Bitdefender

Jakie zagrożenia stoją przed użytkownikami iPhonów w 2024 roku?

18.09.2023

Apple iOS, jak każdy inny system operacyjny, narażony jest na różne zagrożenia bezpieczeństwa – między innymi ukierunkowane ataki złośliwego oprogramowania i oszustwa wykorzystujące inżynierię społeczną. Chociaż system iOS jest ogólnie uważany za bezpieczny, świadomość użytkowników i odpowiedzialne zarządzanie urządzeniami są niezbędne do utrzymania ścisłego bezpieczeństwa. Dlatego zespół Bitdefender przygotował podsumowanie kluczowych zagrożeń, z którymi mogą borykać się właściciele iPhonów w 2024 roku.

Zagrożenia dla iPhonów – inżynieria społeczna (phishing)

Cyberprzestępcy mogą wykorzystywać techniki znane z inżynierii społecznej, aby manipulować użytkownikami iOS w celu ujawnienia danych osobowych lub podjęcia działań zagrażających ich bezpieczeństwu. Phishing jest zdecydowanie najpowszechniejszą z nich.

Niezależnie od tego, czy atak dotyczy wiadomości e-mail, czy wiadomości SMS (smishing), użytkownicy systemu iOS mogą zostać oszukani w celu ujawnienia poufnych informacji, takich jak dane logowania lub dane karty kredytowej.

„Oprócz zachowania świadomości i właściwej higieny cyberbezpieczeństwa użytkownicy iPhonów mogą skorzystać z dedykowanego rozwiązania zabezpieczającego, które pomoże ograniczyć to ryzyko. Skuteczny system antywirusowy wyposażony w moduł antyphishingowy automatycznie skanuje przychodzące SMS-y i zaproszenia z kalendarza w poszukiwaniu oszustw wykorzystujących inżynierię społeczną i złośliwych linków" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Złośliwe aplikacje

Chociaż Apple stosuje rygorystyczny proces sprawdzania aplikacji, w App Store nadal mogą pojawiać się podejrzane aplikacje. Użytkownicy powinni dokładnie sprawdzić każdą nową aplikację, którą zamierzają zainstalować, zwłaszcza pod kątem praktyk gromadzenia danych i uprawnień na urządzeniu. Ogólnie rzecz biorąc, najbezpieczniejszym miejscem do pobierania aplikacji na iOS pozostaje Apple App Store. Chociaż mówi się o tym, że organy regulacyjne mają zamiar zmusić Apple, aby firma umożliwiła sideloading na iOS.

Jailbreaking

Jailbreaking nie jest już tak popularny jak kiedyś. Jednak niektórzy użytkownicy nadal hakują swojego iPhone'a, aby uzyskać większą kontrolę lub dodać dodatkową funkcjonalność. Praktyka ta może jednak osłabić bezpieczeństwo iPhone'a, ponieważ omija wewnętrzne mechanizmy bezpieczeństwa iOS i umożliwia instalację oprogramowania z nieoficjalnych źródeł.

Niebezpieczne sieci Wi-Fi

Niezależnie od dostawcy telefonu i systemu operacyjnego smartfony są z natury podatne na niezabezpieczone połączenia internetowe. Hakerzy mogą tworzyć fałszywe sieci w celu przechwytywania danych, co może prowadzić do kradzieży danych lub podsłuchiwania. Do niezabezpieczonej sieci publicznej można również włamać się w celu przeprowadzenia ataku typu „man-in-the-middle” i zebrania poufnych danych podczas przesyłania. Dlatego, jeśli już musisz skorzystać z publicznej sieci Wi-Fi, to powstrzymaj się przed wprowadzaniem wrażliwych danych do Twojego smartfona. Warto także rozważyć korzystanie z prywatnej sieci VPN.

Programy szpiegujące

Brak regularnej aktualizacji systemu iOS może narazić urządzenia na luki w zabezpieczeniach. W ciągu ostatnich kilku lat operatorzy oprogramowania szpiegującego w pełni wykorzystywali niezałatane błędy, aby instalować złośliwe oprogramowanie na iPhonach niczego niepodejrzewających ofiar. Instalowanie aktualizacji udostępnianych przez firmę Apple jest niezwykle istotne — zwłaszcza aktualizacje

pozapasmowe/backportowane/szybkie reagowanie na zagrożenia, które prawie zawsze mają na celu załatanie luk wykorzystywanych przez atakujących.

Prywatność

Apple skupia się na ciągłym zwiększaniu prywatności użytkowników, jednak nadal pozostawiają pole dla cyberprzestępców. System iOS 17 zapewnia jeszcze więcej ulepszeń w zakresie prywatności danych, ale użytkownicy iPhonów powinni przejrzeć oraz dostosować ustawienia do własnych potrzeb i preferencji w zakresie prywatności, oraz ograniczyć udostępnianie danych aplikacjom, witrynom internetowym, reklamodawcom itp.

Kradzież fizyczna

Jeśli Twój iPhone nie jest chroniony hasłem lub uwierzytelnianiem biometrycznym, złodziej może uzyskać dostęp do przechowywanych na nim danych osobowych. Używaj silnych haseł, Touch ID lub Face ID, aby zabezpieczyć urządzenie i włącz funkcję Znajdź mój iPhone, aby pomóc zlokalizować lub zdalnie wyczyścić dane w przypadku kradzieży.

Aby ograniczyć ryzyko kradzieży danych w 2024 roku:

- Regularnie aktualizuj system iOS i aplikacje.
- Uważaj na oszustwa wykorzystujące inżynierię społeczną (np. phishing i smishing).
- Pobieraj aplikacje wyłącznie z oficjalnego sklepu App Store.

- Podczas łączenia się z publicznymi sieciami Wi-Fi korzystaj z VPN.
- Unikaj jailbreakowania urządzenia, jeśli nie jesteś w pełni świadomy zagrożeń, które za sobą niesie ta praktyka.
- Używaj silnych haseł, Touch ID lub Face ID, aby zabezpieczyć urządzenie.
- Włącz funkcję Znajdź mój iPhone, aby pomóc zlokalizować i zdalnie wyczyścić urządzenie w przypadku kradzieży.
- Regularnie przeglądaj i dostosowuj ustawienia prywatności.
-Zachowaj ostrożność podczas klikania łączy lub podawania danych osobowych w Internecie.
- Korzystaj z dedykowanego rozwiązania zabezpieczającego, aby chronić się przed złośliwym oprogramowaniem, oszustwami i innymi zagrożeniami cybernetycznymi.

Źródło:https://bitdefender.pl/jakie-zagrozenia-stoja-przed-uzytkownikami-iphonow-w-2024-roku/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 18.09.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych

nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.