BEZPIECZEŃSTWO

1. **Bezpieczna transmisja bezprzewodowa**
   Transmisja danych z wykorzystaniem sieci bezprzewodowej WiFi, może ale nie musi wiązać się z ryzykiem, że nasze przesyłane dane zostaną podsłuchane i wykorzystane, bądź ktoś niepożądany wykorzysta możliwość podłączenia się do naszego routera czy też access point'a. Aby tego uniknąć zastosuj się do poniższych rad.

   - Jeżeli jest taka możliwość wyłącz rozgłaszanie nazwy swojej sieci radiowej tzw. BSSID. Twoja sieć przestanie być widoczna dla innych użytkowników, a znając jej nazwę będziesz mógł się do niej podłączyć. Wydłuży to trochę proces konfiguracji podłączenia do sieci, ale dzięki temu unikniesz prób podłączenia się do niej przez osoby postronne
   - Używaj szyfrowania w połączeniach z siecią WiFi. Na swoim urządzeniu ustaw szyfrowanie z wykorzystaniem autoryzacji WPA/PSK lub WPA2/PSK. Unikaj autoryzacji WEP.
   - Zastosuj na urządzeniu zasady dostępu, znając swoje urządzenia wiesz jakie mają mac addressy (adresy fizyczne) kart bezprzewodowych. Pozwól tylko tym urządzeniom na podłączanie się do Twojej sieci
   - zabezpiecz konto administratora swoim hasłem, po prostu zmień hasło domyślne ustawiane przez producenta
   - ogranicz możliwość zarządzania urządzeniem od strony Internetu lub ją wyłącz

2. **Bezpieczny komputer**

   - Zabezpiecz swój komputer hasłem, najlepiej stwórz osobne konto z którego będziesz korzystał na co dzień. Ogranicz prawa tego konta tak, aby z jego poziomu nie można było wprowadzać zmian w plikach bądź ustawieniach systemowych
   - Korzystaj zawsze z legalnego oprogramowania. Programy ściągnięte z Internetu mogą zawierać wirusy, konie trojańskie bądź inne złośliwe oprogramowanie pozwalające przejąć kontrole nad Twoim komputerem
   - Zadbaj aby na Twoim komputerze znalazło się oprogramowanie antywirusowe, uaktualniaj sygnatury bazy wirusów. Wybierz ten program, który w tle potrafi sprawdzić każdy pobrany plik, zintegruje się z programem do odbioru poczty
   - Ogranicz zaufanie do tego co pobierasz z Internetu, zastanów się czy źródło pochodzenia jest sprawdzone
   - Pamiętaj, że programy P2P (Torrent,E-mule, Kazaa) służą do wymiany plików, to że Ty możesz ściągać pliki powoduje to, że sam te pliki udostępniasz. Może to być niezgodne z prawem. Plik taki może również zawierać złośliwe oprogramowanie

3. **Bezpieczna poczta i strony WWW**

   - Zawsze korzystaj z najbardziej aktualnych przeglądarek stron WWW i programów do korzystania z poczty e-mail
   - Dbaj o swoją prywatność, czyść pamięć tymczasową przeglądarki stron WWW
   - Zanim podasz swoje dane osobowe sprawdź w jakim celu będą one wykorzystywane
   - Zanim zgodzisz się na zainstalowanie dodatku do przeglądarki dokładnie zapoznaj się z tym do czego ten dodatek służy, do czego będzie mieć dostęp
   - Nie otwieraj wiadomości e-mail od nieznanych nadawców a szczególnie załączników zawartych do tych wiadomości, mogą zawierać szkodliwe oprogramowanie
   - Nie udostępniaj powszechnie swojego adresu e-mail, może on zostać wykorzystany do rozsyłania niechcianych wiadomości (SPAM)
   - Jeżeli już musisz wysłać wiadomość do wielu odbiorców, korzystaj z opcji BCC/UDW, spowoduje to, że nie będziesz udostępniać adresów e-mail innych osób

4. **Bezpieczne dziecko**

   - Rozmawiaj z dzieckiem o tym, co robiło w Internecie
   - Postaraj się, aby mieć dostęp do konta Twojego dziecka na komputerze
   - Sprawdzaj co dziecko robiło na portalach, z kim rozmawiało poprzez komunikatory, wyjaśnij dziecku, że nie zawsze osoby z którymi rozmawia są tymi za które się podają
   - Zastosuj ochronę rodzicielską, zastosuje filtry treści aby ograniczyć dostęp do treści, których Twoje dziecko nie powinno czytać lub oglądać

5. **Bezpieczne hasło**

   - Postaraj się aby hasło, którym zabezpieczasz swój komputer, dane lub sieć WiFi miało przynajmniej 8 znaków
   - Dobre hasło składa się z liter [a-z A-Z] i cyfr [0-9], stosuje znaki specjalne #$%!.,
   - Staraj się zmieniać hasło przynajmniej raz na 3 miesiące
   - Nie udostępniaj haseł innym osobom
   - Nie zapisuj hasła na kartce