Dobre praktyki pomagające zachować bezpieczeństwo systemu i danych podczas lekcji online

Zasady bezpieczeństwa, o których powinni pamiętać zarówno uczniowie jak i nauczyciele, przygotowując się do lekcji online, aby chronić swoje dane i nie tylko:

1. Na bieżąco aktualizuj systemy operacyjne, w tym firewall.

2. Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware.

3. Ustaw program antywirusowe na automatyczne skanowanie nośników USB po ich włożeniu do gniazda komputera.

4. Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware.

5. Pobieraj oprogramowanie wyłącznie ze stron producentów.

6. Nie otwieraj załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.

7. Nie zapamiętuj haseł w aplikacjach webowych.

8. Nie zapisuj haseł na kartkach.

9. Nie używaj tych samych haseł w różnych systemach informatycznych.

10. Zabezpieczaj serwery plików czy inne zasoby sieciowe.

11. Zabezpieczaj sieci bezprzewodowe – Access Point.

12. Dostosuj złożoność haseł odpowiednio do zagrożeń.

13. Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.

14. Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.

15. Wykonuj regularne kopie zapasowe swoich danych, aktualizuj kopie systemu.

16. Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.

17. Szyfruj dane przesyłane pocztą elektroniczną.

18. Szyfruj dyski twarde w komputerach przenośnych.

19. Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.

20. Odchodząc od komputera, blokuj stację komputerową. Stosuj hasło do swojego konta i wygaszacz z wylogowaniem.

21. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.

Źródło: www.uodo.gov.pl

Edward Krawecki