Автор: Воложанин Владислав Олегович, группа 1, одргруппа 2.

Инструкция носит РЕКОМЕНДАТЕЛЬНЫЙ ХАРАКТЕР.

"Безопасный поиск информации в интернет"

Содержание:

- 1. Безопасный поиск.
- 2. Избегайте перехода по подозрительным ссылкам.
- 3. Предварительный просмотр URL-адреса.
- 4. Проверка SSL-соединения.
- 5. Всплывающие окна.
- 6. Расширения браузера.
- 7. Использование виртуальной частной сети (VPN).
- 8. Ознакомление с политикой конфиденциальности.
- 9. Будьте осторожны с личной информацией.
- 10. Регулярное обновление программного обеспечения.
- 11. Использование надежного пароля.

1. Безопасный поиск.

Включение безопасного поиска - это простой, но важный шаг для обеспечения того, чтобы результаты поиска, которые вы получаете, были подходящими и безопасными для просмотра:

- Фильтрация контента: Функции безопасного поиска, такие как в Google или Bing, отфильтровывают явный или неподходящий контент из результатов поиска.
- Настраиваемые настройки: Большинство поисковых систем позволяют вам настроить уровень фильтрации в соответствии с вашими предпочтениями, от строгого до умеренного.

2. Избегайте перехода по подозрительным ссылкам.

Переход по подозрительным ссылкам может привести к различным онлайн-угрозам, включая попытки фишинга, вредоносное ПО или мошенничество. Вот как ориентироваться в этом:

• Наведите курсор для предварительного просмотра: Наведите указатель мыши на ссылку, не нажимая на нее, чтобы просмотреть URL-адрес в строке состояния. Это может помочь вам идентифицировать вводящие в заблуждение или не соответствующие URL-адреса.

3. Предварительный просмотр URL-адреса.

Когда вы наводите указатель мыши на ссылку, фактически не нажимая на нее, большинство веб-браузеров отображают целевой URL-адрес в окне предварительного просмотра или строке состояния браузера. Это может быть очень полезно по нескольким причинам:

- Идентификация несовпадающих URL-адресов: Это позволяет вам подтвердить, что отображаемый текст ссылки соответствует фактическому URL-адресу назначения. Многие фишинговые атаки используют вводящий в заблуждение текст в гиперссылках, чтобы придать им видимость законных, поэтому наведение курсора на ссылку может раскрыть истинный адресат.
- Обнаружение подозрительных URL-адресов: Это помогает вам обнаруживать подозрительные или неожиданные URL-адреса, которые могут привести к сайтам, зараженным вредоносными программами, или фишинговым страницам. Если URL-адрес выглядит неправильно или кажется не связанным с содержимым, это признак того, что следует проявлять осторожность.

4. Проверка SSL-соединения.

Защищенное соединение SSL (Secure Sockets Layer) необходимо для обеспечения конфиденциальности и сохранности ваших данных при просмотре веб-сайтов. Вот как это проверить:

- Обратите внимание на значок навесного замка: Когда вы посещаете защищенный веб-сайт, в адресной строке вашего браузера должен отображаться значок навесного замка, часто зеленого или серого цвета, в зависимости от браузера. Нажав на этот значок, можно получить дополнительную информацию о SSL-сертификате веб-сайта.
- https:// в URL: URL веб-сайта должен начинаться с "https://" вместо "http://". Буква "s" означает, что соединение защищено и что данные, которыми обмениваются ваше устройство и веб-сайт, зашифрованы.
- Информация о сертификате: Вы можете просмотреть информацию о сертификате SSL, чтобы подтвердить подлинность веб-сайта и организации, выдавшей сертификат. Эта информация может помочь вам определить, является ли сайт законным.

5. Всплывающие окна.

Всплывающие окна могут представлять значительную угрозу безопасности, если с ними не обращаться осторожно. Вот что следует иметь в виду:

- Вредоносное ПО и фишинг: Некоторые всплывающие окна могут содержать вредоносное ПО или перенаправлять вас на фишинговые веб-сайты. Избегайте нажатия на любое всплывающее окно, которое кажется подозрительным или появляется, когда вы его не запускали.
- Используйте блокировщики всплывающих окон: Многие браузеры поставляются со встроенными блокировщиками всплывающих окон. Рекомендуется включить эти блокираторы, чтобы снизить вероятность появления нежелательной всплывающей рекламы.
- Не доверяйте нежелательным всплывающим окнам: Скептически относитесь к всплывающим окнам, в которых утверждается, что вы выиграли приз или вам нужно загрузить программное обеспечение для устранения проблемы. Это часто тактика, используемая киберпреступниками, чтобы обманом заставить вас совершить вредоносные действия.

6. Расширения браузера.

Расширения для браузера могут повысить вашу онлайн-безопасность и конфиденциальность, Например:

- Средства блокировки рекламы: Расширения для блокировки рекламы помогут вам избежать навязчивой и потенциально вредоносной рекламы, которая может содержать вредоносное ПО или вводящий в заблуждение контент.
- Средства защиты от отслеживания: Расширения защиты от отслеживания не позволяют веб-сайтам отслеживать ваше поведение в Сети, повышая вашу конфиденциальность за счет блокировки отслеживающих файлов cookie и скриптов.
- Сканеры вредоносных программ: Некоторые расширения браузера могут сканировать веб-сайты на наличие потенциальных вредоносных программ и предупреждать вас, если сайт подозрителен. Эти дополнения могут обеспечить дополнительный уровень защиты.
- Менеджеры паролей: Хотя расширения password manager напрямую не связаны с безопасностью, они могут помочь вам поддерживать надежные уникальные пароли для ваших онлайн-аккаунтов, снижая риск взлома учетной записи.

7. Использование виртуальной частной сети (VPN).

VPN - это инструмент, который может значительно повысить вашу онлайн-безопасность и конфиденциальность:

- Шифрование данных: VPN шифрует данные, передаваемые между вашим устройством и VPN-сервером. Это предотвращает перехват ваших данных в незащищенных сетях, таких как общедоступный Wi-Fi.
- Маскировка IP-адреса: VPN маскирует ваш реальный IP-адрес с помощью адреса с VPN-сервера, затрудняя веб-сайтам и онлайн-сервисам отслеживание вашей онлайн-активности.
- Доступ к контенту с ограниченным доступом: VPN позволяют вам получать доступ к контенту с географическим ограничением и веб-сайтам, направляя ваше соединение через серверы, расположенные в разных странах.
- Повышенная конфиденциальность: VPN могут помочь защитить вашу конфиденциальность в Интернете, скрывая ваши действия в Интернете от вашего интернет-провайдера (ISP) и других потенциальных шпионов.

8. Ознакомление с политикой конфиденциальности.

Прежде чем предоставлять личную информацию на веб-сайте, крайне важно понять, как будут использоваться ваши данные. Это может помочь защитить вашу частную жизнь и гарантировать ответственное обращение с вашей информацией.

- Политика конфиденциальности: Найдите ссылку на политику конфиденциальности веб-сайта, которую обычно можно найти в нижнем колонтитуле сайта. Политика конфиденциальности описывает, как ваши данные собираются, используются и защищаются веб-сайтом или сервисом.
- Сбор данных: Ознакомьтесь с разделом, посвященным сбору данных, чтобы понять, какие типы информации собирает веб-сайт. Это может включать ваше имя, адрес электронной почты, местоположение и многое другое.
- Использование данных: Изучите, как веб-сайт планирует использовать ваши данные. Делятся ли они им с третьими лицами или используют в маркетинговых целях? Убедитесь, что вас устраивает использование по назначению.
- Безопасность данных: Хорошая политика конфиденциальности также должна описывать меры, принимаемые для защиты ваших данных, включая шифрование и методы обеспечения безопасности данных.

9. Будьте осторожны с личной информацией.

Обмен личной информацией в Интернете может иметь значительные последствия для конфиденциальности и безопасности. Вот как нужно быть осторожным:

- Используйте псевдонимы: Если возможно, используйте псевдонимы или прозвища вместо своего настоящего имени на веб-сайтах или форумах, где личная информация не является существенной.
- Ограничьте публичный доступ: Будьте внимательны к тому, чем вы публично делитесь в социальных сетях. Такая информация, как ваш адрес, номер телефона и финансовые данные, не должна разглашаться открыто.

10. Регулярное обновление программного обеспечения.

Регулярное обновление программного обеспечения имеет решающее значение для поддержания безопасности устройств.

- Исправления безопасности: Обновления программного обеспечения часто включают исправления безопасности, которые устраняют уязвимости и защищают вашу систему от известных угроз.
- Автоматические обновления: Включите автоматическое обновления, чтобы убедиться, что всегда используется самые последние и безопасные версии.

11. Использование надежного пароля.

Надежные, уникальные пароли необходимы для защиты ваших онлайн-аккаунтов. Рекомендации по созданию пароля:

- Сложность: Используйте пароли длиной не менее восьми символов, содержащие сочетание прописных и строчных букв, цифр и специальных символов.
- Уникальность: Избегайте использования одного и того же пароля для нескольких учетных записей. Каждая учетная запись должна иметь свой собственный уникальный пароль.
- Менеджер паролей: Рассмотрите возможность использования менеджера паролей для создания и безопасного хранения ваших паролей. Менеджеры паролей также могут автоматически заполнять формы для входа в систему, что делает процесс более удобным.
- Двухфакторная аутентификация (2FA): Включите 2FA там, где это доступно, для дополнительного уровня безопасности. Для этого требуется, чтобы вы предоставили вторую часть информации в дополнение к вашему паролю.

Источники:

- 1. https://habr.com/ru/articles/534250/
- 2. https://habr.com/ru/companies/globalsign/articles/525290/
- 3. https://rskrf.ru/tips/eksperty-obyasnyayut/politika-konfidentsialnosti-v-c hem-podvokh/
- **4.** https://timeweb.com/ru/community/articles/kak-proverit-ssl-i-tls-sertifikat-na-sayte