20 Sposobów na blokowanie ataków mobilnych

Nie trać czujności tylko dlatego, że korzystasz z urządzenia mobilnego. Bądź tak samo ostrożny jak przy komputerze stacjonarnym!

WiFi

- Nie zezwalaj urządzeniu na automatyczne łączenie z nieznaną siecią.
- Zawsze wyłączaj WiFi gdy z niego nie korzystasz lub gdy go nie potrzebujesz.
- Nigdy nie wysyłaj poufnych informacji przez WiFi, chyba że masz całkowitą pewność, że jest to bezpieczna sieć.

Aplikacje

- Używaj wyłącznie aplikacji dostępnych w oficjalnym sklepie - NIGDY nie pobieraj ich z przeglądarki.
- Uważaj na aplikacje od nieznanych twórców oraz na te z małą liczbą lub złymi opiniami.
- Aktualizuj je, aby mieć pewność, że posiadają najnowsze zabezpieczenia.
- Jeżeli nie są już obsługiwane przez Twój sklep, po prostu je usuń!
- Nie nadawaj aplikacjom wysokich lub administracyjnych uprawnień, jeśli nie masz do nich pełnego zaufania.

Przeglądarka

- Uważaj na reklamy, promocje i konkursy, które wydają się zbyt piękne, by mogły być prawdziwe. Często prowadzą one do stron phishingowych, które wyglądają na legalne.
- Zwracaj szczególną uwagę na adresy URL. Są one trudniejsze do weryfikacji na ekranach telefonów komórkowych, ale efekt jest tego warty.
- Nigdy nie zapisuj danych logowania, gdy korzystasz z przeglądarki internetowej.

Bluetooth

- Wyłącz automatyczne parowanie poprzez Bluetooth.
- Wyłączaj go zawsze, gdy nie jest potrzebny.

Smishing (phishing za pomocą SMS-ów)

- Nie ufaj wiadomościom, które próbują nakłonić Cię do ujawnienia jakichkolwiek danych osobowych.
- Uważaj na podobne taktyki na platformach takich jak What's App, Facebook, Messenger, Instagram itp.
- Traktuj wiadomości w taki sam sposób, w jaki traktujesz email. Zawsze zastanów się, zanim klikniesz!

Vishing (phishing głosowy)

- Nie odpowiadaj na telefoniczne lub mailowe prośby o osobiste informacje finansowe. Jeżeli masz obawy, zadzwoń bezpośrednio do instytucji finansowej, korzystając z numeru telefonu podanego na odwrocie karty kredytowej lub na miesięcznym wyciągu z konta.
- Nigdy nie klikaj na link w niechcianej wiadomości reklamowej.
- Podawaj informacje o koncie wyłącznie podczas rozmowy z żywą osobą i tylko wtedy, gdy sam inicjujesz połączenie.
- Zainstaluj oprogramowanie, które informuje, czy jesteś na bezpiecznej lub fałszywej stronie internetowej.

Partner w Polsce: IMNS

KnowBe4
Human error. Conquered.