# Nowe technologie a prywatność.

# O czym warto pamiętać

# nie tylko w Dniu Bezpiecznego Internetu.

**Nowe technologie są wszędzie i są niezbędne w dzisiejszym świecie. Należy jednak pamiętać, że niosą za sobą nie tylko szansę rozwoju i inne pozytywne aspekty, takie jak np. dostęp do źródeł wiedzy, rozrywki czy komunikacji społecznej w czasie rzeczywistym, ale również wiele zagrożeń.**

Przede wszystkim niezwykle istotna jest tutaj wysoka świadomość każdego użytkownika Internetu i urządzeń podłączonych do globalnej sieci (np. smartphonów), która pozwoli zminimalizować ryzyko niesione przez nieumiejętnie używaną technologię. Wystarczy przestrzegać kilku podstawowych zasad, aby zwiększyć swoje bezpieczeństwo i zyskać większą kontrolę nad własnymi danymi osobowymi w Internecie. Dlatego w Dniu Bezpiecznego Internetu warto przypomnieć kilka najważniejszych kwestii.

**Człowiek - najsłabsze ogniwo niemal każdego systemu bezpieczeństwa**

Należy poznać współczesne zagrożenia, aby świadomie i bezpiecznie korzystać z sieci.

Na plan pierwszy wysuwają się ataki socjotechniczne, których w ostatnim czasie przybywa lawinowo, a oszuści, którzy korzystają z tych metod są coraz bardziej kreatywni w swoich działaniach. Polegają one na manipulowaniu i nakłonieniu użytkownika systemu do nadmiernego udostępniania danych osobowych.

Aby dane osobowe nie stały się łatwym łupem przestępców, wystarczy przestrzegać kilku podstawowych zasad postępowania z informacjami udostępnianymi w sieci, np. w mediach społecznościowych. Jako przykład niech posłużą dobre praktyki zebrane w ramach cyklu „Warto wiedzieć…", który UODO realizuje w programie edukacyjnym „Twoje dane - Twoja sprawa".

**Dobre praktyki, które powinny stać się nawykiem każdego internauty**

**1. Zadbaj o zróżnicowane i silne hasła logowania**. Hasło powinno być trudne do odgadnięcia i zawierać duże/małe litery, cyfry oraz znaki specjalne. Nie zaleca się zapamiętywania haseł w pamięci przeglądarki lub w aplikacji na urządzeniu. Nie należy także używać tej samej nazwy użytkownika w połączeniu z identycznym hasłem we wszystkich aplikacjach, z których korzystasz;

**2. Dopasuj ustawienia prywatności konta.** Ustaw je tak, aby dostęp do prywatnych informacji, danych osobowych, zdjęć, komentarzy miały jedynie zaufane osoby, będące w gronie Twoich znajomych. Rozważ także, czy Twój profil powinien być widoczny dla zewnętrznych wyszukiwarek;

**3. Uważaj, jakimi informacjami, ale też zdjęciami lub filmami, dzielisz się z innymi.** Przykładowo, publikowanie zdjęć, swoich i najbliższych, wystawione jest na ocenę

innych osób, a ewentualna ich reakcja i komentarze mogą okazać się raniące, dokuczliwe, a nawet wulgarne. Pamiętaj, że osoba której zdjęcia zamieszczasz – powinna być, co najmniej poinformowana o tym fakcie. Raz opublikowana informacja, treść bądź fotografia może pozostać w cyberprzestrzeni już na zawsze, a konsekwencje złych wyborów ciągnąć się latami;

**4. Nie ujawniaj zbyt wielu informacji o sobie.** Social media nie są odpowiednimi miejscami do dzielenia się danymi/informacjami takimi, jak adres zamieszkania, numer telefonu czy miejsce pracy rodziców. Uważaj na zamieszczenie zdjęć/nagrań pozwalających osobie nieznajomej zlokalizować miejsce Twojego pobytu. Nie zamieszczaj zdjęć np. legitymacji szkolnej, dowodu tożsamości, karty płatniczej, druków zawierających dane osobowe, kart pokładowych czy prawa jazdy. Należy mieć świadomość, że dane osobowe/kontaktowe mogą pozyskać przestępcy, którzy zechcą wykorzystać je przeciwko Tobie lub Twoim najbliższym;

**5. Uważaj na zaproszenia od nieznanych użytkowników.** Bądź ostrożny i nie akceptuj automatycznie zaproszeń do grona znajomych lub obserwowania od obcych osób. Osoba podająca się za Twojego rówieśnika, może okazać się w rzeczywistości zupełnie kimś innym, dlatego należy być ostrożnym przy zawieraniu nowych znajomości w sieci. Pamiętaj też, że ktoś obcy może się podszyć także za Twojego bliskiego, przejmując wcześniej jego tożsamość w sieci;

**6. Uważaj na tzw. phishing**. Jest to jedno z najbardziej niebezpiecznych działań zmierzających do kradzieży loginów i haseł, które dotyczy również portali społecznościowych. Hakerzy rozsyłają odsyłacze do fałszywych serwisów społecznościowych, do złudzenia przypominających te, z których korzystasz na co dzień. Po kliknięciu w taki link i wprowadzeniu danych do logowania cyberprzestępcy mogą uzyskać dostęp do Twoich danych;

**7. Uważaj na szkodliwe oprogramowanie, które może być przesyłane za pomocą komunikatorów**. Zachowaj czujność zanim otworzysz otrzymany link, upewniając się, że pochodzi z zaufanego źródła. Hakerzy, wykorzystując nieuwagę użytkownika, rozsyłają linki do zainfekowanych stron lub dodają złośliwe rozszerzenia do przeglądarek, dzięki czemu mogą przejąć kontrolę nad kontem użytkownika;

**8. Uważaj na publiczne lub niezabezpieczone połączenia internetowe.** Nie loguj się do serwisów społecznościowych podczas korzystania z otwartych sieci, gdyż może to grozić udostępnieniem wrażliwych informacji cyberprzestępcom.

https://uodo.gov.pl/pl/138/2300