Как защитить мобильное устройство

Интернет и связь. Мошенничество

Киберпреступники постоянно охотятся за чужими личными данными. Часто их целью является секретная информация из смартфонов: номера карт, доступы к онлайн-банкам, домашний адрес, рабочие документы и личные фото. Рассказываем, как защитить свой телефон от действий злоумышленников

Какие бывают угрозы

Случайный доступ

При использовании одного устройства несколькими членами семьи следует контролировать доступ к конфиденциальной информации. Не разрешайте ребёнку использовать устройство, на котором хранится важная информация, а также установлены приложения мобильного банка, почты и другие

Кража

Если у вас украли смартфон, потери могут не ограничиться самим телефоном. Вор может получить доступ к вашим аккаунтам, которые привязаны к устройству. Воспользоваться мобильным банком и вывести с ваших счетов все доступные деньги. Использовать для шантажа и вымогательства вашу личную информацию — рабочие документы, фото, переписки в мессенджерах и соцсетях

Действия хакеров

Киберпреступники атакуют смартфоны с помощью вредоносных программ или файлов с вирусами, получают удалённый доступ к гаджетам и крадут с них секретные данные. Такая ситуация опаснее реальной кражи устройства — человек может не подозревать, что его информацию похитили

Как защитить устройство на случай кражи

Настройте блокировку экрана

Для защиты устройства включите автоматическую блокировку экрана. Для разблокировки используйте длинные пароли и сканер отпечатка пальца. Графический ключ легко подглядеть из-за плеча и несложно подобрать — люди рисуют слишком очевидные траектории

Защитите паролем или отпечатком пальца важные приложения и файлы

Это станет дополнительным фактором защиты и не позволит вору быстро попасть в банковские приложения, диспетчер файлов, галерею, почту, ваши аккаунты в социальных сетях

Как создать надёжный пароль, который легко запомнить

Настройте отслеживание

Установите программу, которая удалённо блокирует телефон. Такие приложения определяют местоположение устройства, включают сирену, фотографируют злоумышленника, а также стирают все личные данные

На мобильных устройствах по умолчанию установлена функция «Найти устройство», которая позволяет также удалённо заблокировать смартфон и удалить с него все данные. Убедитесь, что функция не отключена. Чтобы не потерять свои данные, регулярно делайте резервные копии. Важно, чтобы эти копии хранились в недоступном для злоумышленников месте, например на съёмном диске

Как защититься от киберпреступников

Скачивайте только проверенные приложения

Злоумышленники распространяют вредоносные программы под видом игр и полезных приложений. Загружайте приложения только из официальных магазинов: здесь строгая модерация, рейтинг, статистика по количеству скачиваний и отзывы пользователей

Если необходимо установить приложения банков, попавших под санкции, скачайте их с официальных сайтов организаций

Не переходите по подозрительным ссылкам

Чтобы заразить телефон вирусом, злоумышленники часто рассылают письма и сообщения с информацией о выигрыше, выгодной акции. При переходе по ссылке из такого сообщения на смартфон может загрузиться вредоносная программа. Если случайно перешли и файл загрузился, ни в коем случае не открывайте его и удалите

Установите антивирус на смартфон

Антивирусы смогут обнаружить вредоносную программу, если она уже оказалась на устройстве. Защитные системы блокируют переходы на заражённые сайты, проверяют ссылки, которые приходят в смс и мессенджерах, выявляют небезопасные настройки на смартфоне. Не забывайте периодически обновлять антивирус

Не давайте приложениям лишних разрешений

Не разрешайте приложениям, например планировщику дел или фонарику, получать доступ к камере, файлам на устройстве, совершению звонков, отправке смс. Если приложение получает подобные разрешения, оно сможет пользоваться этими функциями без вашего ведома — отправлять ваши фотографии на сервер злоумышленников или подписывать на платные рассылки. Разрешения приложений можно проверить в общих настройках телефона

Постоянно обновляйте систему

Киберпреступники ищут уязвимости в программном обеспечении и приложениях, поэтому разработчики программ регулярно выпускают обновления, исправляют ошибки и уязвимости. Включите автоматические обновления операционной системы в установленных приложениях. Если обновления не устанавливать, устройство будет хуже защищено от новых киберугроз

По возможности откажитесь от бесплатного вайфая

Публичные сети могут быть недостаточно защищёнными. Злоумышленники взламывают и перехватывают трафик, который идёт с вашего устройства. В их руках окажутся секретные данные, в том числе логины и пароли от различных аккаунтов. Кроме того, мошенники могут сами размещать точки доступа и выдавать их за бесплатный вайфай в парках, кафе и торговых центрах