Warto wiedzieć…

Juice jacking, czyli wyciskanie danych z urządzeń

Uważaj na publiczne porty USB!

JUICE JACKING (ang. juice – potocznie to energia elektryczna, juice jacking - wyciskanie soku), to technika atakowania polegająca na włamaniu do urządzenia podczas jego ładowania w publicznym porcie USB, dostępnym w takich miejscach jak np. lotniska, restauracje, pociągi czy autobusy. Aby doszło do ataku, przestępca podmienia port ładowania w ładowarce publicznej na własny, w celu przejęcia kontroli nad ładowanym urządzeniem. Podmieniony port pozwala na uzyskanie dostępu do pamięci podłączonego urządzenia, a co za tym idzie kradzież danych lub wgranie złośliwego oprogramowania poprzez kabel zasilający. Narażone na tego typu ataki są przede wszystkim telefony, tablety i laptopy.

DO CZEGO MOGĄ UZYSKAĆ DOSTĘP PRZESTĘPCY POPRZEZ ATAK JUICE JACKING?

- Do hasła i loginu do aplikacji zawierających Twoje dane osobowe, takie jak nr PESEL, historia leczenia, numer telefonu czy adres e-mail;
- Do hasła logowania do aplikacji bankowych, co umożliwi przestępcy dostęp do konta bankowego;
- Do podłączonej karty płatniczej;
- Do lokalizacji, adresu IP czy tzw. plików cookies;
- Do loginu do aplikacji mObywatel.

JAK MOŻESZ OBRONIĆ SIĘ PRZED JUICE JAKCING?

Unikaj ładowania urządzeń mobilnych przez publiczne porty ładowania USB. Jeśli jednak musisz naładować urządzenie mobilne to:

- Korzystaj z własnego źródła ładowania, czyli powerbanków lub ładowarek, które możesz bezpośrednio podłączyć do gniazdka elektrycznego;
- Korzystaj z kabli służących tylko do ładowania (only charge);
- Regularnie aktualizuj aplikacje i oprogramowanie systemowe urządzeń;
- Włącz w ustawieniach swojego telefonu opcję potwierdzenia, że podłączone urządzenie jest zaufane (po podłączeniu nieznanego urządzenia pojawi się np. komunikat "Ufasz temu komputerowi?");
- Włącz w ustawieniach telefonu opcję informowania o próbie transmisji danych przez kabel USB;
- Nie klikaj w linki wysłane z nieznanych adresów.

PAMIĘTAJ

Efektem ataku juice jacking jest przejęcie kontroli nad Twoim urządzeniem, w którym znajduje się mnóstwo danych osobowych. Zadbaj o siebie i swoje bezpieczeństwo.

URZĄD OCHRONY DANYCH OSOBOWYCH