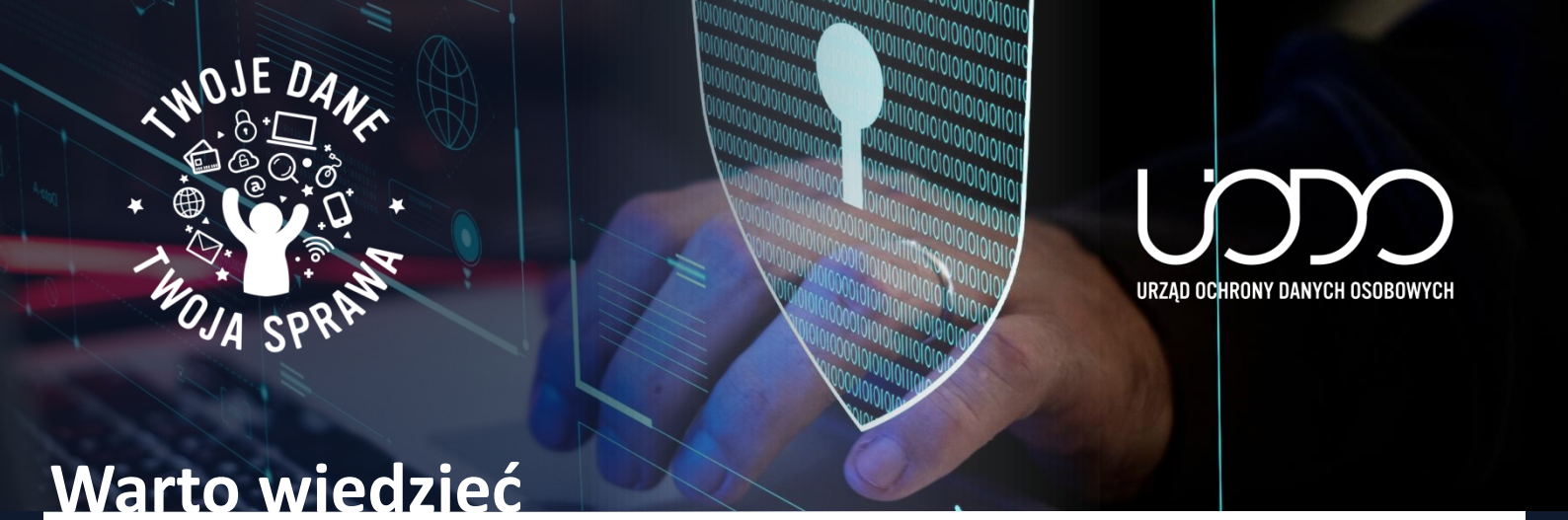

Warto wiedzieć

Portale społecznościowe – 8 wskazówek pozwalających chronić prywatność

Portale społecznościowe (w tym wbudowane w nie komunikatory) stanowią stały element codzienności wielu z nas, a już ponad wszelką wątpliwość – uczniów. Granica wieku, od którego można korzystać z usług społeczeństwa informacyjnego wynosi 16 lat, natomiast przed ukończeniem tego wieku, dzieci mogą posługiwać się nimi za zgodą rodziców. Korzystanie z serwisów społecznościowych może sprawić wiele radości, ale też wiązać się z zagrożeniami dla naszej prywatności i ochrony danych osobowych.

Pamiętajmy, że dane osobowe udostępniane w social mediach to nie tylko imię, nazwisko, ale również szeroki zakres danych, takich jak: nazwa szkoły, nick, czy geolokalizacja naszych urządzeń mobilnych zapisywana na przykład w metadanych zdjęć (obok innych ważnych danych, jak data i czas ich wykonania). Danymi osobowymi może być także nasza aktywność w mediach: polubienia i komentarze pod konkretnymi postami, ale do szczególnej kategorii danych osobowych należą informacje o naszym zdrowiu, wyznaniu czy poglądach politycznych.

Świadomość ryzyka daje możliwość ochrony przed ewentualnymi zagrożeniami. Dlatego, korzystając z tego typu portali, warto pamiętać o kilku istotnych wskazówkach:

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.