**ZASADY BEZPIECZEŃSTWA W INTERNECIE**

**Moduł 4– Wiedza o zdrowiu i wykorzystanie usług interaktywnych: Media społecznościowe**

Poniżej przedstawiamy krótką listę zasad, o których należy pamiętać, aby zachować pozytywne wrażenia z interakcji online, prawidłowo korzystać z urządzeń i zachować bezpieczeństwo w sieci poszukując materiałów

**BEZPIECZEŃSTWO TWOICH URZĄDZEŃ**

* Zablokuj urządzenia, wybierz preferowany sposób ich odblokowania (odcisk palca, hasło, kod PIN, itp.);
* Użyj silnego hasła - hasło powinno mieć co najmniej 12 znaków i być unikalne. Jednym z najłatwiejszych sposobów na zapamiętanie długiego i złożonego hasła bez konieczności zapisania go w dowolnym miejscu jest uczynienie z niego zdania, najlepiej, jeśli jest ono zapisane w lokalnym dialekcie!
* Dowiedz się, jak korzystać z ustawień prywatności w swoich urządzeniach.

**BEZPIECZEŃSTWO APLIKACJI, TABLETU / SMARTFONU**

* Sprawdź uprawnienia wymagane przez aplikację przed pobraniem ich (np. pozwolenie na dostęp do Twoich list kontaktów lub zdjęć);
* Nie podawaj żadnych danych osobowych chyba, że witryna lub aplikacja jest uprawniona do żądania ich (np. krajowe i oficjalne instytucje opieki zdrowotnej i powiązane aplikacje);
* Nie odpowiadaj na żadne wiadomości, które informują, że Twoje urządzenie ma wirusa, nawet jeśli mówią, że są to Microsoft, Apple, Android, itp.;
* Nie otwieraj automatycznie linków w wiadomościach e-mail, szczególnie jeśli brzmią one niepokojąco, np.,,Wygrałeś na loterii”, ,,Wygrałeś smartfona” lub ,,Twoje konto bankowe zostało naruszone”. Zazwyczaj te alarmujące wiadomości e-mail są wykorzystywane przez cyberprzestępców do popełniania oszustw i kradzieży danych.

**BEZPIECZEŃSTWO W MEDIACH SPOŁECZNYCH**

* + Dowiedz się, jak korzystać z uprawnień prywatności dowolnych używanych mediów społecznościowych.
  + Nie udostępniaj zdjęć dzieci (np. siostrzeńców i siostrzenic) lub osób niepełnoletnich (np. uczniowie, grupa wolontariuszy) bez zgody rodziców.
  + Nie udostępniaj żadnych wrażliwych danych.
  + Po opublikowaniu czegoś w Internecie, te materiały mogą zostać pobrane lub przekazane innym osobom. Zawsze miej to na uwadze przed udostępnieniem czegokolwiek!
  + Zastanów się przed opublikowaniem: prowokujących postów, obelg, wulgarnych treści lub intymnych szczegółów (np. dotyczące hospitalizacji), które mogą później narazić Ciebie na problemy (np. zwolnienie z pracy po rasistowskim lub homofonicznym wpisie).
  + Pamiętaj o fałszywych wiadomościach: przed udostępnieniem czegoś, co znalazłeś w Internecie, zawsze pamiętaj o sprawdzeniu źródła (np. strona internetowa z błędną nazwą renomowanych mediów społecznościowych zwykle udostępnia fałszywe wiadomości). Nie wszystko, co znajdujesz w Internecie musi być prawdziwe.
  + Uważaj na mowę nienawiści: naucz się ją rozpoznawać i unikaj stosowania jej. Dowiedz się także, jak zgłosić obraźliwy post lub komentarz, a także jak zablokować użytkownika, który posługuje się wobec Ciebie mową nienawiści (np. za pośrednictwem prywatnych wiadomości, publicznych komentarzy, itp.).
  + Bądź miły/miła dla innych osób. Możesz nie zgadzać się z opinią innych osób i wyrazić ją bez obrażania ich.
  + Jeżeli chcesz spotkać się w prawdziwym życiu z kimś, kogo poznałeś online, zrób to w miejscu publicznym lub idź z przyjacielem. Ludzie mogą kłamać na temat swojej tożsamości.

**BEZPIECZEŃSTWO ZAKUPÓW, BANKOWOŚCI I DAROWIZN ONLINE**

* + Kupuj tylko na renomowanych stronach internetowych. Jeśli ich nie znasz, możesz poszukać informacji lub popytać.
  + Używaj tylko kart kredytowych lub debetowych, nie wysyłaj pieniędzy ani gotówki.
  + Przed przekazaniem darowizny na cele charytatywne, sprawdź czy są one zgodne z prawem.
  + Nie udostępniaj konta bankowego oraz hasła.

Materiał ten związany jest z projektem Elily, który partnerzy opracowali wspólnie lub indywidualnie, w jakiejkolwiek formie i przy użyciu jakichkolwiek środków, odzwierciedla jedynie opinię autora, a Agencja Krajowa i Komisja Europejska nie są odpowiedzialne za jakiekolwiek wykorzystanie zawartych w nim informacji.