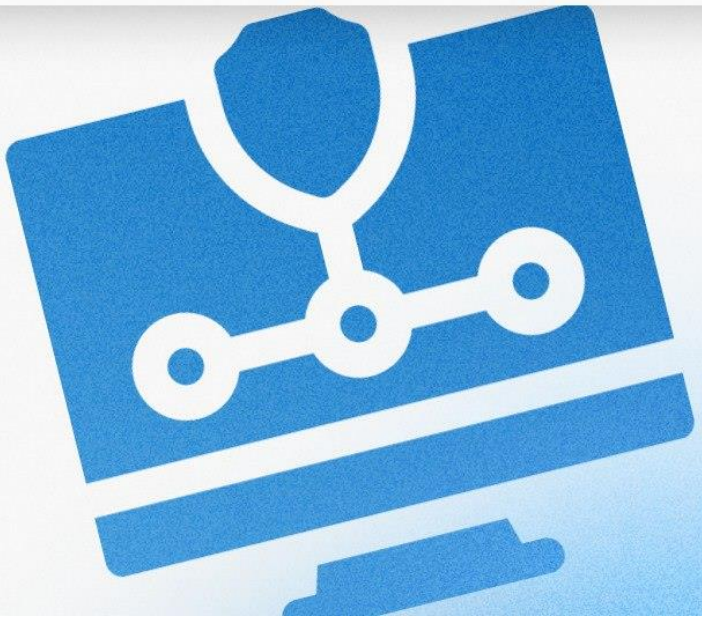

5 СОВЕТОВ ДЛЯ ЗАЩИТЫ ЛИЧНЫХ ДАННЫХ
Интернет без угроз
НЦПТИ

Подключите двухфакторную аутентификацию к личным ресурсам

Двухфакторная аутентификация предполагает ввод пароля и дополнительного кода, который вы можете получить на номер телефона, в приложении или на почту.
Это надежный барьер от злоумышленников, который усложнит им получение доступа к чужим данным.



Не переходите по подозрительным ссылкам

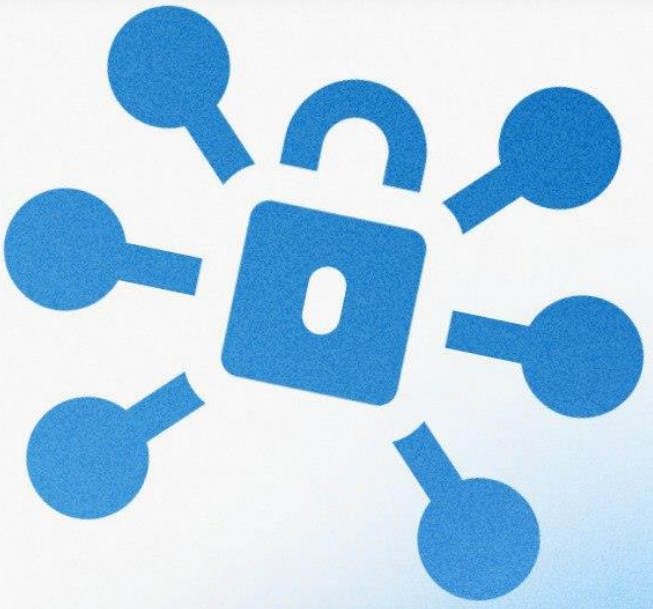
Злоумышленники используют фишинговые ссылки для кражи личных данных. **Всегда проверяйте** адресную строку. Убедитесь, что в названии сайта нет ошибок, домен сайта привычный (.ru, .com, .рф и пр.). Между доменом и названием сайта не должно быть никаких символов. Если перед вами письмо с гиперссылкой, то обратите внимание на отправителя и содержание. Если в письме есть ошибки, угрозы, заманчивые предложения – лучше проигнорировать.

Используйте сложные пароли

Пароль не должен содержать личной информации, чтобы его нельзя было подобрать: не используйте в качестве пароля ФИО или дату рождения. **Надежный пароль** должен содержать буквы, цифры и специальные символы.
Есть сервисы для генерации паролей и их хранения в зашифрованном хранилище. Также полезно периодически обновлять пароли.

Не публикуйте личные данные в социальных сетях

Помните, что все опубликованное в интернете остается в интернете. Не публикуйте фотографии паспорта, банковских карт, адрес проживания и иную чувствительную информацию. **Этим могут воспользоваться мошенники.**



Периодически чистите кэш и cookie-файлы

Файлы cookie предназначены для идентификации пользователя и сбора информации о его действиях на сайтах. Например, **сохраняют логины и пароли,** чтобы пользователю не пришлось вводить их снова. Поэтому кража файлов cookie может быть опасной, так как они могут содержать личные данные.

Не сохраняйте пароли и данные банковских карт, чистите кэш и cookie для профилактики утечки данных.