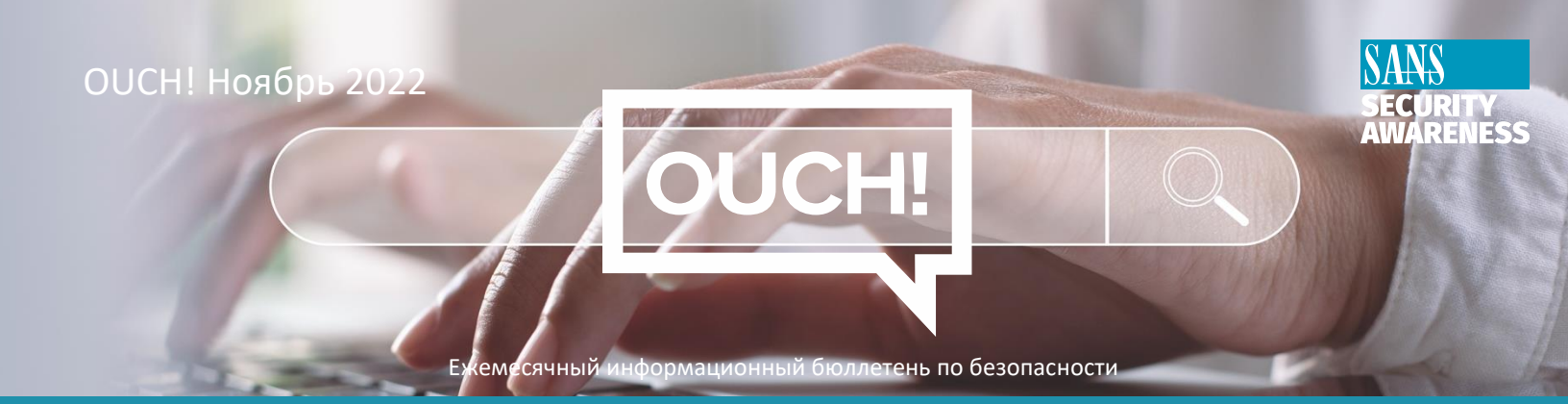

Ежемесячный информационный бюллетень по безопасности

Браузеры

Обзор

Такие браузеры, как Google Chrome, Microsoft Edge, Apple Safari или Mozilla Firefox, являются одним из наиболее распространенных способов взаимодействия людей с Интернетом. Мы используем их для чтения новостей, проверки электронной почты, покупок в Интернете, просмотра видео и игр. В результате браузеры также являются мишенью для кибератак.
Многие люди считают, что просмотр в Интернете безопасен, если вы посещаете только известные и надежные веб-сайты. Однако довольно легко случайно щелкнуть или посетить небезопасную веб-страницу, иногда даже не подозревая об этом. Кроме того, те самые веб-сайты, которые вы знаете и которым доверяете, могут быть взломаны, и кибер-злоумышленники установят на них вредоносное программное обеспечение. Наконец, современные браузеры имеют много новых функций, которые часто могут сбивать с толку, а при неправильной настройке подвергать вас еще большим опасностям.

Безопасное использование вашего браузера

Вот основные шаги, чтобы защитить себя:

Обновление: всегда используйте последнюю версию вашего браузера. Обновленные браузеры имеют последние обновления и намного более безопасны. С современными компьютерами это стало намного проще, поскольку вы просто включаете автоматическое обновление в своей системе. Или для некоторых браузеров вы просто перезапускаете браузер всякий раз, когда он сообщает вам о новом обновлении. После обновления проверьте наличие новых функций безопасности, которыми вы можете воспользоваться.

Предупреждения: современные браузеры часто могут распознавать определенные вредоносные веб-сайты, предназначенные для причинения вам вреда. Если ваш браузер предупреждает вас, что веб-сайт, который вы собираетесь посетить, опасен, закройте вкладку браузера и найдите то, что вам нужно, на другом веб-сайте.

Синхронизация: никогда не синхронизируйте рабочий браузер с личным браузером или любыми личными учетными записями. Синхронизация — это когда вы позволяете браузерам на разных устройствах взаимодействовать друг с другом и обмениваться информацией, такой как история просмотров, закладки и сохраненный контент.

Пароли: многие браузеры поддерживают возможность сохранения ваших паролей на разных сайтах. Вместо того, чтобы хранить ваши пароли в браузере, мы рекомендуем вам использовать специальный менеджер паролей. Менеджеры паролей — это отдельное приложение безопасности, которое имеет гораздо больше функций безопасности.

Подключаемый модуль: подключаемые модули или расширения — это небольшие части программного обеспечения, добавляемые в браузеры, которые могут добавлять функциональные возможности. Однако каждый новый подключаемый модуль, который вы добавляете, также может добавлять новые уязвимости. Добавляйте на рабочий компьютер только авторизованные и одобренные подключаемые модули и, как и ваш браузер, обновляйте их. Удалите плагины, которые не используются или вам больше не нужны.

Режим конфиденциальности: большинство браузеров предлагают опцию конфиденциальности (также называемую «режимом инкогнито»). Это означает, что когда вы открываете вкладку браузера в режиме конфиденциальности, вы ограничиваете сбор информации о вас. Например, ваш браузер не собирает файлы cookie, не отслеживает историю просмотров, не хранит и не распространяет конфиденциальную информацию о вас.

Живой чат: некоторые веб-сайты теперь предлагают функцию живого чата, где вы можете задавать вопросы. Участвуйте в этих онлайн-чатах только с известными и надежными веб-сайтами. Кроме того, ограничьте информацию, которой вы делитесь во время сеанса живого чата, поскольку вы понятия не имеете, кто собирает вашу информацию, что они делают с ней и кому они могут ее продавать или делиться ею.

Остерегайтесь удаленного управления: Мошеннические веб-сайты попытаются взломать ваш компьютер, опубликовав в браузере фальшивое всплывающее окно системы безопасности, предупреждающее о том, что ваш компьютер заражен, и потребовав от вас сеанса онлайн-чата, чтобы починить ваш компьютер. Затем они срочно потребуют, чтобы вы разрешили им установить программу удаленный агент, чтобы они могли починить ваш компьютер. На самом деле с вашим компьютером все в порядке. Вместо этого они пытаются обманом заставить вас установить вредоносное программное обеспечение, чтобы украсть ваши пароли и данные, а также отслеживать все ваши действия в Интернете.

Выйти из системы: когда вы закончите посещение веб-сайта, обязательно выйдите из системы, чтобы удалить конфиденциальную информацию о логине и пароле, прежде чем закрыть браузер.

Приглашенный редактор

Дин Парсонс — генеральный директор ICS Defense Force с более чем 20-летним опытом киберзащиты в сфере ИТ/ICS. Он также является сертифицированным инструктором SANS для ICS515 и соавтором / инструктором ICS418, обучая активной киберзащите, реагированию на инциденты, лидерству и управлению рисками для промышленных систем управления. www.linkedin.com/in/dean-parsons-cybersecurity.

Ресурсы

Менеджеры паролей: https://www.sans.org/newsletters/ouch/password-managers/
Сила обновления: https://www.sans.org/newsletters/ouch/the-power-of-updating
Социальный инжиниринг: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Конфиденциальность: https://www.sans.org/newsletters/ouch/privacy/

Роман Полаков