Автор: Александр Егоров НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР
21.08.2020, 19:10

5 правил цифровой гигиены

Соблюдать правила цифровой гигиены, так же необходимо, как правила гигиены общей. В противном случае могут пострадать или ваши финансы, или ваши данные, или устройства, с которых вы выходите в Интернет. А, может быть, и всё зараз.

1. 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.

2. 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 кликните на фейковый рекламный баннер.

Будьте особенно осторожны при интернет-сёрфинге и обязательно создавайте резервные копии важных файлов.

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.

3. Не делитесь слишком личной информацией в соцсетях

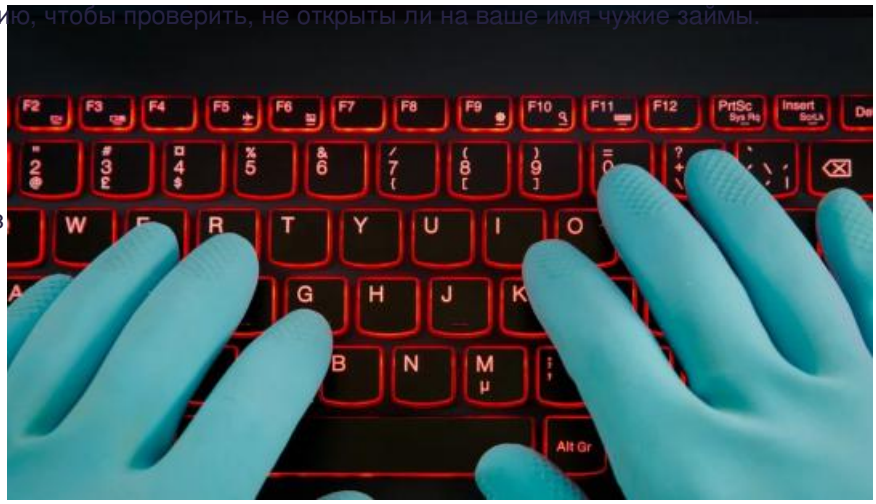
Во-первых, это золотая жила для разных мошенников — в первую очередь для похитителей личности. Они собирают персональные данные пользователей, чтобы получить доступ к их финансам. Во-вторых, часто происходят утечки данных, так что под угрозой даже информация, невидимая для других пользователей. Поэтому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

4. Регулярно проверяйте историю финансовых операций

Мошенники пользуются похищенной информацией, чтобы быстро снять деньги с вашего счёта или взять займ 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 не только пароль, но и код из СМС или пуш-уведомления. Этот метод безопаснее, чем обычная активация приложения.

5. Периодически отписывайтесь от лишнего

Люди сейчас часто меняют один сервис на другой, в итоге у них накапливается масса ненужных рассылок и подписок. Если первые просто захламляют почтовый ящик, то вторые могут стоить денег. 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.

Автор: Александр Егоров © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2262
21.08.2020, 19:10 0
URL: https://babr24.com/?IDE=273473 Bytes: 4295 / 4153 Версия для печати

Автор текста: **Александр Егоров**.

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта