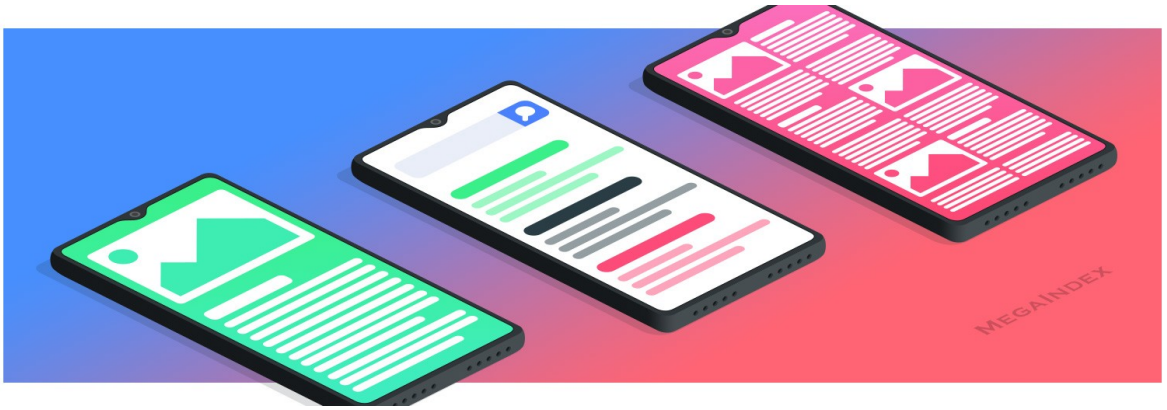
Мобильные устройства и безопасность.



Мобильные устройства стали неотъемлемой частью нашей повседневной жизни и сопровождают нас во всех делах. В смартфоне мы храним контакты и сообщения, всю переписку во всех социальных сетях. Здесь содержится информация о наших действиях и перемещениях. С помощью смартфона мы пересылаем важные документы и файлы, а также вводим данные банковских приложений и карт. Несмотря на то, что в мобильных устройствах сосредоточена вся наша жизнь, мы не всегда осознаем, сколько ценной личной информации они содержат.

Смартфон — фактически второй компьютер, поэтому прежде всего стоит озаботиться установкой достаточно сложного пароля и автоматической блокировки экрана для предотвращения случайного или намеренного несанкционированного использования данных и приложений на планшете или смартфоне третьими лицами. Используя сложный пароль, вы с меньшей вероятностью станете жертвой мошенников, которые могут воспользоваться тем, что вы оставили телефон без присмотра.

Мобильные устройства подвержены атакам злоумышленников так же, как и персональные компьютеры, а важной информации о вас часто содержат даже больше. Здесь установлены банковские приложения, хранится вся переписка, большая часть ваших фотографий, а иногда — рабочие файлы и данные.

В каждой операционной системе постоянно находят все новые и новые уязвимости — ошибки в ПО, которые создают угрозы для безопасности устройства. Одна из ключевых задач обновлений — решать эти проблемы и повышать уровень безопасности. Злоумышленники ориентируются в первую очередь на тех пользователей, которые пренебрегают простыми правилами безопасности, так как чем современнее версия программы, тем выше уровень защиты. В этой связи стоит регулярно проверять наличие обновлений для приложений, которым пользуетесь, в официальных магазинах приложений и применяйте данные обновления всякий раз, когда они доступны. Используйте функцию автоматического обновления, если не хотите помнить об обновлении приложений или каждый раз делать это вручную.

Точно также, как и на персональном компьютере, при работе с мобильными устройствами стоит опасаться вредоносного программного обеспечения. Существует два основных класса вредоносного ПО, опасного для обычных пользователей:

- программы для перехвата информации (они никак не будут проявлять себя на смартфоне и могут бездействовать довольно долго. Их задача — перехват паролей, данных для онлайн-банкинга, банковских SMS. Иногда эти программы получают сохраненные данные, а иногда перехватывают их в процессе ввода. Если вы не храните в телефоне информацию, которую ПО определяет как интересную, ваше устройство будет использовано как плацдарм для дальнейшего распространения по списку контактов);

- программы-блокировщики экрана (такая программа, оказавшись в смартфоне, выводит на экран свое сообщение, не позволяя пользоваться телефоном. Обычно вредоносное ПО этого типа требует немедленной отправки денег на какой-либо счет, а также SMS на какой-нибудь номер. Часто после этого вас подписывают на мошеннические услуги, или таким образом вы подтверждаете вывод денег со счета).

Кроме этого достаточно широко распространены программы, заставляющие телефон «подслушивать», что говорится рядом, и отсылать аудиозаписи на нужные адреса. Существуют программы, незаметно делающие фото, и программы, отслеживающие местонахождение телефона и отсылающие эти данные мошенникам.

Вредоносная программа может попасть на устройство разными способами:

- Вы получили SMS с подозрительной ссылкой, нажали на нее и перешли на сайт;

- Вы нажали на подозрительную ссылку в браузере — нечаянно или думая, что переходите в какое-то интересное вам место;

- Вы самостоятельно запустили установочный файл .apk на своем Android-устройстве, загрузив его на телефон с компьютера;

- Вы загрузили файл неизвестного производителя, полагая, что устанавливаете нужное приложение;

- Вы активировали анонимный QR-код.

Вас должны настораживать любые неожиданные предложения перейти по ссылке, если вы не полностью уверены в том, что увидите после перехода на сайт. Это может быть:

- ссылка на MMS в SMS;

- непрошеная реклама нового приложения;

- QR-код, кнопка загрузки, замаскированная под интересный текст или красивую картинку, или призыв посмотреть веселый видеоролик.

Принцип действия антивируса на мобильных устройствах совершенно такой же, как и на компьютерах: фильтрация входящих файлов. В этой связи важно обращать внимание на то, что загружается на устройство и всегда помнить, что программы,

загруженные с любых сторонних сайтов, проверенных или нет, могут быть заражены вредоносным ПО.

С целью обеспечения личной информационной безопасности и повышения уровня защищенности своих данных помните, что:

- установка «пиратских» приложений может повлечь за собой самые неприятные последствия;

- следует устанавливать только приложения, приобретенные или бесплатно загруженные в официальных магазинах;

- если вы не хотите платить за приложение, воздержитесь от загрузки пиратской версии и найдите бесплатный аналог;

- даже при загрузке приложений из официальных магазинов предварительно их следует проверять антивирусом.

Официальные магазины приложений — вполне безопасное место для поиска и установки необходимого ПО. В официальных магазинах всегда можно посмотреть рейтинг приложения, количество загрузок, а также почитать отзывы, чтобы получить представление о том, что вы собираетесь загрузить и не мошенническое ли это приложение. Кроме этого официальные магазины предоставляют возможность связаться с разработчиком приложения.

Устанавливая любое приложение очень важно обращать внимание на разрешения — действия, которые приложение сможет выполнять после установки. Разрешения у фальшивой программы могут сильно отличаться от разрешений оригинала. Всегда стоит задуматься об установке приложения если Вы даете ему разрешение на отправку смс-сообщений или осуществление звонков, а также на доступ к персональной и финансовой информации, а права администратора обычным приложениям вообще не нужны. Если вы загружаете приложение из официального магазина, про все разрешения можно прочитать подробнее, нажав на галочку около каждого пункта.