PUBLICZNE ŁADOWANIE TELEFONU – RYZYKO CZY WYGODA?

Posted on 2024-02-29

W dzisiejszym świecie, gdzie nasze życie zawodowe i prywatne jest ściśle związane z urządzeniami elektronicznymi, korzystanie z publicznych portów USB może prowadzić do niebezpiecznych konsekwencji. Ładowanie telefonu czy tabletu, choć wydaje się być niegroźnym działaniem, może zostać wykorzystanie przez cyberprzestępców do ingerencji w system operacyjny urządzenia. Jednym z takich zagrożeń jest tzw. „juice jacking", który w ostatnich latach stał się coraz bardziej rozpowszechniony.

Czym jest „juice jacking"?

Juice jacking to szczególnie podstępny atak wykorzystujący naturalną potrzebę ładowania urządzenia poprzez podłączenie do publicznego, zewnętrznego źródła zasilania. Realizowany jest w taki sposób, że osoby atakujące modyfikują fabryczne ładowarki USB poprzez zainstalowanie dodatkowego modułu sprzętowego, co może doprowadzić do kradzieży danych lub zainstalowania złośliwego oprogramowania na urządzeniu użytkownika.

Zagrożenia związane z juice jackingiem

PUBLICZNE ŁADOWANIE TELEFONU – RYZYKO CZY WYGODA?

Publiczne porty USB, znajdujące się na lotniskach, w centrach handlowych, hotelach, kawiarniach czy w środkach transportu publicznego, mogą stać się miejscami potencjalnych ataków na nasze urządzenia. Oto kilka zagrożeń:

• Kradzież danych: Atakujący mogą wykorzystać juice jacking do kradzieży danych przechowywanych na urządzeniu, takich jak kontakty, pliki, hasła itp.

• Zainstalowanie złośliwego oprogramowania: Poprzez zainfekowanie urządzenia złośliwym oprogramowaniem, atakujący mogą uzyskać zdalny dostęp do urządzenia lub zgromadzić poufne informacje.

• Ransomware: Atakujący mogą zainstalować ransomware na urządzeniu, co prowadzi do zablokowania dostępu do danych na urządzeniu i żądania okupu za ich odblokowanie.

• Podsłuchiwanie aktywności: Atakujący mogą wykorzystać juice jacking do podsłuchiwania aktywności użytkownika na zainfekowanym urządzeniu, co może prowadzić do kradzieży poufnych informacji.

Istnieją jednak sposoby ochrony przed takim atakiem, które mogą pomóc użytkownikom zminimalizować ryzyko kradzieży danych podczas ładowania urządzeń mobilnych.

Dzięki odpowiednim środkom ostrożności można zabezpieczyć się przed tego rodzaju zagrożeniami.

Co zatem należałoby zrobić, żeby nie paść ofiarą juice jackingu?

1.Przede wszystkim staraj się unikać korzystania z publicznych portów USB do ładowania urządzeń.

2.W razie konieczności korzystania z publicznych portów USB, należy pamiętać, żeby upewnić się, że nie mamy uruchomionego trybu „debugowanie USB”, gdyż może to stanowić potencjalne zagrożenie dla bezpieczeństwa danych, ponieważ umożliwia dostęp do

zaawansowanych funkcji urządzenia. Dlatego zaleca się wyłączenie tej opcji, co pozwoli na zminimalizowanie ryzyka nieautoryzowanego dostępu do urządzenia.

3. Alternatywnie, można korzystać z zewnętrznych baterii przenośnych do ładowania urządzeń lub kabli „only charge", które są przeznaczone wyłącznie do ładowania urządzenia i uniemożliwiają przesyłanie danych.

4.Zaleca się również regularnie sprawdzanie i instalowanie dostępnych aktualizacji systemu operacyjnego, aby zapewnić ochronę przed różnymi rodzajami ataków oraz utrzymać urządzenie w jak najbezpieczniejszym stanie.

5.Warto również zadbać o wyłączenie funkcji udostępniania danych na urządzeniu, gdy korzystamy z publicznych portów USB, aby ograniczyć ryzyko kradzieży danych. Ta prosta czynność może stanowić dodatkową warstwę ochrony dla użytkowników, którzy nie posiadają baterii przenośnych.

6.Ochronę urządzeń przed wirusami lub nieautoryzowanym pobraniem danych może zapewnić również tzw. bloker danych USB. Może być skuteczną formą ochrony nie tylko w przypadku juice jacking, ale również ataków typu badUSB (np. przy wykorzystaniu specjalnie spreparowanych pendrive'ów), zapobiegając podłączeniu zainfekowanego urządzenia do komputera, ograniczając w ten sposób ryzyko zainfekowania.

Publiczne porty USB mogą stanowić poważne zagrożenie dla bezpieczeństwa naszych danych i urządzeń, jednak świadomość tych zagrożeń oraz stosowanie odpowiednich środków ostrożności, takich jak unikanie publicznych portów USB i korzystanie z zabezpieczeń fizycznych, jest kluczowe dla ochrony naszych danych.