



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

1. Na bieżąco aktualizuj systemy operacyjne.
2. Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware.
3. Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware.
4. Pobieraj oprogramowanie wyłącznie ze stron producentów.
5. Nie otwieraj załączników z nieznanymi źródłami dostarczanych poprzez korespondencję elektroniczną.
6. ~~Nie zapamiętuj haseł w aplikacjach webowych.~~
7. ~~Nie zapisuj haseł na kartkach.~~
8. ~~Nie używaj tych samych haseł w różnych systemach informatycznych.~~
9. ~~Zabezpieczaj serwery plików czy inne zasoby sieciowe.~~
10. Zabezpieczaj sieci bezprzewodowe – Access Point.
11. Dostosuj złożoność haseł odpowiednio do zagrożeń.
12. Unikaj wchodzenia na nieznaną czy przypadkową stronę internetową.
13. ~~Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanymi urządzeniami lub publicznymi niezabezpieczonymi sieciami Wi-Fi.~~
14. Wykonuj regularne kopie zapasowe.
15. Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
16. ~~Szyfruj dane przesyłane pocztą elektroniczną.~~
17. ~~Szyfruj dyski twarde w komputerach przenośnych.~~
18. Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.
19. Odchodząc od komputera, blokuj stację komputerową.
20. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.