Warto wiedzieć

Użytkowanie Smarfona a ochrona naszej prywatności

Smartfon to przenośne urządzenie multimedialne łączące w sobie funkcje telefonu komórkowego i komputera przenośnego. Jest to często najbardziej osobiste urządzenie elektroniczne, którego używamy. Zabieramy go do szkoły, do pracy, na spotkania, a nawet jest tuż obok, gdy idziemy spać. Wykorzystując jego możliwości, używamy wielu aplikacji (akceptując przy tym regulaminy), przeglądamy Internet, wymieniamy wiadomości, korzystamy z serwisów społecznościowych, robimy zdjęcia, kręcimy filmiki, oraz pozwalamy na gromadzenie danych o naszym położeniu. Jednymi słowy, nasze urządzenie jest skarbnicą informacji o nas, naszych upodobaniach i stylu życia – „wie o nas" praktycznie wszystko.

Cyberprzestępcy dostrzegli ogrom możliwości, jakie dają smartfony, na nielegalne zdobycie naszych danych osobowych, poufnych informacji i innych ważnych treści, które przechowujemy w urządzeniach. Dlatego musimy być szczególnie czujni podczas używania swoich przenośnych urządzeń i jeszcze bardziej chronić własne dane osobowe, oraz szeroko pojętą prywatność.

Dlatego warto wiedzieć, jak chronić dane…

- **Blokuj ekran**. Ustawienie automatycznej blokady urządzenia i konieczność jego odblokowania za pomocą kodu PIN lub wzoru, ograniczy ryzyko dostępu do naszej prywatnej przestrzeni i możliwość kradzieży danych;
- **Systematycznie aktualizuj oprogramowanie urządzenia oraz korzystaj ze sprawdzonego programu antywirusowego.** Regularne skanowanie smartfona może wykryć zainfekowane pliki czy też niebezpieczne aplikacje;
- **Sprawdzaj uprawnienia aplikacji**. Przemyśl czy określona aplikacja powinna mieć dostęp, do zasobów takich jak galeria, kontakty, geolokalizacja, wiadomości, ale też czy godzisz się na dostęp do kamery i mikrofonu. Rozważ, czy ewentualny dostęp do zasobów smartfona ma być stały czy jedynie na czas działania aplikacji;
- **Zastosuj tryb prywatny**. Umożliwia on przeglądanie stron WWW bez zapisywania historii, plików cookie i wyszukiwanych fraz. Pamiętaj, że nie gwarantuje on pełnej anonimowości w sieci, ale pozwala na zwiększenie poziomu prywatności;
- **Uważaj na ładowanie przez kabel USB.** Bądź ostrożny, podłączając smartfon do obcego komputera lub gniazdka USB – może być to niebezpieczne i narazić Cię na kradzież danych lub zainfekowanie urządzenia. Warto posiadać kabel, który pozwala wyłącznie na ładowanie urządzenia, ale nie na przesył danych;
- **Rozważnie korzystaj z publicznych sieci bezprzewodowych Wi-Fi.** Pamiętaj, że nazwa sieci Wi-Fi może być ustalona dowolnie i celowo wprowadzać w błąd, sugerując, że należy np. do Twojej szkoły, a tak naprawdę być siecią uruchomioną w celach przestępczych. Dlatego staraj się korzystać wyłącznie z serwisów oraz usług z zaszyfrowanym ruchem, np. w przeglądarce będą to połączenia zabezpieczone za pomocą protokołu HTTPS. Możesz też rozważyć wykorzystanie sprawdzonej aplikacji VPN;
- **Pomyśl nad kupnem folii prywatyzującej.** Naklejenie tego typu filtru na ekran, uniemożliwia osobom będącym w pobliżu podglądanie wyświetlanych w smartfonie treści. Oznacza to tyle, że osoba siedząca obok nas, np. w pociągu, w poczekalni, nie zobaczy co czytamy i jakie wykonujemy operacje na naszym urządzeniu;
- **Systematyczne czyść urządzenie**. Kasuj „śmieci systemowe" - aplikacje i dane, z których już nie korzystasz. Pamiętaj również o kasowaniu historii przeglądania i zamykaniu zbyt wielu otwartych wcześniej kart (w niektórych nadal możemy być zalogowani do stron WWW). Zwiększy to bezpieczeństwo, jak również szybkość działania urządzenia;
- **Pamiętaj o wylogowaniu się z serwisów WWW.** Spowoduje to przerwanie uwierzytelnionego połączenia ze stroną, a nawet usunięcie danych logowania, np. w postaci plików cookie, zmniejszając przy tym możliwość kradzieży Twojej tożsamości;
- **Bądź przezorny.** Zabezpiecz się na wypadek zagubienia/kradzieży smartfona. Warto włączyć usługi lokalizujące urządzenie oraz umożliwiające zdalne usunięcie danych czy też zresetowanie do fabrycznych ustawień;
- **Zadbaj o kopię zapasową.** Twórz regularnie lokalną kopię danych lub korzystaj z backupu w chmurze. Dzięki temu szybko odzyskasz dostęp do ważnych danych w przypadku awarii, zgubienia lub kradzieży telefonu;
- **Gdy chcesz sprzedać/oddać telefon zwróć szczególną uwagę, aby Twoje poufne dane nie dostały się w ręce obcej osoby, a zwłaszcza cyberprzestępców.** Oprócz procesu przywrócenia ustawień fabrycznych urządzenia, warto włączyć opcję szyfrowania danych, znajdującą się w ustawieniach prywatności.