

Полезные рекомендации по защите мобильных устройств.

Когда мобильный телефон недостаточно хорошо защищен, его владелец легко может оказаться жертвой телефонного хакера. Если у вас не установлено необходимое ПО или вы не соблюдаете правила безопасности, вы можете даже не узнать, что ваше устройство взломали.

Вот какие сигналы могут свидетельствовать о том, что ваш телефон взломан:

телефон разряжается быстрее, чем обычно;

телефон работает медленнее, чем обычно;

появляются записи о непонятных звонках и сообщениях;

в онлайн-аккаунтах замечается подозрительная активность.

Даже если вы не видите признаков взлома, все равно важно соблюдать полезные рекомендации по безопасному использованию мобильных устройств, чтобы защитить себя от инцидентов в будущем.

Своевременно обновляйте операционную систему

Как только появляется новая киберугроза, разработчики операционных систем выпускают обновления, чтобы защитить своих клиентов. Если вы игнорируете эти обновления, ваш телефон становится уязвимым перед потенциальными угрозами.

Используйте ПО для защиты всей семьи

Следите за тем, что смотрят ваши дети, безопасно контролируйте их перемещения и управляйте тем, как они используют свое устройство и какие веб-сайты посещают. Решение Kaspersky Safe Kids позволяет делать это легко и помогает защитить детей от негативных столкновений в интернете.

Отключайте инструменты удаленного подключения

Находясь в публичном пространстве, отключайте Bluetooth, Airdrop и Wi-Fi, чтобы посторонние не могли подключиться к вашему устройству.

Не давайте лишние разрешения приложениям

Загружая новое приложение, обязательно проверьте, какие данные оно будет использовать и обрабатывать, и установите необходимые ограничения. Если вы обнаружили на телефоне приложение, которое вы не устанавливали, удалите его немедленно.

Проверяйте приложения перед установкой

Скачивайте приложения только из официальных магазинов, таких как Google Play для Android, App Store для Apple, RuStore в России, AppGallery и GetApps в Китае. Обязательно прочитайте отзывы, политику конфиденциальности и список требуемых разрешений, прежде чем устанавливать приложение. Так вы будете знать, куда будут

отправляться ваши данные.

Используйте доступ по биометрии

Технология распознавания лиц и отпечатков пальцев в качестве дополнительной защитной меры для телефона гарантирует, что в случае кражи устройства злоумышленник не сможет быстро получить доступ к вашей информации.

Включите двухфакторную аутентификацию (2FA)

Этот метод идентификации означает, что для совершения онлайн-платежа или входа в персональный аккаунт требуется дополнительное подтверждение, например с помощью кода, полученного в SMS-сообщении или в электронном письме. С помощью вы можете безопасно создавать ключи для двухфакторной аутентификации, что гарантирует дополнительный уровень безопасности при использовании этой функции в приложениях.

Используйте сложные и неповторяющиеся пароли

Сложные, или «сильные», пароли необходимо использовать на любых веб-сайтах, но особенно это важно для банковских аккаунтов, личной электронной почты и любых других приложений, где содержится персональная информация. Это может не остановить хакеров, но, по крайней мере, сильно затруднит им задачу проникновения в ваши аккаунты, что в конечном счете может заставить их отступить.

Установите надежное приложение для защиты мобильных устройств

Ищите программное обеспечение с хорошей репутацией, которое может обеспечить защиту и стационарного компьютера, и мобильного телефона, особенно если вы часто пользуетесь публичными Wi-Fi-сетями. Такое ПО не даст хакерам проникнуть на ваш телефон и заранее предупредит вас о попытке проникновения.

Защищайте деловую информацию

Для утечки данных достаточно всего лишь одного незащищенного устройства. Если вам приходится использовать мобильные устройства для работы, примите дополнительные меры для защиты от мобильных угроз. По возможности используйте для работы отдельное устройство.