Уважаемые коллеги, в связи с возрастающим числом атак на мобильные устройства, публикуем рекомендации по обеспечению безопасности мобильных устройств:

1. **Не устанавливайте на ваш смартфон приложения из неизвестных источников.** Всегда загружайте приложения из официальных магазинов приложений. Google и Apple проверяют каждое приложение перед размещением в Google Play или App Store, а значит, загрузка приложений из официального магазина менее рискованна, чем из других источников
2. **Используйте надежный антивирус.** Антивирусы применяются не только для ноутбуков и компьютеров, они также необходимы для мобильных устройств. Надежный мобильный антивирус защищает смартфоны от вирусов и попыток взлома. Kaspersky для Android обеспечивает круглосуточную защиту, имеет функцию поиска устройства и обнаружения шпионских приложений.
3. **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.
4. **Используйте надежный пароль для телефона и приложений.** Установите [надежный пароль](https://www.kaspersky.ru/resource-center/threats/how-to-create-a-strong-password) для смартфона. После определенного количества ошибок при попытке ввода пароля телефон заблокируется или отключится.
5. **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 (с особой осторожностью относитесь к сообщениям с просьбой «Попал в беду, займи несколько тысяч», «Проголосуй за племянницу» и т.п. )**.
6. **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.
7. **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.
8. **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.
9. **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.
10. **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.
11. **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.

**В случае если ваш аккаунт в мессенджере был взломан необходимо совершить следующие шаги:**

1. **Установить на всех менеджерах 2-х факторную аутентификацию (в т.ч. указать эл. Почту – в случае если забудете код, можно будет востановить);**
2. **Зайти в настройки и найти пункт «Связанные устройства» и удалить все записи кроме используемого мобильного устройства;**
3. **Произвести полную проверку устройства с помощью средства антивирусной защиты;**
4. **Посмотрите переписку, которую вел злоумышленник от вашего имени, вам необходимо оповестить всех, с кем он успел связаться;**
5. **В случае если есть подозрение о том, что на ваше имя могли быть оформлены, кредиты необходимо обратиться в правоохранительные органы;**
6. **Если после взлома вам начали приходить смс-сообщения от организаций (в т.ч. микрофинансовых, банков и пр.), не в коем случае нельзя переходить по ссылкам, содержащимся в сообщениях.**

**В статье использованы материалы с сайта kaspersky.com**