1. STOSUJ MĄDRE HASŁA

Mądre hasło jest trudne do odgadnięcia, ale łatwe do zapamiętania, jak np. pierwsze litery ulubionego cytatu, z dodatkowymi symbolami specjalnymi i cyframi.

Stosuj różne hasła dla ważnych miejsc i urządzeń (e-mail, komputer osobisty, telefon, najczęściej używany profil społecznościowy).

Nie zapominaj blokować telefonu, gdy go zostawiasz!

2. USTAW PRYWATNOŚĆ PROFILU

Czy wszyscy znajomi powinni widzieć wszystkie Twoje zdjęcia i inne informacje? W ustawieniach profilu na portalu społecznościowym zablokuj widoczność wszystkiego co publikujesz i innych Twoich danych dla osób spoza listy znajomych.

Sprawdź, komu domyślnie pokazujesz publikowane przez siebie treści i zdjęcia. Stwórz grupy wśród znajomych np. bliższa rodzina, przyjaciele – i tylko tym osobom udostępniaj osobiste zdjęcia i swoje opinie.

3. CHROŃ WAŻNE DANE

Nie umieszczaj swojego adresu e-mail, numeru telefonu, adresu ani żadnych innych Twoich danych osobistych w miejscach, gdzie inni internauci mogliby je zobaczyć. Jeśli chcesz aby inni mogli się z Tobą skontaktować na blogu lub innej stronie www, dodaj specjalny widżet kontaktowy, który w bezpieczny sposób pozwoli wysłać do Ciebie wiadomość. Nie przechowuj wrażliwych danych (skan paszportu itp.) w chmurze, chyba że w archiwum chronionym silnym hasłem!

Pamiętajmy, nie mamy nigdy pewności kto czyta to, co wysyłasz przez internet. Nie wysyłaj zdjęć, filmów ani treści, które mogą skompromitować Ciebie lub inne osoby – dobrą zasadą jest nie wysyłać niczego, co wstydzilibyśmy się pokazać tacie, babci czy nauczycielowi.

Regularnie aktualizuj system, aplikacje oraz odinstalowuj aplikacje i rozszerzenia przeglądarki, z których nie korzystasz.

4. NIE WIERZ WSZYSTKIEMU

Uważaj na wiadomości i informacje wyświetlane w internecie, które obiecują szybkie zrealizowanie marzeń. Ich celem jest zachęcenie do kliknięcia, tymczasem konsekwencje mogą być poważne.

Nie klikajmy w linki, o które nie prosiliśmy. Nawet jeśli znajomy podsyła nam linka, lepiej dowiedzieć się co to - przed kliknięciem.

Otwierając strony sprawdzaj, czy ich adres zaczyna się od: HTTPS a zamknięta (zielona) kłódka wyświetla się obok adresu. Jeśli kłódka jest otwarta lub czerwona, nie wprowadzaj żadnych swoich danych (np. adres e-mail!) na takiej stronie!

5. WYŁĄCZ ŚLEDZENIE

Kontroluj, które aplikacje używają GPS w urządzeniu mobilnym. Pamiętaj, że przy robieniu zdjęć Twoja lokalizacja może być dodawana do nich automatycznie. Jeśli niepowołane osoby otrzymają do nich dostęp, zwiększa to ryzyko np. włamania do mieszkania podczas wyjazdu.

Wyłącz personalizowane reklamy w przeglądarkach internetowych, aby nie ułatwiać roboty naciągaczom.

Wyłącz pokazywanie treści wiadomości na zablokowanym ekranie smartfona, aby przypadkowe osoby ich nie podejrzały.

Ostrożnie korzystaj z publicznych sieci Wi-Fi - nie wysyłaj wrażliwych danych, bez szyfrowanego połączenia (VPN).