Zasady bezpieczeństwa w sieci

(dla nauczycieli i rodziców)

1. Pamiętaj o tym, aby zawsze korzystać z aktualnego programu antywirusowego – wybieraj oprogramowanie zaufanych dostawców. Warto również na bieżąco i regularnie skanować komputer pod kątem wirusów i złośliwego oprogramowania. Dbaj o aktualność systemu operacyjnego.

2. Twórz bezpieczne, skomplikowane hasła – nie wybieraj tych, które są łatwe do odgadnięcia. Zadbaj o to, aby mieć inne hasło do każdego portalu i profilu – dzięki temu nawet w sytuacji, kiedy Twoje hasło do jednego miejsca zostanie wykradzione, inne hasła pozostaną bezpieczne. Warto również korzystać ze specjalnych generatorów haseł, które pozwalają na stworzenie długich, bardzo skomplikowanych haseł zabezpieczających.

3. Zwracaj uwagę, czy witryna, z którą chcesz się połączyć, posiada certyfikat SSL – dzięki temu zyskasz pewność, serwer, z którym się łączysz, jest tym właściwym, a IP nie zostało podmienione. Dzięki certyfikatom SSL internetowe transakcje są o wiele bardziej bezpieczne – na przykład w sklepach internetowych. Strona z certyfikatem jest zwykle oznaczona na początku adresu symbolem kłódki lub napisem https://. Kliknięcie na ikonie kłódki pozwala uzyskać więcej informacji na temat certyfikatu.

4. Nie podawaj w Internecie żadnych prywatnych danych – unikaj wszelkich ogłoszeń o pracę lub serwisów, wymagających podania numeru PESEL, numeru dowodu osobistego, adresu, nazwiska czy numeru telefonu.

5. Unikaj pobierania plików z niepewnych źródeł, na przykładu plików z serwisów typu Torrent.

6. Nie otwieraj podejrzanych wiadomości e-mail, nie pobieraj załączonych w nich plików oraz nie wchodź na strony z linków w takich wiadomościach – mogą one zawierać złośliwe oprogramowanie.

7. Unikaj nawiązywania relacji z osobami, których nie znasz – jeśli ktoś obcy zaprasza Cię do znajomych na portalu społecznościowym, bezpieczniej będzie odrzucić takie zaproszenie.

8. Uważaj na skrócone adresy URL – często mogą stanowić niebezpieczną pułapkę. Jeśli chcesz skorzystać ze skróconego linku, upewnij się, że został udostępniony przez osobę, którą znasz lub pochodzi z bezpiecznego źródła (Np. z dziennika elektronicznego Librus).

9. Dwukrotnie przemyśl, zanim pozwolisz aplikacji na uzyskanie dostępu do Twojej lokalizacji, czy treści w telefonie. Ta sama zasada dotyczy korzystania ze stron internetowych – nie klikaj “Akceptuję”, czy “Potwierdzam” za każdym razem, kiedy chcesz jak najszybciej dostać się na witrynę internetową. W ten sposób udzielasz zezwoleń na dostęp do wielu informacji – warto najpierw zapoznać się z regulaminem i dokładnie sprawdzić, co akceptujesz.

10. Do połączeń bezprzewodowych wykorzystuj tylko zaufane punkty dostępowe. Nie loguj się do otwartych/publicznych, niezabezpieczonych sieci Wi-Fi.

11. Jeżeli korzystasz z aplikacji dostępnych w chmurze za pośrednictwem przeglądarki internetowej, to każdorazowo po zakończeniu pracy pamiętaj o wylogowaniu się z tego typu usług i zamknij program przeglądarki.