

10 правил информационной безопасности (памятка)

Содержание:

- 1. Создавайте сложные пароли
- 2. Установите антивирус
- 3. Проверяйте безопасность сайтов
- 4. Остерегайтесь общественного Wi-Fi
- 5. Двухфакторная аутентификация — ваш друг
- 6. Не сохраняйте пароли в браузере
- 7. Остерегайтесь фишинговых писем
- 8. Минимум личной информации в социальных сетях
- 9. Загружайте приложения только из официальных источников
- 10. Используйте отдельную карту для покупок в интернете

Безопасность в интернете сегодня не менее важна, чем защита дома или автомобиля. В сети можно потерять не только доступ к личной информации, но и деньги, а иногда даже репутацию. Мошенники используют украденные данные, чтобы оформлять кредиты на чужое имя, шантажировать владельцев или продавать информацию в даркнете. Звонки из «службы безопасности банка» или «полиции» стали обычным явлением: злоумышленники представляются сотрудниками финансовых организаций или правоохранительных органов и пытаются выманить данные карт. По данным Роскомнадзора, ежегодно от кражи персональных данных страдают сотни тысяч россиян.

Ваши соцсети, почту, доступ к банковским приложениям могут «увести» очень легко и быстро, если не соблюдать простые меры безопасности. Разбираем 10 правил информационной защиты, которые сохранят ваши личные данные от злоумышленников.

1. Создавайте сложные пароли

Частая и очень нелепая ошибка — ставить один и тот же пароль на все сервисы и сайты. Если его взломают, злоумышленник получит доступ сразу ко всему: от почты до онлайн-банка. Пароль должен быть длинным, содержать заглавные и строчные буквы, цифры и специальные символы. Не стоит хранить его в заметках или записывать на бумажке. Мы рекомендуем установить менеджеры паролей, которые автоматически создают и сохраняют надёжные комбинации. Самые популярные — LastPass, KeePass и 1Password. Главное — не потерять пароль уже от них.

2. Установите антивирус

«Ничего не качаю, вирусов не боюсь» — так думают многие, пока не сталкиваются с проблемой. Антивирус защитит устройство от вредоносных программ, которые могут похитить личные данные. Главное — не забывать обновлять его, ведь вирусы постоянно эволюционируют. Современное ПО умеет блокировать фишинговые сайты и защищать данные даже в общественных Wi-Fi-сетях.

3. Проверяйте безопасность сайтов

Перед вводом пароля или платежных данных обратите внимание на адресную строку. Надёжные сайты используют защищённое соединение (HTTPS), а рядом с адресом есть значок замка. Если видите HTTP без буквы S — задумайтесь, стоит ли доверять этому ресурсу. Фишинговые площадки часто маскируются под известные сервисы, используя поддельные домены: например, sberbank-security.com вместо официального sberbank.ru.

4. Остерегайтесь общественного Wi-Fi

Кафе, аэропорты, ТЦ — удобные места, но сеть здесь может быть незащищённой. Подключившись к общедоступному Wi-Fi, вы рискуете передать данные злоумышленникам. Если срочно нужен интернет, лучше воспользоваться мобильным подключением или включить VPN-сервис для шифрования данных.

5. Двухфакторная аутентификация — ваш друг

Большинство сервисов позволяют включить двухфакторную проверку: например, при входе нужно не только ввести пароль, но и подтвердить вход через SMS или приложение. Это значительно снижает риск взлома. Особенно важно активировать этот метод на почте и в банковских аккаунтах.

6. Не сохраняйте пароли в браузере

Автосохранение удобно, но крайне небезопасно. Если злоумышленник получит доступ к вашему компьютеру или телефону, он сможет войти в ваши аккаунты без лишних усилий. Используйте менеджеры паролей: они надёжнее и безопаснее.

7. Остерегайтесь фишинговых писем

Электронную почту мошенники «угоняют» чаще всего, потому что именно её люди оставляют для регистрации на форумах, в приложениях или соцсетях.

Если получаете письмо с просьбой срочно ввести пароль или номер карты, не торопитесь! Проверьте адрес отправителя, посмотрите, нет ли в тексте грамматических ошибок, верно ли прописана ссылка. Надёжные компании не требуют личных данных по почте. Никогда не переходите по подозрительным ссылкам из писем: они могут вести на вредоносные сайты.

8. Минимум личной информации в социальных сетях

Ещё одно правило: не указывайте в соцсетях номер телефона, адрес или другие личные данные, если этого можно избежать. Чем меньше информации о вас в открытом доступе, тем сложнее мошенникам использовать её против вас. Особенно опасно делиться снимками удостоверений личности, билетов, банковских карт: эти данные быстро утекают к различного рода аферистам.

9. Загружайте приложения только из официальных источников

Скачивание программ с неизвестных сайтов — прямая дорога к заражению устройства. Приложения для интернет-банкинга, мессенджеры, игры — всё это лучше устанавливать из проверенных магазинов: Google Play, RuStore или App Store. Также не стоит отключать встроенную защиту смартфонов от загрузки непроверенных приложений.

10. Используйте отдельную карту для покупок в интернете

Для покупок на маркетплейсах или в других онлайн-магазинах заведите отдельную карту. Положите на неё небольшую сумму. Даже если данные утекут, основной счёт останется в безопасности. Многие банки предлагают виртуальные карты, которые можно удалить сразу после покупки, — это удобный вариант.

Соблюдая эти правила, вы снижаете риски кражи данных, звонков мошенников и финансовых потерь. Информационная безопасность — это личная ответственность каждого человека, такая же, как и забота о здоровье. Поэтому крайне важно следить за обновлениями программ, не доверять подозрительным ссылкам и использовать современные методы защиты.