УДК 004.056.53

СОТОВЫЙ ТЕЛЕФОН С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. В. Чекалова, В. О. Куренная, Э. М. Гугулян
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

В настоящее время мобильный телефон является и средством связи, и кошельком, и фото - видеокамерой, и компьютером. Поэтому так важно знать и понимать риски утечки из него личной информации, а также принимать определённые меры для их минимизации. Кражу могут осуществить мошенники, которые используют для этого различные вредоносные программы. Кроме того, лишиться важной информации можно, просто потеряв телефон. Все это приведет к возникновению проблем, связанных с защитой персональных данных.

Ключевые слова: информационная безопасность, мобильный телефон, утечка, вирус, вредоносная программа, персональные данные.

CELL PHONE FROM THE POINT OF VIEW OF INFORMATION SECURITY

A. V. Chekalova, V. O. Kurennaya, E. M. Gugulyan
Don State Technical University (Rostov-on-Don, Russian Federation)

Currently, a mobile phone is a means of communication, a wallet, a photo-video camera, and a computer. Because of this, it is worth knowing and understanding the risks of leakage of important and personal information, as well as taking certain measures to minimize these risks. A person can easily and quickly lose important information, for the theft of which various malicious programs are used. In addition, you can lose important information by simply losing your phone. All this will lead to problems related to the protection of personal data.

Keywords: information security, mobile phone, leak, virus, malware, personal data.

Введение. Сегодня мобильный телефон используется как средство связи, для выхода в Интернет и для хранения личных данных, к которым относятся сообщения, фотографии, видео, данные банковских карт и счетов и многое другое. Мошенники, понимая всё это, применяют различные меры для получения персональных данных владельца телефона, чтобы достичь свою главную цель — завладеть его денежными средствами. Цель данной статьи — рассмотреть основные факторы защиты смартфонов от несанкционированного проникновения и советы, как избежать внешних угроз.

Основная часть. Почти все смартфоны работают на двух операционных системах — Google Android и Apple iOS. Если iOS содержится только в телефонах фирмы Apple, то Android может быть абсолютно везде. Исходя из этого главный плюс iOS — она не запускает приложения, которые не одобряются Apple.

Самым важным фактором безопасности операционной системы является её постоянное обновление. На некоторых смартфонах с операционной системой Android такой функции не имеется, как правило, это касается дешевых телефонов. Поэтому именно они более прочих уязвимы перед угрозами. Ниже авторы предлагают перечень основных настроек безопасности для iOS и Android:

1. Если вы владеете устройством Android, то вам необходимо приобретать приложения только с площадок Google Play или Play Market.

2. Используйте надёжный пароль, в состав которого входят буквы латинского алфавита, цифры и дополнительные символы.

3. Не храните пароли в памяти телефона или в заметках.

4. Отключите вывод уведомлений на экран блокировки, исключив возможность чужому человеку посмотреть сообщение, пришедшее вам [1].

5. Используйте двухэтапную аутентификацию [2].

6. Запретите Siri, Алисе и другим голосовым помощникам работать по голосовой команде. При заблокированном экране голосовой помощник может выдать конфиденциальную информацию злоумышленнику.

7. Не используйте автоматическую синхронизацию данных.

8. Запретите вашему устройству автоматически подключаться к Wi-Fi, потому что таким образом устройство может подключиться к сети мошенника [3].

9. Старайтесь использовать VPN. VPN — это инструмент, который зашифрует переданные и полученные данные.

10. Отключите в браузерах использование cookie-файлов. Данные файлы хранятся в браузере после того, как вы посетили сайт, и содержат в себе основную информацию о вас.

11. Настройте сервисы браузера так, чтобы у него не было возможности записывать данные о вас. К таким данным относится местоположение, история посещаемых сайтов, переписки, онлайн-покупки и многое другое.

12. Отключите в браузерах автозаполнение. Когда пользователь соглашается на автозаполнение, он автоматически даёт браузеру возможность записывать и хранить пароли пользователя. Тем самым злоумышленнику будет легко узнать ваши пароли, просто зайдя в браузер.

13. Запретите приложениям доступ к вашим фотографиям, контактам, сообщениям.

14. Не храните номера мобильных телефонов на SIM-карте, потому что их нельзя зашифровать.

15. Делайте периодически резервные копии и сохраняйте их либо на компьютере, либо на внешних носителях. Резервные копии необходимо держать в надёжном месте.

16. Если вам доступна функция защиты сотового номера, которая предоставляется оператором мобильной связи, то обязательно ею воспользуйтесь, так как мошенники могут украсть номер телефона. Это действие откроет им дорогу к вашим аккаунтам, привязанным к номеру телефона.

Действия при краже или потере мобильного телефона. Международный идентификатор мобильного оборудования (International Mobile Equipment Identity, IMEI) используется во всех мобильных устройствах в виде 15-значного числа. Этот код идентифицирует устройство в сети. Чаще всего IMEI записан под аккумулятором, но также его можно посмотреть в настройках телефона либо получить по запросу *#06#. IMEI необходимо записать, чтобы в случае кражи можно было доказать, что именно вы являетесь владельцем данного устройства. Если вы поменяли SIM-карту, то это никак не повлияет на IMEI.

Стоит задуматься о достоинствах и недостатках регистрации сотового номера у оператора связи. Достоинством этого решения является то, что при потере мобильного устройства оператор обычно имеет возможность отключить телефон. Недостатком является то, что этим действием пользователь ещё больше привязывает свою личность к номеру телефона.

Почти у всех мобильных устройств есть функция «Поиск телефона», которая позволяет отследить или отключить телефон в случае потери/кражи.

Что делать, если нужно передать устройство другому человеку?

1. Прежде чем вы выбросите ненужный телефон, отнесёте его в ремонт или выставите на продажу, убедитесь, что в нём не хранится ваша личная информацию, которая обычно расположена на карте памяти или на SIM-карте. Данное действие необходимо выполнить даже в том случае, если устройство давно не использовалось. Избавиться от карты памяти и SIM-карты можно очень просто — извлечь из устройства и физически уничтожить. Но самый лучший способ — это сбросить телефон до заводских настроек.

2. Мобильный телефон необходимо покупать только в том магазине, которому вы доверяете. Это касается и ремонтных мастерских. Данное действие позволит снизить риск потери данных, когда вы покупаете ранее использованное устройство или относите своё устройство в мастерскую.

Слежка и прослушивание мобильного телефона. Мобильные устройства и сети сотовой связи тесно взаимосвязаны между собой. Когда пользователь отправляет сообщение или совершает звонок, телефон связывается с ближайшей вышкой сотовой связи. В результате этого действия оператор сотовой связи записывает информации о местонахождении телефона.

Признаки того, что телефон прослушивается:

1. Температура батареи. Если вы давно не используете телефон, а он при этом горячий, значит, он прослушивается.

2. Слишком быстрая разрядка телефона. Если телефон используется в обычном режиме, но заряжать его приходится значительно чаще, то можно сделать вывод, что ваше мобильное устройство прослушивается. Во время прослушки телефон записывает ваши звонки, разговоры в помещении, мошенники также могут включить камеру и видеть всё происходящее вокруг вас. Впрочем, телефон может быстро разряжаться, если он старый, со временем батарея изнашивается и не держит заряд.

3. Пауза во время выключения. Если вы выключаете телефон и видите, что он долго не выполняет указаний или выключается не до конца, т. е видна подсветка, которая не сразу тухнет, или телефон вовсе отказывается выключаться, возможно, это признаки прослушки.

4. Непонятная активность. Во время пользования смартфоном начинают открываться другие приложения, происходит самостоятельное отключение или включение — это признак того, что телефон используется кем-то другим удалённо.

5. Постоянный фоновой шум. В большинстве случаев телефон, который прослушивается, создаёт помехи при разговоре. Непонятный шум во время разговора по телефону может является для вас сигналом того, что диалог прослушивается [4].

В случае, если ваш телефон прослушивают, необходимо быть дешифратором, т. е. выдавать ложную информацию, тем самым выводя шпиона на «чистую воду». Затем необходимо обратиться за помощью к специалистам.

Заключение. Мобильный телефон — это устройство, которое очень сильно подвергается различным атакам извне. Всегда необходимо помнить, что не следует хранить в своём устройстве информацию, которую вы не хотели бы отдать мошеннику. Мошенника всегда интересуют только две вещи — денежные средства и личные данные, которые он может продать или использовать для кражи денежных средств.

Библиографический список

1. Савицкий, Алекс. 10 настроек, которые сделают ваш iPhone еще защищеннее / Алекс Савицкий // Kaspersky daily : [сайт]. — URL: https://www.kaspersky.ru/blog/iphone-maximum-security-tips/5382/ (дата обращения: 12.12.2021).

2. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Е. К. Баранова, А. В. Бабаш ; 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019. — 322 с.

3. Ярочкин, В. И. Информационная безопасность : учебник для студентов вузов / В. И. Ярочкин. — Москва : Академический проект; Гаудеамус, 2004. — 544 с.

4. Признаки прослушивания мобильного телефона / Центр безопасности данных : [сайт]. — URL: https://data-sec.ru/public/protect/mobile-wiretapping/ (дата обращения: 12.12.2021).

Об авторах:

Чекалова Анастасия Валерьевна, студент факультета «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), nassstu@bk.ru

Куренная Валерия Олеговна, студент факультета «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), lera.kurennaya@mail.ru

Гугулян Эрик Меружанович, студент факультета «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), ericgugulyan@gmail.com

About the Authors:

Chekalova, Anastasiya V., Student, Faculty of Computer Science and Computer Engineering, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), nassstu@bk.ru

Kurennaya, Valeriya O., Student, Faculty of Computer Science and Computer Engineering, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), lera.kurennaya@mail.ru

Gugulyan, Erik M., Student, Faculty of Computer Science and Computer Engineering, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF),ericgugulyan@gmail.com