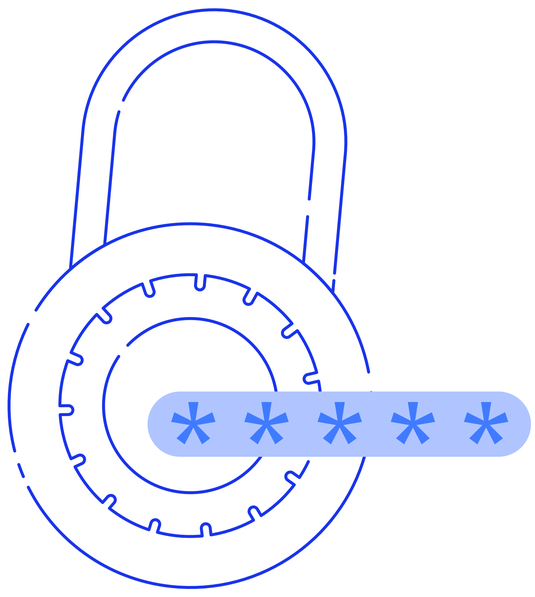
Медиабезопасный чек-лист

Вероятно, ваше устройство взломано, если:

- [ ] Замедлилась его работа
- [ ] Появляются новые файлы и приложения, наблюдается аномалия в их поведении
- [ ] Часто всплывают системные сообщения об ошибках
- [ ] Браузер работает медленно, при вводе адреса открывается другой ресурс, нет возможности закрыть вкладку
- [ ] Антивирус отключился или стал работать некорректно. При включении компьютера операционная система не загружается
- [ ] Не получается отключить устройство
- [ ] Вашим знакомым приходят сообщения от вашего имени, которые вы не отправляли
- [ ] В почтовом ящике много сообщений без адреса отправителя и темы письма

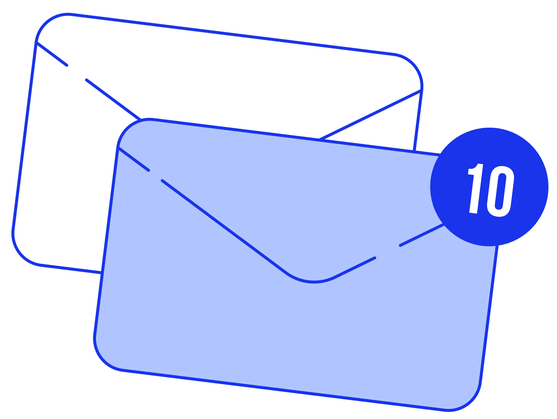
Чтобы избежать или минимизировать риски взлома, следуйте этим рекомендациям:

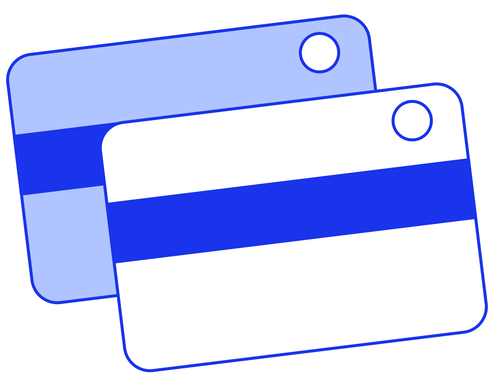
- Пользуйтесь надёжными паролями, не применяйте один пароль для всех аккаунтов.
- Храните пароль в специализированных защищённых приложениях, например, LastPass и Kaspersky Password Manager. Желательно не хранить в браузере.
- Установите дополнительный пароль на телефон или на конкретное приложение.
- Применяйте двухфакторную аутентификацию. Вход в личный кабинет нужно подтвердить с помощью другого устройства/ресурса. Генерируйте одноразовые коды с помощью Google Authenticator и Яндекс.Ключ.



- Настройте видимость своих данных, ограничьте доступ к своему профилю. Будьте внимательны к тому, кого добавляете в друзья.
- Проверяйте подключённые устройства.
- Не забудьте скрыть номер телефона и ограничьте поиск профиля по номеру.
- Отключите геолокацию в приложении.

- Проверьте, какие приложения имеют доступ к данным вашего аккаунта.
- После авторизации с использованием соцсети, удаляйте данные, почистите файлы cookie.
- Не передавайте важные файлы и личную информацию вовремя включённого VPN, а лучше вовсе откажитесь от его использования.
- Чтобы обезопасить данные на своём почтовом сервисе установите соответствующие лицензированные программы, например, KasperskySecurity.





- Открывайте ссылки только из надёжных источников.
- Не используйте мобильный банк при подключении к общественному Wi-Fi.
- Не заряжайте свои устройства, используя общественные кабели.
- Разграничьте использование персональных и служебных устройств для доступа в корпоративную сеть.

Следите за новостями в социальных сетях НЦПТИ. Там мы рассказываем о новых схемах кибератак и держим в курсе наших подписчиков!

Телеграм

ВКонтакте

НЦПТИ