T: Jak dbać o bezpieczeństwo dziecka w Internecie – zdalne nauczanie

Przypominam!

Podczas poprzednich zajęć uczniowie klasy VII mieli wykonać test ze strony Migra.pl odnoszący się do wiadomości z działu „Praca z dokumentem tekstowym". Jedynie dwie osoby przystąpiły do jego rozwiązania.

Na kolejnych zajęciach w dniu 23.04.2020 r. test będzie udostępniony na stronie test.migra.pl – przystąpienie do niego jest obowiązkowe.
Test będzie aktywny w godz. 9.00 – 21.00.

Na dzisiejszych zajęciach chciałbym przekazać kilka ważnych informacji zarówno dla uczniów jak też dla ich rodziców. Dlatego też, podane poniżej informacje z zajęć, proszę by zostały przekazane również rodzicom, aby mogli się z nimi zapoznać.

Nauka jest bardzo ważna ale równie ważne jest bezpieczne zdobywanie, o co nieustanie wszyscy walczymy.

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 nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.
6. Nie zapamiętuj haseł w aplikacjach webowych (program internetowy na serwerze łączący się z Twoim komputerem przez przeglądarkę).
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 nieznane czy przypadkowe strony internetowe.

13. Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci 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 (ruch połączeń w sieci).
19. Odchodząc od komputera, blokuj stację komputerową.
20. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.