«Правила цифровой гигиены»

Устанавливайте сложные пароли и регулярно меняйте их

Чем длиннее и сложнее пароль, тем труднее его будет взломать. Лучший вариант — большая комбинация случайных букв, чисел и символов. Ни в коем случае не используйте имена детей и родственников, дни рождения и другие личные данные, которые легко найти в соцсетях.

Но каким бы сложным ни был ваш пароль, не забывайте менять его хотя бы раз в полгода. И не поддавайтесь соблазну повторно использовать какой-нибудь из старых. Чем дольше используется один пароль, тем выше вероятность, что он попадёт в руки хакеров или будет скомпрометирован. Кроме того, не используйте одну и ту же комбинацию на разных сайтах. Тогда в случае взлома аккаунта на каком-нибудь форуме злоумышленники не смогут попасть в ваш кабинет в онлайн-банках.

Чтобы не запутаться с большим количеством комбинаций, используйте менеджер паролей, например LastPass или 1Password. Они хранят все ваши коды и автоматически вводят их на сайтах, а вам нужно помнить только один мастер-пароль.

Делайте резервное копирование данных

С каждым днём всё больше распространяются вирусы-вымогатели. Они блокируют устройство и угрожают удалить с него все данные, если вы не заплатите выкуп. Такие вирусы могут попасть на компьютер или смартфон, если вы перейдёте по ссылке в фишинговом письме или кликнете на фейковый рекламный баннер.

Это можно автоматизировать. Есть специальные платные сервисы вроде Carbonite, которые регулярно копируют и сохраняют ваши данные. В Mac и Windows также есть возможность создавать резервные копии на внешнем носителе. В MacOS эта функция называется Time Machine.

В Windows 10 подобный инструмент находится в параметрах «Обновление и безопасность», а в Windows 7 в «Системе и её обслуживании». Убедитесь, что после копирования данных вы отсоединили внешний носитель, тогда в случае заражения файлы на нём точно останутся целыми.

Не делитесь слишком личной информацией в соцсетях

Во-первых, это золотая жила для разных мошенников — в первую очередь для похитителей личности. Они собирают персональные данные пользователей, чтобы получить доступ к их финансам. Во-вторых, часто происходят утечки данных, так что под угрозой даже информация, невидимая для других пользователей.

Поэтому максимально сократите количество данных, которыми делитесь на разных медиаплатформах.

Не публикуйте в открытом доступе дату своего рождения, не указывайте свой адрес, местоположение и контакты. Отключите геотеги на фотографиях. Хотя сами по себе такие данные кажутся безобидными, с их помощью преступники могут многое о вас узнать.

Регулярно проверяйте историю финансовых операций

Мошенники пользуются похищенной информацией, чтобы быстро снять деньги с вашего счёта или взять заём от вашего имени. Поэтому обязательно смотрите выписки

по картам, особенно кредитным. А раз в год запрашивайте свою кредитную историю, чтобы проверить, не открыты ли на ваше имя чужие займы.

При возможности настройте в банковском приложении двухфакторную аутентификацию. Тогда при входе вам нужно будет вводить нетолько пароль, но и код из СМС или пуш-уведомления. Этот метод безопаснее, чем обычная активация приложения.

Периодически отписывайтесь от лишнего

Люди сейчас часто меняют один сервис на другой, в итоге у них накапливается масса ненужных рассылок и подписок. Вспомните, чем вы в последнее время перестали пользоваться, и проверьте, не настроено ли у вас автоматическое списание средств.

Не сохраняйте данные банковской карты на сайтах и в приложениях. Особенно там, где есть пробный период, после которого использование станет платным. Всегда есть шанс, что вы забросите сервис через пару дней, а деньги продолжат списываться автоматически.

Следите за тем, какой цифровой отпечаток вы оставляете

Браузеры и поисковики хранят данные о пользователях: фиксируют ваше местоположение, запросы, настройки. Сотовые операторы тоже этим занимаются: они хранят список набранных номеров и текстовые сообщения. Apple и Google собирают информацию о том, как вы пользуетесь их устройствами: какие приложения устанавливаете, что ищете.

И всё это совершенно законно, ведь вы дали согласие на обработку персональных данных и нажали на соответствующую кнопку.

Полностью от этого оградиться нельзя, но вы можете ограничить объём собираемых о вас данных. Изучите настройки своего устройства. Отключите доступ к вашему местоположению для тех приложений, которым он по сути не нужен. Отключите историю местоположений в «Google Картах», чтобы информация не отправлялась в компанию.

Регулярно обновляйте программное обеспечение

В обновлённых версиях исправляются ошибки, которыми хакеры могли бы воспользоваться в своих целях. Поэтому чем старее ваша версия операционной системы, программы или браузера, тем вы уязвимее. Включите автообновление, чтобы не забывать об апдейтах. Удаляйте программы и приложения, которыми вы перестали пользоваться или которые больше не поддерживаются разработчиками.

Не забывайте о роутере и всевозможных умных устройствах: им тоже необходимы регулярные обновления. Проверьте информацию на сайте производителя и следуйте инструкциям.