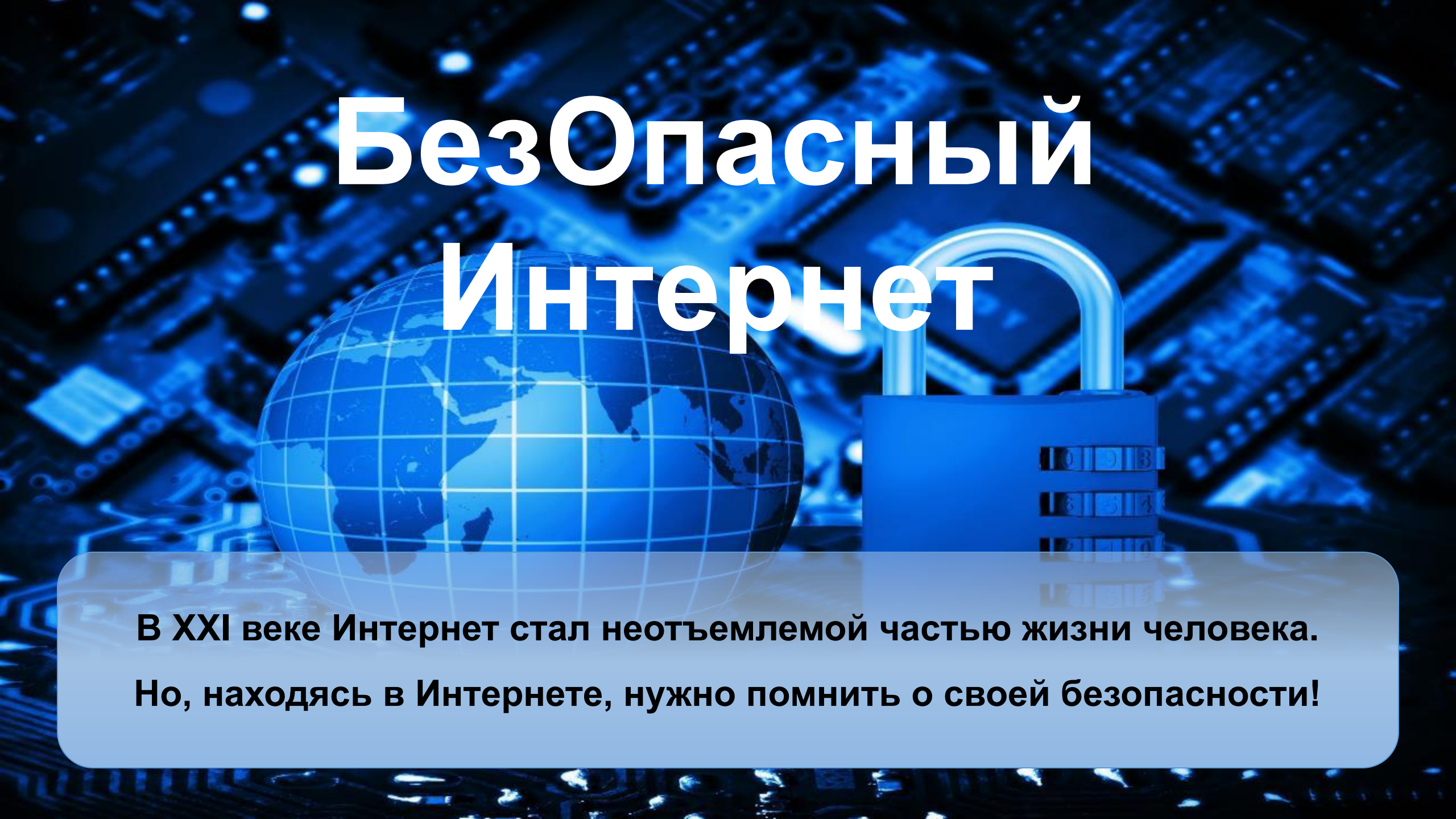


БезОпасный Интернет



**В XXI веке Интернет стал неотъемлемой частью жизни человека.
Но, находясь в Интернете, нужно помнить о своей безопасности!**

Создайте надежный пароль



Остерегайтесь бесплатного Wi-Fi



Установите хороший антивирусник



Используйте защищенные соединения



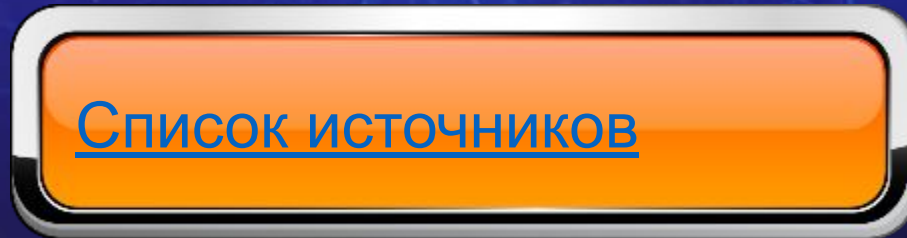
Фильтруйте информацию



Откажитесь от «пиратки»



Список источников



Пароль это основа безопасности, которой большая

ПРИНЦИПЫ СОЗДАНИЯ НАДЕЖНОГО ПАРОЛЯ: O

1 Будьте сложнее. Любые пароли, **преенебрегают** простое слово, популярную фразу или простую последовательность цифр — быстро подбираются специальными программами. А если недоброжелатель может выяснить из сети или государственных баз данных информацию о вас, то использование в качестве пароля даты рождения вас или ваших родственников, их фамилий (в т.ч. девичьих), номеров телефонов и прочей доступной информации — небезопасно.

2 Размер имеет значение. Для подбора паролей некоторые взломщики могут использовать большие компьютерные мощности. Время на подбор короткого пароля (6-8 символов) уйдет очень небольшое. Но если пароль состоит из более чем 14 символов — на его подбор могут понадобиться годы, что сделает такую задачу бессмысленной.

3 Один пароль — один сервис. Нельзя использовать один пароль одновременно для двух соцсетей, почты и любимого форума. Иначе кража этого пароля на одном из сервисов будет значить взлом всех остальных.

4 Легко запоминается, надежно хранится. Смысла в пароле, который вы забудете, будет не много. Записывать его на бумажку очень ненадежно: вам легко потерять, другим легко найти. Поэтому лучше иметь один «главный» мастер-пароль. Его лучше использовать для входа в программу хранения паролей, где вы будете хранить все остальные ключи от



НА ГЛАВНУЮ



Для защиты своего компьютера необходимо регулярное обновление программного обеспечения, использование надежных антивирусных и антишпионских программ.

Заходите в интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом. Это в разы уменьшит вероятность поймать вирус или зайти на вредоносный сайт.

Бесплатные версии наиболее популярных антивирусных программ

- 1 AVG AntiVirus Free
- 2 Avira Free Security Suite
- 3 Bitdefender Antivirus Free Edition
- 4 Comodo Internet Security
- 5 Avast Free Antivirus
- 6 Kaspersky Free
- 7 Panda Free Antivirus
- 8 360 Total Security
- 9 Sophos Home
- 10 Защитник Windows



НА ГЛАВНУЮ



Скачивайте программы либо с официальных сайтов разработчиков, либо с крупных торрент трекеров. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите риск скачать вирус вместо программы.

Пользуясь пиратскими программами, человек легко может стать жертвой киберпреступников, которые с помощью таких программ получают информацию о банковских счетах, картах и доступах к виртуальным кошелькам пользователей нелегального программного обеспечения.

Существует огромное количество бесплатных и на 100% легальных приложений, применяемых для решения широкого круга задач. Очень часто найти такие приложения значительно проще, чем искать в сети ключи и скачивать кряки, подвергая компьютер опасности.



НА ГЛАВНУЮ



Каждая соцсеть — это бесценный источник информации для злоумышленников, собирающих персональные данные, которые они затем используют для обмана и мошенничества. Поэтому так важно правильно настроить конфиденциальность вашего профиля Facebook, «ВКонтакте», «Одноклассиков» и любой другой соцсети.

При создании профилей в соцсетях люди оставляют о себе самые разные сведения: дату рождения, место проживания, родственные связи, фотографии, номер телефона и адрес электронной почты. Все эти данные могут быть использованы злоумышленниками для атаки — например, рассылки персонализированных сообщений с фишинговыми ссылками. Публикуйте онлайн фотографии ваших документов, билетов и платежных чеков. Также не стоит рассказывать о том, когда вы собираетесь уехать или уйти из дома. Эти данные очень интересуют как кибермошенников, охотящихся за чужими финансами, так и обычных домушников, ждущих, когда люди уйдут куда-нибудь надолго.

Помните о том, что для детей проблема конфиденциальности так же актуальна, как и для взрослых. Кибертравля — не миф, от нее страдают множество подростков по всему миру. Поэтому важно не публиковать посты, фото и видео, которые могут смутить ваше чадо сейчас или в



[НА ГЛАВНУЮ](#)





Не используйте открытые Wi-Fi-сети. Они могут выглядеть как вполне надежный источник Интернета, предоставленный местным кафе или даже библиотекой, но вам будет сложно отличить «добропорядочный» Wi-Fi от «зловредного». Чтобы создать такую сеть, преступнику понадобятся всего лишь ноутбук и Wi-Fi-адаптер. И мошенники действительно используют этот метод, чтобы перехватить логины и пароли пользователей, пытающихся подключиться к Интернету с помощью их Wi-Fi-сетей.

Выключайте Wi-Fi, когда им не пользуетесь. Обязательно отключите функцию автоматического подключения к Wi-Fi в вашем телефоне или планшете.

Не заходите в онлайн-банки и другие важные сервисы через открытые Wi-Fi-сети в кафе или на улице. Воспользуйтесь мобильным интернетом.

[НА ГЛАВНУЮ](#)

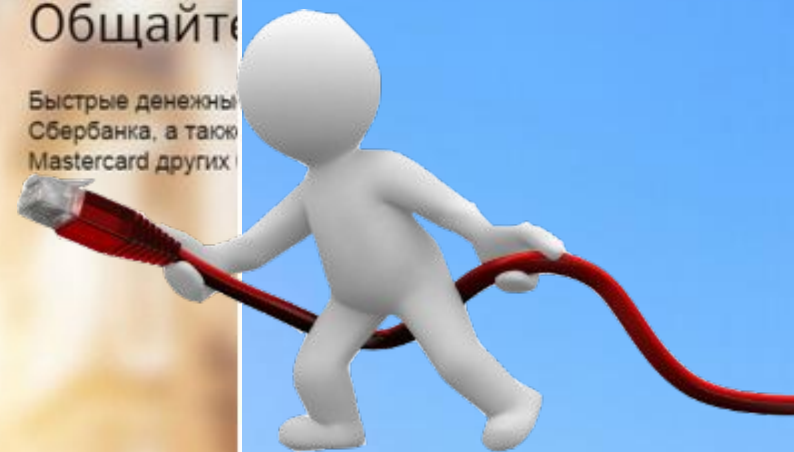
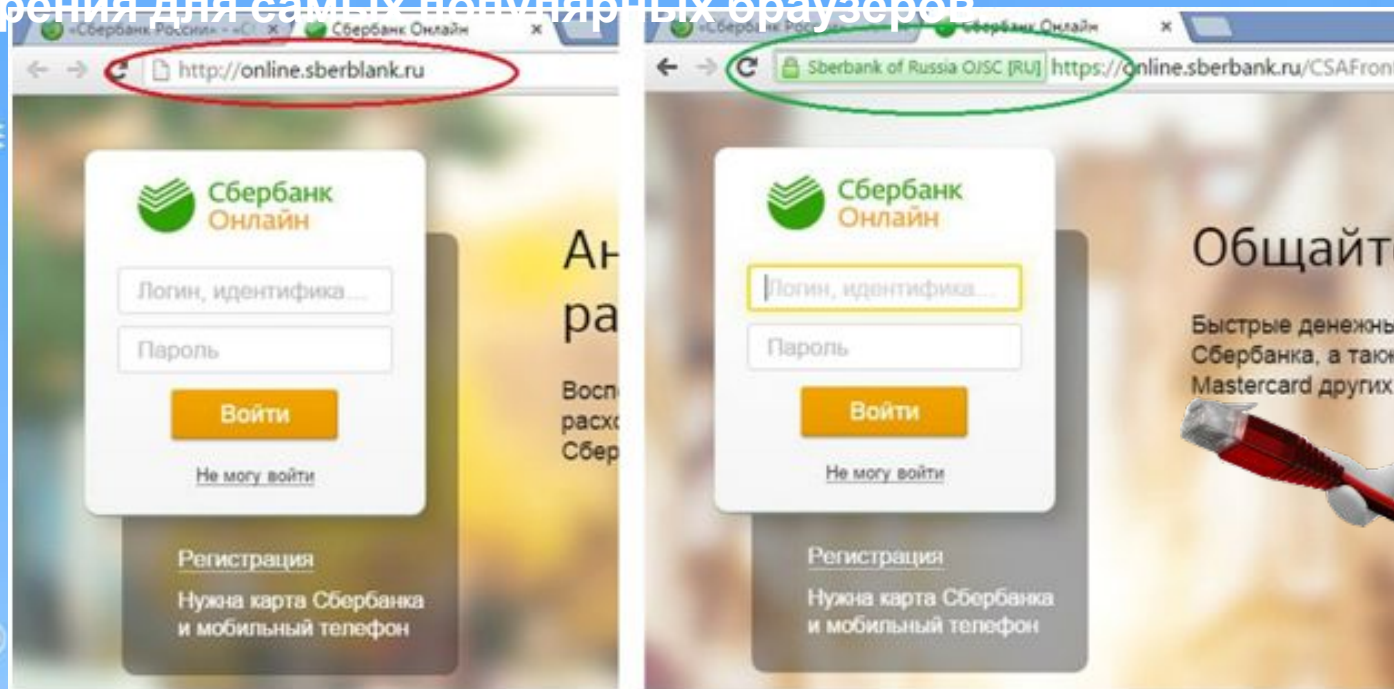


Почтовыми сервисами стоит пользоваться только с защищённым соединением. Большинство социальных сетей научилось работать с HTTPS-протоколом, на него же перешли интернет-банки и платёжные сервисы.

Совершая покупки и другие потенциально опасные действия, обратите внимание на значок слева от адресной строки. Убедитесь, что работаете с сайтом по зашифрованному соединению.

Если же работать с защищённым соединением нельзя, можно использовать специальные сервисы, например Disconnect.me. Он перенаправляет пользователя на HTTPS-версию сайта.

Ещё одно приложение, которое автоматически перенаправляет вас на HTTPS-версию, — HTTPS Everywhere. Есть расширения для самых популярных браузеров.



НА ГЛАВНУЮ

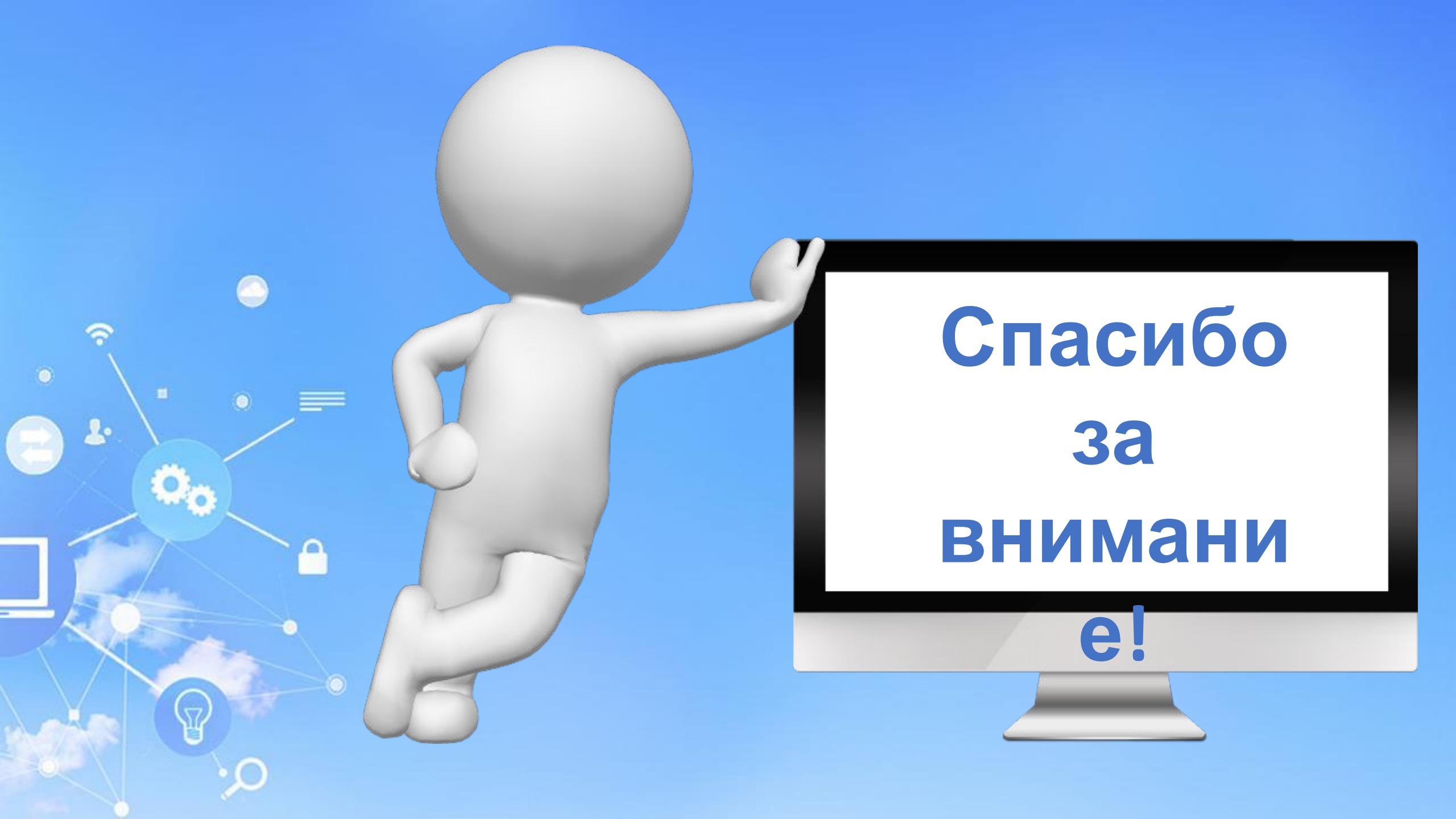


Список источников:

1. Пароли: главные в системе безопасности. Как создать и запомнить надежный пароль.
<https://hrdco.org/featured/paroli-i-ih-mesto-v-sisteme-bezopasnosti-kak-sozdat-i-zapomnit-nadezhnyj-parol/>
2. 10 лучших бесплатных антивирусов. <https://lifehacker.ru/10-luchshix-antivirusov/>
3. Как защитить личные данные в интернете: 10 советов.
<https://www.kaspersky.ru/blog/privacy-ten-tips/10390/>
4. Как защитить личные данные в интернете. <https://lifehacker.ru/protecting-your-personal-data/>

НА ГЛАВНУЮ





**Спасибо
за
внимани
е!**