

5 полезных советов по конфиденциальности для вашего смартфона

Смартфон – хранилище данных, в котором содержатся мобильные номера, фото и скрины документов, текстовые файлы с паролями, важной информацией или личными заметками. Потеря конфиденциальной информации может обернуться взломом аккаунтов и другими серьезными проблемами.

Нужно позаботиться о защите логинов и паролей к учетным записям почты gmail или любой другой, логинов и паролей для входа в соцсети и прочие важные аккаунты. Недоступными для посторонних должны быть SMS-сообщения, а также телефонная книга. Еще одно приложение, хранящее важную информацию о владельце смартфона – его браузер, запоминающий посещенные сайты, учетные записи. На самом устройстве и карте памяти хранятся конфиденциальные файлы или документы, загруженные из сети.

Данные смартфона следует защитить от человека, который найдет устройство в случае его утери. Скорее всего, информация, имеющаяся в телефоне, не будет представлять ценности для него ценности, но лучше дополнительно обезопасить себя. Также устройство защищают от членов семьи или других близких людей, у которых есть доступ к смартфону. Важнее всего защитить телефон от целенаправленной кражи: когда злоумышленник стремится заполучить аппарат, чтобы завладеть личными данными и навредить владельцу.

Полезные советы для защиты вашего устройства

1. Отключайте геолокацию, если она не нужна. Большинство современных смартфонов поддерживают функцию GPS или другой сервис, позволяющий отследить местоположение. Эти функции нужны, чтобы воспользоваться картами или составить маршрут. Если человек не хочет, чтобы его отследили, достаточно выключить геолокацию.

2. Настройте экран блокировки. Графический ключ или пароль – два равноценных способа защиты данных. Если смартфон будет утерян или забыт где-то, посторонний человек не сможет им воспользоваться. Чтобы выбрать подходящий способ блокировки, достаточно запустить настройки, а затем перейти к разделу Security -> Screen lock. Чтобы сделать этот способ еще более безопасным, можно расширить поле ввода, выбрав не 3x3 точки, а 6x6. Можно скрыть направление графического ключа, чтобы никто не мог его подсмотреть. Для повышения безопасности стоит настроить смартфон таким образом, чтоб экран автоматически блокировался через 1-2 минуты бездействия.

3. Настраивайте права приложений. Многочисленные приложения запрашивают доступ к данным о местоположении, контактам и другой важной информации. Устанавливая приложение, подумайте, есть ли необходимость в предоставлении этих сведений. Если есть сомнения – поищите другое аналогичное приложение. Также нужно следить за тем, чтобы все приложения были установлены из официального источника и одобрены официальным хранилищем. Программы, скачанные со сторонних сайтов, могут содержать вредоносный код или быть взломаны.

4. Используйте VPN. Это приложение обеспечить защиту от цензуры и постороннего вмешательства. VPN может зашифровать ваше соединение и даст возможность просматривать заблокированные сайты из любой точки мира. Пользователь сможет легко получить доступ в Facebook, Twitter, Skype, YouTube и Gmail, а также любым веб-сайтам. Когда вы используете такую программу, интернет-провайдер не может расшифровать данные или узнать, какие сайты посещал пользователь. Надежная система шифрования, которую имеет программа ExpressVPN (скачать можно по ссылке:

<https://www.expressvpn.com/ru/what-is-vpn>), защитит не только браузер, но и банковские счета, транзакции, разговоры через популярные мессенджеры.

5. Зашифруйте память смартфона. Эту функцию имеют все устройства Android, версия которых выше 4.0. Благодаря ей пользователь сможет зашифровать память устройства так, чтобы доступ открывался только после введения пароля или PIN-кода. Даже после кражи такого устройства, злоумышленник не воспользуется личными данными. Функция позволит защитить данные SD-карты, на которой зачастую хранят личные документы. При шифровании названия файлов и их структура остаются неизменными, сохраняется возможность предпросмотра в виде иконок. Чтобы начать использовать функцию необходимо назначить пароль для дисплея длиной не менее 6 символов.

Чтобы не допустить утечку важных данных, нужно внимательно следить за функционированием смартфона и обращать внимание на наличие неизвестных программ и процессов, странных системных сообщений и технических сбоев. Если какие-либо функции или приложения незнакомы или не нужны пользователю, лучше отключить их, а при возможности – удалить.