

OUCH!

Месечен бюлетин за Информационна Сигурност насочен към потребителите

Защита на мобилно устройство

Преглед

Мобилните ви устройства са страхотен и лесен начин да общувате с приятели, да пазарите или да ползвате онлайн банкови услуги, да играете игри и още куп други дейности. Тъй като тези устройства са толкова важна част от живота ви, тук даваме няколко прости стъпки с които да предпазите себе си и устройствата си.

Защитете устройствата си

Може да ви изненада фактът, че най-големият риск за мобилното ви устройство не са хакерите, а самите вие. Много по-вероятно е да изгубите устройството си, отколкото някой да го хакне. Първото нещо, което трябва да направите, за да защитите устройството си, е да активирате автоматичното заключване на екрана. Това означава, че всеки път когато искате да използвате устройството, трябва първо да отключите екрана с парола или пръстов отпечатък. По този начин, ако устройството бъде изгубено или откраднато, не може да бъде ползвано от друг. В допълнение, ето още няколко съвета с които да защитите устройствата си:

Обновяване

Включете автоматичното обновяване на устройствата си, за да бъдат винаги с последната версия на операционната система и приложенията. Злосторниците винаги търсят нови слабости в програмите, а разработчиците постоянно публикуват нови версии и кръпки за тях. Ако винаги имате последната версия на операционната система и мобилни приложения, правите хакването на устройствата си много по-трудна задача.

Проследяване

Инсталирайте или активирайте софтуер за отдалечено проследяване на мобилното си устройство през Интернет. По този начин, ако устройството бъде изгубено или откраднато, можете да се свържете с него чрез Интернет и да откриете къде се намира, и в краен случай да изтриете информацията, съхранена на него.

Доверени Приложения

Сваляйте само приложения, които са ви нужни, и то само от надеждни източници. За iPad и iPhone това означава да се ползва само Apple App Store. За Android сваляйте приложенията от Google Play, а за таблети на Amazon се придържайте към Amazon App Store. Въпреки че можете да сваляте приложения и от други места, те не биха били проверени и е много по-вероятно да бъдат заразени. Също така, преди да свалите приложение, проверете дали има много положителни отзиви, и дали е често обновявано от автора. Избягвайте чисто нови приложения

с малко отзиви, или такива, които рядко се обновяват. Накрая, независимо откъде е едно приложение, ако вече не ви трябва ви препоръчваме да го изтриете от устройството.

Опции за поверителност

Когато инсталирате ново приложение, прегледайте опциите за поверителност. Например, дали приложението, което току-що изтеглихте наистина има нужда от достъп до вашият списък с приятели и контакти? Също така препоръчваме да изключите проследяване на местоположението за всичко, и да го включвате само за приложения, за които смятате, че е нужно. Ако се чувствате несигурно с изискванията на някое приложение, намерете друго, което върши същото. В допълнение, проверявайте периодично до какво имат достъп приложенията, за да сте сигурни, че нещо не се е променило междувременно.

Архиви

Винаги архивирайте данните си. При мобилните устройства голяма част от информацията ви се архивира автоматично, като например снимките и съобщенията. Въпреки това, архивирайте и съхранявайте също така и настройките, приложенията и друга информация, тъй като това ще направи възстановяването много по-лесно в случай, че изгубите устройството си или преминете на ново.

Работа

Когато сте на работа, бъдете особено внимателни и никога не правете снимки или видеозаписи, които могат случайно да съдържат поверителна информация, като например изображения на бели работни дъски или компютърни екрани.

Мобилното ви устройство е мощен инструмент, който бихме желали да ползвате с удоволствие. Следването на тези няколко прости стъпки ще допринесе много за това вие и устройството ви да сте защитени.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:

<https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962>

<https://www.linkedin.com/pub/NIKOLAY-DACHEV/7b/5bb/96b>

Ресурси

Фрази-пароли:	https://www.sans.org/u/A3E
Архивиране / Възстановяван:	https://www.sans.org/u/A3z
Изхвърляне на мобилно устройство:	https://www.sans.org/u/A3u
Безопасна употреба на мобилни приложения:	https://www.sans.org/u/A3p
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

Iisensi

OUCH! се публикува от SANS Securing The Human и се разпространява под лиценза на [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Имате право да разпространявате този бюлетин или да го използвате във вашата информационна кампания, при условие че не го модифицирате. За преводи или повече информация моля пишете на www.sans.org/security-awareness/ouch-newsletter. Редакторски колектив: Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли | Превод: Николай Дачев и Радослава Несторова