Najważniejsze rady dotyczące cyberbezpieczeństwa w domu

Internet rzeczy (IoT) to sieć wszystkich urządzeń, które można podłączyć do internetu. W pierwszej chwili może Ci przyjść na myśl Twój laptop lub telewizja hybrydowa, ale internet rzeczy obejmuje również takie urządzenia, jak konsole do gier, inne urządzenia domowe, alarm lub nianię elektroniczną.

Urządzenia te mogą usprawnić nasze życie i pracę, pamiętaj jednak, że wszystko, co jest podłączone do internetu, może być narażone na ataki cyberprzestępców. Oto kilka kroków, dzięki którym możesz ochronić swój dom.

1. Zabezpiecz wszystkie urządzenia

Należy zadbać o to, by wszystkie urządzenia były chronione silnymi hasłami lub wprowadzić uwierzytelnianie dwuskładnikowe (2FA), które jest dostępne w przypadku większości urządzeń będących częścią internetu rzeczy.

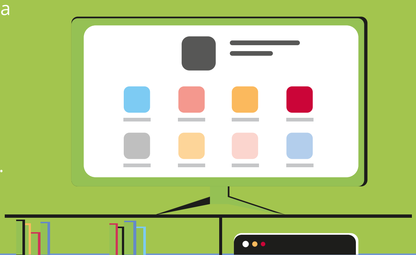
Zmień również hasło domyślne i nazwę domowej sieci bezprzewodowej. Pamiętaj, aby nie umieszczać w nazwie sieci żadnych informacji dotyczących Twojego domu lub rodziny, np. swojego nazwiska lub adresu.

2. Sprawdź swoje aplikacje

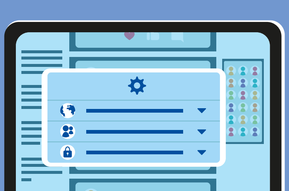
Pobieranie aplikacji bezpośrednio z oficjalnego sklepu aplikacji (Google Play, Apple App Store itp.) to najbezpieczniejszy sposób ich pozyskania. Kliknięcie na przypadkowe łącze, aby pobrać aplikację, może prowadzić do zainfekowania Twojego urządzenia.

Zastanów się dobrze, jakich informacji i pozwoleń udzielasz przed instalacją.

Regularnie przeglądaj aplikacje i usuwaj to, co zbędne.



3. Zapoznaj się z ustawieniami prywatności na swoich kontach w mediach społecznościowych



Przejdź do ustawień prywatności Twojego konta i wybierz ustawienia, które Ci odpowiadają.

Zastanów się dobrze, jakie informacje należy uwzględnić w Twoim profilu. Platformy mogą prosić o informacje, których nie musisz podawać.

4. Ustaw automatyczne aktualizacje na wszystkich urządzeniach i twórz zapasowe kopie danych

Urządzenia internetu rzeczy są narażone na ataki cyberprzestępców, dlatego najnowsze aktualizacje są niezbędne do zapewnienia bezpieczeństwa tych urządzeń.

Ustawienie automatycznych aktualizacji oznacza, że nie trzeba będzie pamiętać, aby robić to samodzielnie. Upewnij się, że posiadasz kopie ważnych informacji, które przechowujesz poza internetem lub w chmurze, np. zdjęcia lub kontakty.

5. Rozdziel urządzenia służbowe i prywatne

Sugerujemy używanie osobnych urządzeń do pracy i spraw prywatnych. Urządzenie używane do pracy powinno być używane wyłącznie do celów zawodowych, co pomoże zminimalizować straty w razie włamania do urządzenia.

Jeśli musisz korzystać ze wspólnego urządzenia, upewnij się, że każdy użytkownik posiada odrębny profil użytkownika.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

#CyberSecMonth

#ThinkB4UClick