Почему важна безопасность мобильного телефона?

Владимир Безмалый

Смартфоны наиболее широко используемые электронные устройства в нашей повседневной жизни. Когда-то мы использовали наши мобильные телефоны только для того, чтобы кому-то позвонить или отправить важное текстовое сообщение.

В наши дни они стали больше похожи на портативные компьютеры. Благодаря множеству функций, социальным сетям и приложениям для экономии времени смартфоны стали неотъемлемой частью нашей повседневной жизни. Независимо от того, составляете ли вы свой рабочий график, встречаетесь ли вы с кем-нибудь в Tinder или отслеживаете свой фитнес-режим, защищенный мобильный телефон обеспечивает душевное спокойствие, что ваши личные данные не попадут в руки тех, кто может им воспользоваться, причинить вам вред.

Во-первых, мы храним и передаем много конфиденциальных и личных данных на наших телефонах сообщения, изображения, видео, учетные данные для входа, пароли и многое другое. Независимо от того, станете ли вы жертвой взлома смартфона или просто потеряете устройство, на карту будет поставлено многое, если данные вашего телефона будут скомпрометированы.

В нашем списке лучших практик мобильной безопасности есть как базовые, так и расширенные советы по безопасности для пользователей смартфонов, но стоит помнить, что здравый смысл ваш лучший друг. Постоянное обновление вашего устройства предотвращает многие эксплойты операционной системы. Избегание подозрительных веб-сайтов и сторонних приложений – это может помочь защитить вас от вредоносных программ, в то время как наличие экрана или гостевой/детской блокировки на вашем телефоне затрудняет случайным людям получить легкий доступ к вашим файлам, просто подняв телефон. Эти и многие другие советы более подробно описаны ниже, так что давайте приступим к делу.

1. Убедитесь, что ваш экран всегда заблокирован

Первый совет может показаться очевидным, но вы будете удивлены, увидев, сколько людей забывают об этом.

Существует несколько допустимых методов блокировки смартфона, и вы даже можете использовать приложения для блокировки телефона.

Безусловно, самым надежным методом является длинный Pin-код, состоящий из букв и цифр. Но, увы, это неудобно. Поэтому чаще используют отпечаток пальца. Если у вас нет доступа к самому безопасному методу защиты мобильного телефона и вам интересно, как заблокировать свои приложения, есть и другие варианты, такие как идентификация лица, пароли и шаблоны разблокировки. Только будьте осторожны, чтобы не использовать чрезмерно упрощенные шаблоны или очевидные PIN-коды, такие как год рождения или легко угадываемая последовательность чисел. Учтите, что использование отпечатка пальца – это скорее удобство, чем безопасность.

2. Обновляйте программное обеспечение телефона

Многие хакерские эксплойты полагаются на уязвимости в мобильных операционных системах вдвойне на платформах Android, которые подвержены наибольшему количеству взломов смартфонов среди всех платформ смартфонов. Безопасность смартфонов Android зависит от постоянных обновлений, чтобы опережать хакеров, но многие люди отключают автоматические обновления. Более того, чтобы побудить покупателей покупать новые телефоны, многие производители сознательно сократили поддержку новейших операционных систем в своих старых моделях. Если вы хотите быть в курсе дел, обязательно внимательно следите за обновлениями ОС, чтобы избежать множества потенциальных проблем с безопасностью смартфона, которые возникают из-за устаревшего программного обеспечения на вашем телефоне. И учтите, что в среднем ОС от Google поддерживается всего два года, таким образом, у вас всего два года до смены телефона.

3. Создавайте надежные пароли

Еще один очевидный совет, который относится не только к мобильным телефонам, -будьте особенно осторожны с паролями. Многие соглашаются на очевидные и легко угадываемые пароли. Они могут включать их имена или фамилии, имена их домашних животных или членов семьи, а также другую очевидную информацию, такую как год, месяц или число рождения. Попробуйте использовать пароли, которые включают символы и цифры. Для еще большей безопасности вы можете использовать сокращения или использовать диспетчер паролей смартфона.

4. Не используйте пароли повторно

Говоря о советах по безопасности смартфонов, не только слабые пароли, но и отсутствие разнообразия паролей могут привести к утечке данных. Многие люди выбирают простой выход и используют одни и те же два или три

пароля для каждого приложения и сайта, который они посещают. Не делайте этого.

5. Не сохраняйте на телефоне личные данные для входа и платежные данные

Если «как защитить мой телефон от хакеров» появляется в вашем списке дел, начните с нескольких простых шагов, чтобы хакерам пришлось изрядно потрудиться, чтобы получить доступ к вашим данным. Даже лучшие приложения для обеспечения безопасности смартфонов не могут компенсировать простую халатность. Многие люди склонны жертвовать безопасностью ради удобства, оставляя важную информацию на своих телефонах, чтобы им не приходилось вводить ее снова при входе в социальные сети или совершении онлайн-платежей. Это позволяет тем, у кого есть доступ к вашему телефону, действительно легко пролистывать информацию, которая потенциально может стоить вам больше, чем просто утечка неловкой личной переписки.

Веб-браузеры еще одно популярное место охоты для хакеров. В советах по безопасности смартфона для вашего браузера часто упоминаются различные риски, связанные с просмотром веб-страниц на вашем телефоне. Мы говорим не только о рисках, которые возникают из-за различных уязвимостей внутренней безопасности. Более распространенный и упускаемый из виду риск заключается в том, что ваш браузер должен отвечать за вход в систему и пароли, позволяя ему запоминать все данные за вас. Будьте умны и ответственны при использовании телефона проще каждый раз вводить пароль электронной почты, вход на форум или данные кредитной карты, чем справляться с такой потерей данных.

6. Загружайте приложения только из безопасных источников

Говоря о смартфонах и безопасности, часто упускают из виду еще один аспект использование только официального и санкционированного программного обеспечения. Хотя может возникнуть соблазн сделать джейлбрейк или root доступ на телефоне и использовать сторонние приложения, обещающие ускорить и разблокировать дополнительные функции на вашем телефоне, постарайтесь избежать соблазна. И у Google, и у Apple есть строгие правила относительно того, какие приложения разрешены в их магазинах по определенной причине многие интернет-приложения для телефонов содержат вредоносные программы и эксплойты, предназначенные для кражи личных данных с вашего телефона. Использование только официального программного обеспечения необязательно даст вам самый безопасный телефон, но это определенно важный и часто упускаемый из виду шаг в процессе обеспечения

безопасности ваших личных данных. Неслучайно производители мобильных устройств недоброжелательно относятся к людям, которые рутируют, взламывают свои устройства или используют сторонние сайты приложений эти меры предосторожности существуют не просто так.

7. Установите антивирус на свой мобильный телефон

Вот еще одна идея, которая не исходит от мобильных устройств, но работает также хорошо, как и на персональных компьютерах. Существует множество приложений для обеспечения безопасности сотовых телефонов как для устройств Android, таки для iOS. Вы должны использовать один, даже если это может показаться немного утомительным.

В прессе было много плохих отзывов о том, как приложения для защиты телефона могут замедлить работу вашего устройства. На самом деле большинство хороших из них довольно не навязчивы и вызывают замедление только при глубоком сканировании. С другой стороны, они могут убедиться, что ваш телефон защищен от вредоносных файлов и эксплойтов, даже если вы посещаете подозрительные сайты или пытаетесь загрузить приложения, которые в противном случае могли бы повредить ваше устройство или украсть данные. Однако они не всемогущи, поэтому вы все равно должны быть осторожны с загружаемыми файлами и посещаемыми сайтами.

8. Рассмотрите возможность использования VPN и будьте осторожны с общедоступными подключениями Wi-Fi

В настоящее время в техническом сообществе часто используется термин «VPN». В советах по безопасности смартфонов от Wired, PC Mag и других популярных технических сайтов часто говорится о важности осторожности при подключении к общедоступным точкам доступа Wi-Fi и незащищенным источникам бесплатного Интернета. VPN-виртуальные частные сети отличное решение. Хотя обычно рекомендуется держаться подальше от незащищенных общедоступных сетей (которые любят большинство хакеров, поскольку им часто не хватает важных функций безопасности и шифрования, что значительно упрощает их работу), использование VPN может повысить безопасность ваших мобильных данных в таких ситуациях, когда вам нужно выйти в Интернет и у вас нет других вариантов. Для этого они подключаются к внешнему серверу и маскируют ваш IP-адрес, чтобы скрыть истинное местоположение вашего устройства.

9. Убедитесь, что вы защищены при использовании Bluetooth

Удивительное количество людей не осознают опасности Bluetooth. Хотя этот удобный протокол сопряжения устройств может сэкономить вам много

хлопот при передаче файлов или беспроводном подключении устройств, он также может быть простым способом для хакеров проникнуть в ваш телефон, если вы не используете его ответственно. Убедитесь, что ваше устройство не может быть обнаружено, и всегда отключайте Bluetooth, когда вы его не используете. Не смотря на то, что предлагают некоторые советы по безопасности мобильных устройств, хакер не скрывается каждую секунду, пока ваше устройство доступно в сети, но, тем не менее, стоит быть осторожным.

Всегда убедитесь, что вы распознали устройство, с которым вы сопряжены, и старайтесь поддерживать соединение только до тех пор, пока это необходимо для того, что вы пытаетесь сделать. Не ленитесь – слишком многие люди оставляют Wi-Fi и Bluetooth включенными навсегда, чтобы потом пожалеть об этом. Конечно, забыть выключить Bluetooth не так опасно для безопасности вашего мобильного устройства, как подключение к незащищенным общедоступным сетям, загрузка подозрительных файлов или использование устаревшего программного обеспечения… но почему бы не охватить все аспекты, когда вы уже прилагаете усилия?

10. Держитесь подальше от облачного хранилища и включите удаленное стирание данных

В наши дни облачные хранилища в моде. Он предлагает множество надежных хранилищ для всех ваших данных и предоставляет еще один способ сохранить ваш и файлы в безопасности на случай, если ваш телефон потеряется или повредится. Но есть загвоздка.

Устройства Android автоматически синхронизируются с учетными записями Gmail и Google Диском. Посмотрим правде в глаза: несмотря на то, что говорится в некоторых советах по безопасности смартфонов iOS и Android, Google и другие поставщики аналогичных облачных услуг, такие как Megaupload, были вовлечены в различные теневые сделки, связанные с личными данными людей. Хотя у Большого Брата, вероятно, нет времени или интереса просматривать тысячи фотографий с вашей свадьбы или выпускного вечера, вам все равно стоит помнить, что большинство правительств оставляют за собой право заставлять таких поставщиков делиться имеющимися у них данными.

Некоторые утверждают, что им нечего скрывать. Тем не менее, если вы беспокоитесь о безопасности смартфонов, вы убедитесь, что точно понимаете, на что вы подписываетесь при использовании и облачных сервисов. Вместо того, чтобы жертвовать удобством простого облачного хранилища на потенциальные риски безопасности, подумайте об использовании зашифрованных USB-дисков или аналогичного оборудования.

Также рассмотрите возможность включения возможности удаленного стирания всех данных вашего телефона. Это позволит вам быстро уничтожить любые личные данные в случае потери, кражи или взлома вашего телефона.

8 декабря, 2020

https://ib-bank.ru/bisjournal/news/14755