Угрозы при использовании мобильных устройств и меры противодействия.

Смартфоны очень прочно вошли в современную жизнь. Это теперь не просто средство телефонной связи, а многофункциональный портативный компьютер со множеством полезных приложений для коммуникации, выполнения платежей и прочими полезными инструментами. Смартфон сегодня - незаменимый помощник. Там же хранятся персональные данные пользователя, логины, пароли от различных сервисов, личные фотографии и т.п. Поэтому хакеры и прочие мошенники будут пытаться различными путями заполучить эту информации с целью собственной наживы.

Виды угроз.

Поскольку смартфон - это по сути портативный компьютер, то ему присущи многие виды компьютерных угроз.

Одной из значительных угроз является **вредоносное ПО**. Самые распространенные виды вредоносного ПО:

- **Вирусы, трояны.** Они предназначены для копирования, изменения, блокирования, удаления данных.
- **ПО-вымогатель.** Шифрует данные на устройстве, а затем предлагает за вознаграждение их расшифровать.
- **Рекламное ПО.** Назойливое появление окон с различными объявлениями, кликнув на которые можно загрузить и запустить вирус или троян.
- **Фишинг.** Это выманивание конфиденциальных данных на поддельных сайтах. Пользователь думает, что вводит свои данные или данные банковской карты на нужном сайте. А на самом деле этот сайт поддельный, обычно очень похожий на настоящий. Адрес его тоже похож на настоящий, только отличается на один символ или этот символ заменен. Например, буква «о» заменена на цифру «0».
- **Скамерское ПО.** Это когда пользователю предлагается получить некую компенсацию за пользование скачанной программой или выигрыш, но нужно заплатить за это небольшую комиссию. В результате скам-мошенникам достается эта комиссия, а нередко и реквизиты платежного средства слишком доверчивого пользователя и его персональные данные. Пользователь же не получает ничего.

Большинство указанного вредоносного ПО предназначено для системы Android, но есть и вредоносное ПО для системы IOS.

Есть угрозы, которые не являются следствием вредоносного ПО. Например, мошеннические объявления в мессенджерах или социальных сетях типа «Ваш родственник попал в ДТП», «на Ваше имя пытаются оформить кредит», «просьба дать взаймы деньги для покупки жизненно

важных лекарств, на оплату лечения или покупку медицинского оборудования». Есть угроза потерять свои средства при совершении онлайн покупок, когда пользователь оплачивает товар, а потом не получает товар и возврата денег не происходит.

Распознавание угроз.

Современное вредоносное ПО достаточно хорошо маскируется и распознать его довольно сложно. Наряду с использованием специализированного антивирусного (и другого защитного) ПО есть и косвенные признаки, указывающие, что на смартфоне работает вредоносное ПО. Можно обозначить следующие наиболее распространенные признаки:

- Смартфон начал быстро разряжаться в режиме ожидания;
- Смартфон начал работать медленнее, чем обычно или «зависать»;
- Смартфон как будто сам перезагружается или выключается;
- Активность в учетных записях которую Вы не инициировали. Например, запросы на подтверждение и сброс пароля, создания новой учетной записи, необычного места входа в учетную запись.

Угрозы, не вызванные вредоносным ПО, чаще всего связаны с психоэмоциональным воздействием на человека и затрагивают жизненно важные моменты. Мошенники обычно действуют с использованием телефонной связи или с использованием распространенных мессенджеров, для большей достоверности применяя правоохранительную или банковскую (финансовую) терминологию. Они также могут обратиться по фамилии, имени, отчеству и с использованием других персональных данных.

Меры противодействия угрозам.

В связи с тем, что вредоносное ПО очень хорошо маскируется, то для его поиска и нейтрализации лучше всего использовать специализированное антивирусное (защитное) ПО. Защитное ПО бывает различного типа, с разным набором встроенных функций. Поэтому если есть неуверенность в правильности выбора защитного ПО, то лучше обратиться за консультацией к специалисту. Необходимо понимать, что защитное ПО тоже будет использовать часть ресурсов смартфона и помнить - панацеи от всех видов вредоносного ПО не существует. К сожалению злоумышленники чаще всего идут на шаг впереди, поэтому новые определения угроз в защитном ПО появляются после выявления их у пользователей.

Нужно внимательно наблюдать за работой смартфона, чтобы определить признаки угроз, указанные выше. Вполне вероятно, что «неадекватное поведение» смартфона может быть вызвано и его технической неисправностью. Опять же, если есть сомнения в правильности своих оценок и предполагаемом плане действий, то лучше обратиться за консультацией к специалисту.

Для скачивания и установки приложений необходимо пользоваться только проверенными источниками (сайты разработчиков программ) или магазинами приложений, рекомендуемые изготовителем устройства.

Установка приложений из неофициальных источников повышает риск заражения смартфона. Также лучше избегать использование приложений с большинством отрицательных отзывов.

При работе программ необходимо контролировать, какие разрешения для доступа к ресурсам смартфона они запрашивают. Необходимо предоставлять только те разрешения, которые нужны только для выполнения функций конкретной программы.

При работе на каком-либо сервисе устанавливайте двухфакторную аутентификацию (если сервис это позволяет сделать), т.е. после проверки пароля сервис отправляет SMS (или сообщение электронной почты) с одноразовым паролем на «привязанное» к сервису мобильное устройство (или адрес электронной почты) и только после ввода полученного пароля сервис предоставляет доступ к его использованию.

Не рекомендуется переходить по ссылкам из сомнительных сообщений, даже если эти сообщения прислали ваши знакомые. При входе на сайт необходимо внимательно проверять его адрес, чтобы избежать перехода на поддельный сайт (сайт «двойник»).

Избежать угроз, связанных с психоэмоциональным воздействием поможет спокойное, скептическое отношение к такому воздействию. Слишком щедрое обещание должно насторожить пользователя, также как и пугающее. Если получено сообщение или звонок якобы от попавшего в беду родственника, то следует самому связаться с ним и выяснить всю необходимую информацию. Также нужно самому связаться с финансовой организацией, якобы от лица которой поступило сообщение или звонок. Мошенники могут подменить исходящий номер телефона и кажется, что звонок поступил от знакомого абонента. Никогда, не смотря на любые уговоры или угрозы, нельзя сообщать данные платежных средств или кодов, поступивших на Ваш телефон. Сотрудники правоохранительных органов или банковские работники никогда не запрашивают такую информацию. Также они никогда не звонят с помощью мессенджеров.

Зная, с какими видами угроз с использованием мобильных устройств можно столкнуться, а также меры противодействия этим угрозам, можно обезопасить себя от большинства проблем и получить достаточно полезный инструмент для коммуникаций.