Bitdefender

10 największych zagrożeń dla Twojego smartfona

31.10.2023

Smartfony stają się coraz ważniejszymi narzędziami, których używamy w codziennym życiu do pracy, kontaktu z rodziną i przyjaciółmi oraz wykonywania różnych innych czynności, w tym bankowości, robienia zakupów czy uczenia się nowych umiejętności. Są jednak również bardzo dochodowym celem dla cyberprzestępców, którzy chcą zdobyć ogromne ilości informacji przechowywanych na naszych urządzeniach kieszonkowych. Dlatego tak ważne stało się, aby użytkownicy zachowali czujność i odpowiednio zabezpieczyli swoje smartfony przed nieautoryzowanym dostępem, złośliwymi atakami i kradzieżą tożsamości. Aby złagodzić te zagrożenia i zachować kontrolę nad swoim cyfrowym życiem, postanowiliśmy podzielić się listą 10 najczęstszych zagrożeń dla bezpieczeństwa urządzeń mobilnych, którą przygotował zespół do spraw cyberbezpieczeństwa Bitdefender.

10 najpoważniejszych cyberzagrożeń dla użytkowników smartfonów

Chyba każdy użytkownik sieci i smartfonów spotkał się chociaż raz z

jakąkolwiek formą cyberprzestępstwa. Mogła to być wiadomość z niebezpiecznym linkiem na mediach społecznościowych, SMS, który zachęcał nas do drobnej wpłaty lub złośliwe oprogramowanie szpiegowskie. Niezależnie od tego, jak często korzystamy ze smartfonów, powinniśmy mieć na uwadze to, że zawsze możemy stać się ofiarami bezdusznego cyberprzestępcy. Dlatego zespół Bitdefender przygotował krótką listę najpowszechniejszych cyberzagrożeń, na które podatni są właściciele smartfonów.

1. Socjotechnika – ataki phishingowe, smishingowe i vishingowe

Phishing to taktyka socjotechniczna wykorzystywana przez hakerów i oszustów w celu uzyskania dostępu do wrażliwych danych, przejmowania kont oraz kradzieży pieniędzy. Podczas ataku phishingowego cyberprzestępcy wykorzystują e-maile, SMS-y i rozmowy telefoniczne do dostarczania fałszywych wiadomości, których celem jest nakłonienie użytkowników do przekazania ich danych osobowych i danych uwierzytelniających (dotyczących kont bankowych, usług online lub kont w mediach społecznościowych) lub pobrania złośliwego oprogramowania na ich urządzenia.

Środki zaradcze: aby nie stać się ofiarą, należy zawsze sprawdzić autentyczność wiadomości i przestrzegać zasad higieny cybernetycznej, np. nie odpowiadać na niechcianą korespondencję, klikać podejrzane linki i załączniki lub przekazywać poufne informacje osobom, które niespodziewanie się z Tobą skontaktują. Nie zapomnij skorzystać ze skutecznego systemu antywirusowego, które zablokuje złośliwe i fałszywe linki, jeśli nieświadomie uzyskasz do nich dostęp.

2. Wycieki danych

Źle zabezpieczone oraz zarządzane aplikacje instalowane na smartfonie mogą powodować wyciek danych osobowych, takich jak zdjęcia, imię i nazwisko, lokalizacja, listy kontaktów, historia przeglądania i wiele innych, w zależności od rodzaju używanej aplikacji. Niezależnie od tego, czy wyciek jest niezamierzony, czy też nastąpił w wyniku cyberataku, nie brakuje cyberprzestępców, którzy mogą niewłaściwie wykorzystać Twoje dane.

Łagodzenie cyberincydentów: Aby ograniczyć ryzyko, Bitdefender zaleca wprowadzenie ograniczenia uprawnień aplikacji i dostosowanie kontroli bezpieczeństwa smartfona, aby ograniczyć dane gromadzone przez każdą aplikację. Powinieneś także rozważyć przeczytanie drobnego druku dla każdej zainstalowanej aplikacji i unikać korzystania z tych, które żądają dostępu do zbyt wielu informacji.

3. Niezabezpieczone sieci Wi-Fi

Bezpłatne i publicznie dostępne sieci Wi-Fi w kawiarniach, centrach handlowych, a nawet na lotniskach są zazwyczaj niezabezpieczone (nie wymagają hasła i nie mają szyfrowania), co czyni je niezwykle podatnymi na ataki. Łączenie się z takimi sieciami Wi-Fi może umożliwić cyberprzestępcom szpiegowanie Twojej aktywności online i kradzież poufnych danych, takich jak dane uwierzytelniające oraz dane karty kredytowej.

Środki zaradcze: jeśli to możliwe, unikaj łączenia się z bezpłatną siecią Wi-Fi; jeśli to zrobisz, nigdy nie przeprowadzaj transakcji finansowych ani nie uzyskuj dostępu do poufnych danych biznesowych bez VPN.

4. Oprogramowanie szpiegowskie

Narzędzia cyfrowego nadzoru, znane jako oprogramowanie szpiegowskie lub oprogramowanie stalkerware, są instalowane na urządzeniu mobilnym w celu śledzenia SMS-ów, e-maili i lokalizacji telefonu użytkownika, robienia zrzutów ekranu, a nawet podsłuchiwania rozmów w pobliżu. Cyberprzestępcy, służby wywiadowcze i inni złoczyńcy cyfrowi mogą używać oprogramowania szpiegującego do monitorowania miejsca pobytu ofiary lub jej aktywności w Internecie, a także wyrządzania szkody fizycznej, emocjonalnej i finansowej.

„Ponieważ oprogramowanie szpiegowskie jest potajemnie instalowane na urządzenie ofiary, użytkownicy nigdy nie powinni pozostawiać swojego urządzenia mobilnego bez nadzoru, unikać pobierania nieznanych aplikacji, upewniać się, że ich telefony są chronione hasłem. Pamiętajmy także o tym, że niektóre złośliwe oprogramowania takie, jak Pegasus może zainstalować się przez kliknięcie w złośliwy link lub inny obiekt sieciowy” – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

5. Przeoczenie aktualizacji systemu operacyjnego i oprogramowania

Aktualizowanie systemu operacyjnego i aplikacji telefonu jest kluczem do ochrony urządzeń przed lukami w zabezpieczeniach, exploitami i

cyberatakami. Aktualizacje i poprawki często usuwają znane luki lub obejmują funkcje zabezpieczeń, które pomagają zabezpieczyć system operacyjny i aplikacje.

Środki zaradcze: Zawsze aktualizuj swoje smartfony i aplikacje. Pamiętaj, aby automatyczne aktualizacje były zawsze domyślnie włączone, dzięki temu będziesz miał pewność, że korzystasz z najnowszych wersji aplikacji. Jeśli Twoje urządzenie nie otrzymuje nowych poprawek lub nie jest już wspierane przez producenta, powinieneś rozważyć zmianę urządzenia.

6. Złośliwe aplikacje

Złośliwe aplikacje to niebezpieczne lub niechciane oprogramowanie, które może kraść Twoje dane osobowe i pieniądze, lub uszkodzić dysk smartfona. Sklepy z aplikacjami są pełne takich niebezpiecznych aplikacji, które mogą imitować te legalne i na pozór bezpieczne. Hakerzy wabią użytkowników bezpłatnymi aplikacjami, które oferują bardzo atrakcyjne funkcjonalności, oraz podróbkami legalnych aplikacji (grami, platformami mediów społecznościowych, aplikacjami do zakupów lub edycji zdjęć) i zamiast zapewniać reklamowane funkcje, blokują telefon, kradną dane i pieniądze, bombardują Cię reklamami lub pobierają wysokie opłaty abonamentowe.

Środki zaradcze: zachowaj czujność wobec fałszywych i złośliwych aplikacji za każdym razem, gdy pobierasz nowe programy na swoje urządzenie. Korzystaj wyłącznie z legalnych sklepów z aplikacjami, dokładnie sprawdzaj recenzje i drobny druk pod opisem oraz

przeprowadź wyszukiwanie w Internecie na temat aplikacji. W przypadku już zainstalowanych aplikacji poszukaj tych, które obciążają baterię i mobilną transmisję danych (zwłaszcza jeśli aplikacja nie wymaga połączenia z Internetem), korzystając z menu konfiguracji telefonu. Następnie zainstaluj renomowane mobilne rozwiązanie antywirusowe, które uchroni Cię przed złośliwym oprogramowaniem.

7. Słabe hasła

Większość użytkowników smartfonów ryzykuje swoją prywatnością i bezpieczeństwem, korzystając z tych samych haseł na wielu kontach. Złe nawyki związane z hasłami mogą prowadzić do nieautoryzowanego dostępu, przejęcia kont i oszustw.

Środki zaradcze: twórz silne i unikalne hasła do wszystkich swoich kont lub użyj menedżera haseł, aby bezpiecznie generować i przechowywać złożone hasła. Skonfiguruj dodatkowe warstwy zabezpieczeń (2FA, MFA lub dane biometryczne) i nigdy nie udostępniaj swoich danych uwierzytelniających, szczególnie w niechcianej korespondencji.

8. Kradzież tożsamości i ataki polegające na zmianie karty SIM

Co roku miliony internautów są ofiarami przestępstw związanych z tożsamością. Niestety, użytkownicy smartfonów są również narażeni na unikalny rodzaj ataku tożsamości w postaci zamiany karty SIM. Atak ten polega na tym, że hakerzy przekonują operatorów telefonii komórkowej do zmiany numeru telefonu ofiary na nowe urządzenie, umożliwiając im dostęp do wrażliwych danych, takich jak dane użytkownika numery kont i

kart kredytowych.

Środki zaradcze: atak polegający na wymianie karty SIM rozpoczyna się od zebrania przez cyberprzestępców danych osobowych swojej potencjalnej ofiary. W takim przypadku pierwszą linią obrony jest zachowanie prywatności danych osobowych i usunięcie numerów telefonów z kont, które ich nie wymagają. Powinieneś także włączyć uwierzytelnianie dwuskładnikowe na swoich kontach i natychmiast skontaktować się ze swoim operatorem, jeśli zauważysz podejrzane aktywności związane ze swoimi kontami.

9. Zagubione lub skradzione urządzenia mobilne

Zgubione lub skradzione urządzenia stanowią ogromne ryzyko dla bezpieczeństwa cyfrowego i tożsamości, ponieważ zazwyczaj przechowują różnorodne dane osobowe i wrażliwe, od danych logowania do aplikacji bankowych po hasła, zdjęcia, a nawet poufne dokumenty służbowe. Gdy cyberprzestępcy dostaną w ręce zgubione lub skradzione urządzenie, mogą dokonywać nieautoryzowanych zakupów przy użyciu powiązanych kart kredytowych, uzyskiwać dostęp do Twoich kont, zbierać dane osobowe lub uzyskiwać pożyczki na Twoje dane i popełniać inne przestępstwa związane z kradzieżą tożsamości.

Środki zaradcze: włącz lub użyj funkcji „znajdź mój telefon”, aby zlokalizować zaginiony telefon i zablokować urządzenie. Niektóre aplikacje do lokalizowania telefonu umożliwiają zdalne usuwanie danych z telefonu. Jest to opcja, którą warto rozważyć, jeśli chcesz uniemożliwić oszustom dostęp do Twoich danych. Zgłoś zgubiony lub skradziony

telefon swojemu operatorowi telefonii komórkowej i miejscu pracy, a także złóż raport na policji. Jeśli masz zapisane na urządzeniu karty kredytowe, skontaktuj się ze swoim bankiem i powiadom członków rodziny i znajomych o zdarzeniu.

10. Połączone urządzenia IoT

Wady bezpieczeństwa lub niewłaściwe wykorzystanie połączonej technologii IoT, w tym urządzeń do noszenia (inteligentnych zegarków) i innych urządzeń, które jeszcze bardziej rozszerzają obszar ataku użytkowników ze względu na słabe hasła (lub ich brak), niezabezpieczone transfery danych, naruszenia danych i wycieki.

Środki zaradcze: Aktualizuj podłączone urządzenia IoT, konfiguruj ustawienia prywatności, aby zmaksymalizować swoje cyberbezpieczeństwo, usuwaj dane osobowe ze starych, nieużywanych urządzeń, przeglądaj uprawnienia aplikacji i czytaj politykę prywatności przed zakupem nowych urządzeń w celu dodania sieci domowej.

Źródło: https://bitdefender.pl/10-najwiekszych-zagrozen-dla-twojego-smartfona/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 31.10.2023
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.