

Jak bezpiecznie korzystać ze smartfona?

Przede wszystkim pamiętaj, że:

- w telefonie przechowujesz więcej wrażliwych danych, niż gdziekolwiek indziej!
- utrata dostępu do telefonu może „odciąć” Cię od wielu kluczowych aktywności
- konsekwencją przejęcia przez oszusta kontroli nad Twoim telefonem może być nie tylko utrata pieniędzy – również tożsamości, prywatności, poczucia bezpieczeństwa!

1. Wstępna konfiguracja telefonu

- zabezpiecz swoje konto Google/Apple trudnym do złamania hasłem
- włącz uwierzytelnianie dwuskładnikowe na koncie Google/Apple

2. Zabezpieczenia telefonu

- włącz w ustawieniach możliwość zdalnego odnalezienia/wyczyszczenia swojego urządzenia
- do odblokowania urządzenia używaj odcisku palca (Android) lub skanu twarzy (iPhone)
 - nie konfiguruj odcisków osób bliskich; jeśli będziesz potrzebować udostępnić komuś Twoje urządzenie, nie stracisz nad tym kontroli
 - blokada twarzą na Androidzie jest relatywnie bezpieczna wyłącznie w przypadku telefonów wykonujących skan 3D twarzy; jeśli chcesz z niej skorzystać, upewnij się, że Twoje urządzenie wykonuje skan 3D
- jako zapasową metodę odblokowania wybierz hasło składające się z liter i cyfr
 - jeśli decydujesz się na PIN, niech ma 6-8 cyfr i nie składa się z prostych kombinacji
 - nie używaj „szlaczka” – brudny ekran i tłusty palec powodują, że na ekranie widać ślad wzoru odblokowania
- wyrób w sobie nawyk blokowania telefonu pozostawianego bez opieki
- gdy z Twojego telefonu korzystają dzieci – załóż im oddzielne konto, z dostępem wyłącznie do używanych przez nie aplikacji
 - przełączanie między kontami jest proste i intuicyjne
- jeśli Twój telefon miał fabrycznie zainstalowanego Androida w wersji niższej lub 10 – w internecie znajdziesz informację jak włączyć szyfrowanie urządzenia (iOS i Android 10 i wyższy mają je włączone domyślnie); dzięki temu nawet gdy zgubisz urządzenie, dane nie trafią w obce ręce

3. Instalacja aplikacji

- instaluj wyłącznie aplikacje, których potrzebujesz; rób raz na jakiś czas „audyt” aplikacji i wyrzucaj niepotrzebne
- instaluj na telefonie oprogramowanie wyłącznie z oficjalnych sklepów (Sklep Play/App Store/Xiaomi AppMall)
- przy instalacji aplikacji sprawdzaj uprawnienia systemowe, których wymagają
 - w przypadku uprawnień wrażliwych (dostęp do sieci, rozmowy, SMS-y) – upewnij się, czy ta aplikacja musi mieć do nich dostęp
- zabezpiecz płatności systemowe odciskiem palca lub hasłem

4. Pozostałe

- pamiętaj o kopii bezpieczeństwa
 - przede wszystkim zdjęć, ale też np. archiwum komunikatorów oraz ustawień systemu operacyjnego
- nie odkładaj aktualizacji systemu operacyjnego – w znacznej większości przypadków wprowadzają one poprawki bezpieczeństwa
- jeśli korzystasz z karty microSD – miej świadomość, że dane, które na nią trafiają, są niezaszyfrowane
- transakcje finansowe wykonuj z poziomu aplikacji swojego banku – nie strony WWW
- korzystanie z NFC nie jest niebezpieczne, **skanowanie karty to miejska legenda**; kartę płatniczą włożoną między telefon i etui zeskanować dużo łatwiej
- jeśli sprzedajesz telefon – wyczyść dane/doprowadź go do ustawień fabrycznych



Orange
Polska

<https://cert.orange.pl>

https://twitter.com/cert_opl