sieci bezprzewodowe – Access Point.
- Dostosuj złożoność haseł odpowiednio do zagrożeń.
- Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.
- Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urzędów lub publicznych niezabezpieczonych sieci Wi-Fi.
- Wykonuj regularne kopie zapasowe.
- Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
- Szyfruj dane przesyłane pocztą elektroniczną.
- Szyfruj dyski twarde w komputerach przenośnych.
- Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.
- Odchodząc od komputera, blokuj stację komputerową.
- Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.

Źródło: www.uodo.gov.pl

Dane osobowe bezpieczne podczas zdalnego nauczania

W związku z pandemią koronawirusa poczta elektroniczna i inne elementy pracy grupowej, takie jak narzędzia konferencyjne lub komunikatory internetowe stały się wsparciem dla wielu uczniów i nauczycieli, wykorzystujących zdalne metody nauczania. Korzystając z nich, warto pamiętać o bezpiecznym przetwarzaniu danych.

Jeśli jesteś nauczycielem...

— Nauczyciel może przetwarzać dane osobowe uczniów i ich rodziców tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.

— Nauczyciel musi pamiętać o bezpiecznym korzystaniu z komputerów i innych urządzeń zarówno wtedy, gdy zapewnił mu je pracodawca, jak i wtedy, gdy korzysta z własnych.

— RODO nie zabrania wykorzystywania przez nauczyciela prywatnego komputera, tabletu, czy telefonu do przetwarzania danych osobowych w związku ze zdalnym prowadzeniem zajęć. Urządzenia te muszą być jednak odpowiednio zabezpieczone, a nauczyciel powinien postępować zgodnie z polityką lub inną procedurą wprowadzoną w tym zakresie w szkole.

— Jeżeli nauczyciel używa własnego urządzenia, powinien samodzielnie spełnić podstawowe wymogi bezpieczeństwa. Przede wszystkim należy sprawdzić, czy wykorzystywane urządzenie ma aktualny system operacyjny, czy używane są na nim programy, w szczególności programy antywirusowe, czy dokonane są niezbędne aktualizacje. Na bieżąco aktualizowane powinny być także zainstalowane programy antymalware i antyspyware. Należy rozważnie instalować na swoich urządzeniach oprogramowanie i pobierać je tylko z wiarygodnych źródeł (ze stron producentów).

— Przechowując dane na sprzęcie, do którego mogą mieć dostęp inne osoby, należy używać mocnych haseł dostępowych, a przed odejściem od stanowiska pracy urządzenie powinno zostać zablokowane. Zalecane jest także skonfigurowanie automatycznego blokowania komputera po pewnym czasie bezczynności oraz założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób.

— Podczas korzystania z programów lub aplikacji mobilnych należy korzystać z możliwych do zastosowania w nich mechanizmów ochrony prywatności użytkowników. Jeśli użycie jakiegoś programu wymaga logowania, warto zadbać o silne hasło dostępu, a dodatkowo chronić je przed utratą czy dostępem osób nieuprawnionych.

— Gdy dane są przechowywane na urządzeniach przenośnych (np. pamięć USB), muszą być bezwzględnie szyfrowane i chronione hasłem, by zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub

niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

— W podstawowym zakresie komunikację z uczniami i rodzicami prowadzi się poprzez wdrożone w szkole rozwiązania teleinformatyczne, np. dzienniki elektroniczne. W takiej sytuacji nauczyciel musi nadal zachowywać podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z dziennikiem elektronicznym ze swojego urządzenia w domu.

— Prowadzenie zajęć zdalnych może wymagać korzystania przez nauczyciela z poczty elektronicznej do kontaktu z uczniami lub rodzicami. Nauczyciel powinien prowadzić taką korespondencję ze służbowej skrzynki pocztowej, którą powinna zapewnić mu szkoła. Jeżeli szkoła nie zapewniła nauczycielom służbowych skrzynek poczty elektronicznej, to jeżeli wykorzystują oni do celów służbowych prywatną skrzynkę pocztową muszą pamiętać, aby korzystać z niej w sposób rozważny i bezpieczny.

— Szczególną uwagę nauczyciel musi zwrócić na zabezpieczenie danych osobowych udostępnianych w przesyłanych wiadomościach. Zawsze przed wysłaniem wiadomości, należy upewnić się, czy niezbędne jest wysłanie danych osobowych, oraz że zamierza wysłać ją do właściwego adresata. Ponadto trzeba sprawdzić, czy w nazwie adresu e-mail adresata nie ma np. przestawionych lub pominiętych znaków tak, aby nie wysłać takiej wiadomości do osób nieupoważnionych. Podczas wysyłania korespondencji zbiorczej powinno się korzystać z opcji „UDW”, dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail.

— Nauczyciel powinien wykorzystywać w zdalnym prowadzeniu zajęć te platformy edukacyjne lub narzędzia do e-learningu, które zostały wdrożone w szkole. W takiej sytuacji może oczekiwać, że prowadzenie zajęć zdalnych będzie bezpieczne. Powinien wtedy przestrzegać przyjętych przez szkołę instrukcji i procedur dotyczących ochrony danych osobowych oraz musi zachować podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z taką platformą ze swojego urządzenia w domu.

– Szkoła powinna samodzielnie wdrożyć wybraną spośród dostępnych metodę i technikę kształcenia na odległość lub inny sposób realizacji zadań zdalnie. Nauczyciele nie powinni jednak sami decydować o korzystaniu z konkretnych rozwiązań (np. prowadzenie lekcji za pomocą komunikatorów czy wideonarzędzi). Biorąc jednak pod uwagę nadzwyczajną sytuację i konieczność natychmiastowego rozpoczęcia zajęć zdalnych, może to być w niektórych sytuacjach uzasadnione. Należy jednak pamiętać, że za przetwarzanie danych uczniów przy wykorzystaniu narzędzi wdrożonych samodzielnie przez nauczyciela zawsze odpowiedzialność ponosi szkoła. Dlatego przyjmowanie określonego rozwiązania powinno się odbywać w uzgodnieniu z dyrektorem szkoły, który musi mieć świadomość jakie narzędzia są wykorzystywane do prowadzenia zdalnej edukacji w szkole, lub wyznaczonym przez niego koordynatorem pracy zdalnej w szkole. Takie rozwiązanie powinno być traktowane jako tymczasowe.

– Zawsze przy wyborze aplikacji lub innych narzędzi wykorzystywanych do zdalnej edukacji bądź komunikacji z uczniami należy się zastanowić, czy jest niezbędne, aby przetwarzały one dane osobowe, a jeżeli tak, czy można zminimalizować ich zakres, bądź wykorzystywać tylko pseudonimy (np. pierwsza litera imienia itp.). Należy także sprawdzić zasady świadczenia usługi i zasady przetwarzania danych przez usługodawcę (politykę prywatności).

– W obecnej sytuacji nauczyciel w porozumieniu z dyrektorem szkoły powinien uwzględnić, jakie realne możliwości komunikowania się z nim mają uczniowie lub rodzice, pod warunkiem, że wskazany przez nich konkretny rodzaj komunikatora internetowego zapewnia bezpieczeństwo komunikacji.

– Na ogólnie dostępnych portalach lub stronach internetowych nauczyciel może jedynie publikować materiały edukacyjne, natomiast nie może przetwarzać danych osobowych uczniów lub rodziców.

– W celu sprawdzania i monitorowania obecności uczniów w zajęciach prowadzonych zdalnie nauczyciel powinien zachować proporcjonalność i minimalizację danych. Dla przykładu nie może w tym celu korzystać z narzędzi

zbierających dane biometryczne, w tym wykorzystujących systemy wykrywania twarzy.

Jeśli jesteś rodzicem...

—Szkoła może wymagać od ucznia jedynie danych niezbędnych do założenia przez niego konta w odpowiednim systemie zdalnego nauczania oraz w celu realizacji obowiązku nauki w formie zdalnej (na podstawie art. 35 ustawy – Prawa oświatowego w związku z art. 6 ust. 1 lit. e RODO).

— Rodzic (opiekun prawny) ma prawo wiedzieć, jak szkoła jako administrator będzie przetwarzała dane osobowe jego dziecka w trakcie nauki zdalnej oraz jakie w związku z tym przysługują mu prawa.

— Jeżeli platformy wykorzystywane do zdalnego nauczania są odrębnymi od szkoły administratorami przetwarzanych przez siebie danych, to rodzice i dzieci powinni od nich otrzymać klauzulę informacyjną o podstawowych zasadach i zakresie zbierania danych oraz administratorze, np. podczas zakładania konta.

Uwaga!

Podstawę prawną realizacji zajęć szkolnych w formie pracy zdalnej określa rozporządzenie Ministra Edukacji Narodowej z 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. poz. 493).

Warto przeczytać:

- ochrona danych osobowych podczas pracy zdalnej>> <https://uodo.gov.pl/pl/138/1459>
- dane dzieci bezpieczne w sieci>> <https://uodo.gov.pl/pl/138/1363>
- ochrona danych osobowych w szkole>> <https://uodo.gov.pl/pl/383/479>
- tworzenie haseł dostępowych>> <https://uodo.gov.pl/pl/138/1285>

Źródła:

www.sieciaki.pl

<https://www.gov.pl/web/edukacja/zdalne-nauczanie-uodo>