Для многих из нас смартфоны – это самые используемые в повседневной жизни устройства. Времена, когда мобильные телефоны в основном использовались для звонков и отправки текстовых сообщений, давно прошли – теперь они исполняют роль портативных компьютеров с огромным набором разнообразных приложений, от социальных сетей до онлайн-банкинга. Зависимость пользователей от телефонов, а также объем хранящихся на них данных, объясняет, почему безопасности телефонов придается такое большое значение.

С ростом зависимости пользователей от мобильных устройств растут и угрозы мобильной безопасности. В этой статье рассказывается о безопасности мобильных телефонов и о способах их защиты.

Угрозы безопасности мобильных телефонов

Вредоносные приложения и веб-сайты

Мобильные вредоносные программы (вредоносные приложения) и вредоносные веб-сайты могут использоваться для кражи и шифрования данных как на мобильных телефонах, так и на компьютерах. Существуют разные виды вредоносных приложений. Наиболее распространенными являются трояны, осуществляющие переходы по вредоносным ссылкам и рекламным объявлениям.

Мобильные программы-вымогатели

Мобильные программы-вымогатели – это вредоносные программы, блокирующие доступ пользователей к мобильным устройствам и требующие выкуп, обычно в криптовалюте. Рост использования мобильных устройств в рабочих целях привел к распространению программ-вымогателей и повышению их опасности.

Фишинг

Большинство фишинговых атак на компьютеры и ноутбуки начинается с электронного письма, содержащего ссылку или вложение для загрузки вредоносных программ. Однако доля электронных писем при фишинговых атаках на мобильные устройства составляют лишь 15%. Большинство мобильных фишинговых атак осуществляется через SMS-сообщения, социальные сети и другие приложения.

Атаки типа «человек посередине» (Man-in-the-Middle)

В атаках типа «человек посередине» злоумышленники перехватывают сетевые сообщения с целью прослушки или изменения передаваемых данных. Этот тип атаки применим для различных систем, однако мобильные устройства наиболее уязвимы. В отличие от веб-трафика, для передачи которого обычно используется протокол HTTPS, поддерживающий шифрование, SMS-сообщения можно легко перехватить, а в мобильных

приложениях для передачи конфиденциальных данных может использоваться не поддерживающий шифрование протокол HTTP.

Перепрошивка и получение root-прав

Перепрошивка и получение root-прав – это получение доступа уровня администратора к мобильным устройствам iOS и Android. Пользователи мобильных устройств могут получить такие права, чтобы удалить установленные по умолчанию неиспользуемые приложения или установить приложения из ненадежных магазинов приложений, однако это сопряжено с риском. Расширение прав пользователя может позволить злоумышленникам получить доступ к данным и нанести ущерб.

Шпионские программы

Шпионские программы могут собирать и использовать личные данные без ведома и согласия пользователя. Данные, на которые обычно нацелены шпионские программы, включают историю вызовов, текстовые сообщения, местоположение пользователя, историю поисковых запросов, список контактов, электронную почту и личные фотографии. Киберпреступники могут использовать эту информацию для кражи личных данных или финансового мошенничества.

Что безопаснее: iPhone или Android?

Распространенный вопрос в сфере безопасности телефонов – что надежнее: iPhone или Android? Основное различие заключается в том, что iOS – это закрытая операционная система, тогда как Android используется разными производителями. Поскольку Apple не делится своим исходным кодом, снижается вероятность обнаружения уязвимостей в операционной системе iOS злоумышленниками. В результате этого многие считают iOS более безопасной операционной системой. Однако даже пользователям телефонов Apple не гарантирована полная безопасность, поэтому важно знать базовые правила обеспечения безопасности телефона и понимать их важность.

Не забывайте, что старые телефоны защищены хуже, чем новые. Например, ранние модели iPhone больше не получают обновления безопасности. Использование более новых моделей смартфонов поможет повысить их безопасность.

Рекомендации по защите смартфонов

Чтобы защитить свой смартфон, следуйте приведенным ниже рекомендациям по обеспечению безопасности.

Храните телефон в заблокированном состоянии

В случае кражи устройства злоумышленники могут получить доступ к личной информации. Для предотвращения этого используется блокировка экрана с помощью пароля, графического ключа, отпечатка пальца или

распознавание лица, в зависимости от ваших предпочтений и возможностей устройства.

Обычно при настройке блокировки экрана можно указать время бездействия телефона до включения блокировки. Чтобы повысить безопасность телефона, выберите минимальное значение времени. Автоматическая блокировка экрана обеспечивает защиту, даже если вы забыли заблокировать его самостоятельно. Кроме того, это позволяет экономить заряд батареи, поскольку после установленного периода бездействия гаснет экран телефона.

Настройка блокировки экрана, как правило, не вызывает сложностей. Для большинства устройств Android инструкции приведены в разделе Настройки местоположения и безопасности. Для пользователей iOS блокировку можно настроить из раздела Общие.

Используйте надежный пароль для телефона и приложений
Установите надежный пароль для смартфона. После определенного количества ошибок при попытке ввода пароля телефон заблокируется, отключится, а в некоторых случаях даже сотрет все данные. По данным опросов, многие бизнес-пользователи не меняют установленные по умолчанию пароли мобильных устройств и не используют многофакторную аутентификацию. Использование ненадежных паролей является источником угроз для всей организации.

Также рекомендуется установить надежные пароли для приложений, чтобы злоумышленникам было сложнее их подобрать. Использование уникального пароля для каждого приложения гарантирует, что злоумышленники не получат доступ сразу ко всей информации, подобрав один пароль.

С осторожностью относитесь к текстовым сообщениям
Текстовые сообщения – легкая мишень для мобильных вредоносных программ. Избегайте отправки конфиденциальных данных, таких как данные кредитной карты или важная личная информация, в виде текста. Также будьте осторожны с получаемыми текстовыми сообщениями.

Смишинг (SMS-фишинг) и вишинг (голосовой фишинг, осуществляемый по телефону) – популярные способы обмана пользователей мобильных телефонов. При SMS-фишинге злоумышленники отправляют текстовые сообщения, имитирующие сообщения от известных компаний. В сообщениях содержится просьба позвонить по определенному номеру и сообщить конфиденциальную информацию об учетной записи, чтобы решить возникшую проблему. При получении электронных писем или текстовых сообщений с просьбой подтвердить или обновить информацию об учетной записи, свяжитесь с компанией-отправителем напрямую, чтобы подтвердить

этот запрос. Не переходите по ссылкам в нежелательных электронных письмах или текстовых сообщениях.

Обращайте внимание на значок замка в адресной строке браузера
Значок замка в адресной строке браузера указывает, что используется безопасное соединение и что просматриваемый веб-сайт имеет актуальный сертификат безопасности. Проверяйте наличие этого атрибута при вводе личных данных, таких как адрес или платежная информация, и при отправке электронных писем из мобильного браузера.

Загружайте приложения из надежных источников
Всегда загружайте приложения из официальных магазинов приложений. Google и Apple проверяют каждое приложение перед размещением в Play Store или App Store, а значит, загрузка приложений из официального магазина менее рискованна, чем из других источников. Киберпреступники создают поддельные мобильные приложения, имитирующие реальные приложения известных производителей, чтобы получить конфиденциальную информацию пользователей. Чтобы не попасть в их ловушку, ознакомьтесь с обзорами приложений и проверьте последние обновления и контактную информацию разработчика. Эти данные должны содержаться в информации о приложении в магазине. Также рекомендуется удалять неиспользуемые приложения.

Регулярно обновляйте операционную систему устройств
Обновление операционной системы мобильного телефона позволяет улучшить его работу по всем аспектам – от производительности до безопасности. Чтобы обеспечить безопасность смартфона, важно поддерживать его операционную систему в актуальном состоянии. Обновление операционной системы защищает устройство от новых, недавно выявленных угроз. Проверить, обновлена ли операционная система телефона, можно в разделе О телефоне или Общие, нажав Обновления системы или Обновление ПО (в зависимости от устройства).

Подключайтесь к безопасному Wi-Fi
Мобильные устройства позволяют выходить в интернет практически из любого места. Наше первое действие в новом месте – это, чаще всего, поиск сети Wi-Fi. Использование бесплатного Wi-Fi позволяет сэкономить трафик, однако незащищенные сети – это источник рисков для безопасности устройства. Чтобы обеспечить максимальную безопасность при использовании общедоступных сетей Wi-Fi, подключитесь к виртуальной частной сети (VPN). VPN шифрует данные, скрывает местоположение и защищает вашу информацию от посторонних. Аналогично, для обеспечения максимальной безопасности проверьте надежность домашней сети.

Не выполняйте перепрошивку и получение root-прав

Перепрошивка и получение root-прав – это процесс разблокировки телефона и снятия установленных производителем средств защиты с целью получения доступа ко всем функциям и возможностям. Пользователи выполняют перепрошивку и получение root-прав на телефонах для доступа к неофициальным магазинам приложений, однако это сопряжено с риском. В таких магазинах не осуществляется проверка приложений, а значит устанавливаемые оттуда приложения могут шпионить за телефоном и красть конфиденциальную информацию.

Выполняйте шифрование данных

В смартфонах хранится огромное количество данных. В случае потери или кражи телефона может оказаться под угрозой конфиденциальная информация, например, электронные письма, контакты и финансовая информация. Шифрование помогает защитить данные на мобильном телефоне, поскольку зашифрованные данные хранятся в нечитаемом виде. Параметры шифрования большинства телефонов можно настроить в меню безопасности.

Чтобы проверить, зашифровано ли iOS-устройство:

Перейдите в меню настроек.

Нажмите Touch ID и код-пароль.

Вам будет предложено ввести код блокировки экрана.

Если ваш телефон зашифрован, в нижней части страницы отобразится надпись «Защита данных включена».

Чтобы зашифровать Android-устройство:

Во-первых, убедитесь, что заряд батареи устройства составляет не менее 80%.

Если на телефоне получены root-права, перед продолжением отмените их.

Перейдите в раздел Безопасность и выберите Зашифровать телефон.

Если процесс шифрования окажется прерван, например, при разрядке устройства, или если не отменены root-права, все данные могут быть потеряны. Шифрование может занять час и больше.

Включите дистанционное удаление данных с телефона

В случае потери или кражи телефона, можно дистанционно удалить личные данные из его памяти. Если ранее была создана резервная копия данных в облаке, о потере удаленных данных беспокоиться не придется. Инструкции по дистанционному удалению данных с iPhone и с Android-устройств приведены на страницах службы поддержки Apple и Google.

Выходите с сайтов после совершения оплаты

Если вы используете смартфон для онлайн-покупок или онлайн-банкинга, выполняйте выход с соответствующих сайтов после завершения транзакций. Не храните имена и пароли на телефоне, избегайте выполнения конфиденциальных транзакций при использовании общедоступных сетей Wi-Fi.

Отключайте Wi-Fi и Bluetooth, если они не используются

При включенном Wi-Fi и Bluetooth злоумышленники могут увидеть, к каким сетям вы подключались раньше, подделать их и обманным путем заставить ваш телефон подключиться к своим устройствам по Wi-Fi или Bluetooth. Подключившись к вашему телефону, злоумышленники могут без вашего ведома установить на него вредоносные программы, украсть данные или шпионить за вами. Поэтому рекомендуется отключать Wi-Fi и Bluetooth, когда они не используются.