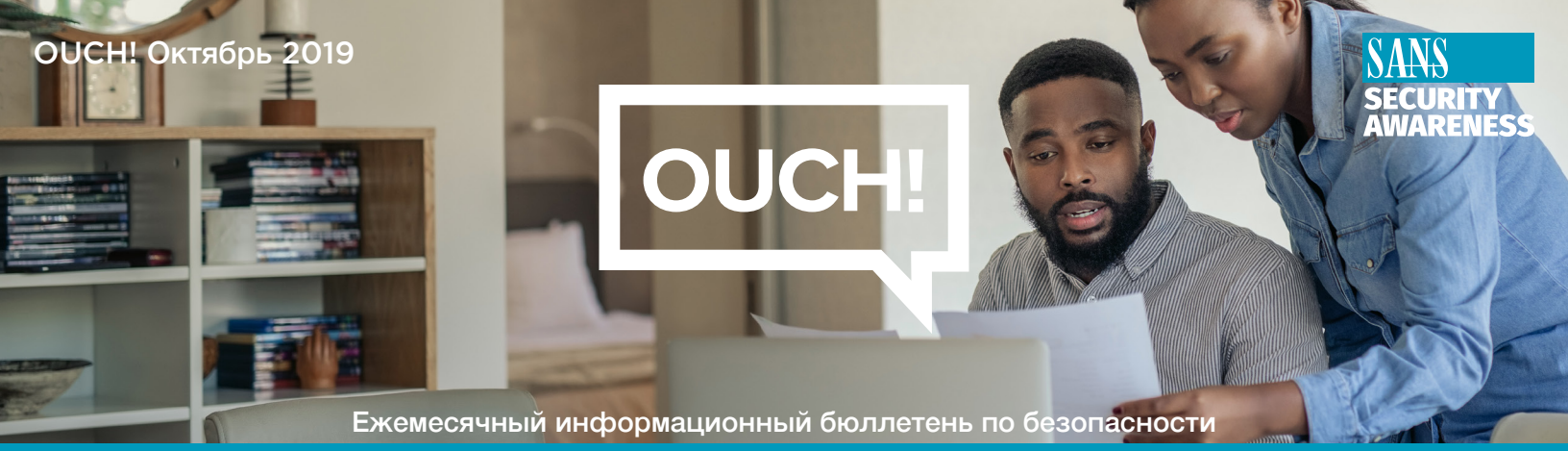
OUCH! Октябрь 2019



Ежемесячный информационный бюллетень по безопасности

Четыре простых шага к безопасности

Обзор

Использование технологии безопасно и надежно может показаться подавляющим и запутанным. Тем не менее, независимо от того, какие технологии вы используете или как вы их используете, вот четыре простых шага, которые помогут вам оставаться в безопасности.

1. Вы: В первую очередь, не одна технология сама по себе не может полностью защитить вас. Вы лучшая защита. Злоумышленники поняли, что самый простой способ получить то, что они хотят, - это нацелиться на вас, а не на ваш компьютер или другие устройства. Если они хотят получить ваш пароль, кредитную карту или контроль над вашим компьютером, они попытаются обманом заставить вас их передать, часто создавая ощущение срочности. Например, они могут позвонить вам, притворяясь технической поддержкой Microsoft, и заявить, что ваш компьютер заражен, хотя на самом деле это киберпреступники, которые хотят, чтобы вы предоставили им доступ к вашему компьютеру. Или, они отправят вам электронное письмо с предупреждением о том, что ваша посылка не может быть доставлена, и заставят вас нажать на ссылку для подтверждения вашего почтового адреса, на самом деле они выманивают вас на посещение вредоносного веб-сайта, который взломает ваш компьютер. В конечном счете, лучшая защита от злоумышленников - это вы. Используя здравый смысл, вы можете обнаружить и остановить множество атак.

2. Парольные фразы: современные скорости вычислений сделали старый 8-символьный пароль устаревшим и уязвимым. Когда сайт просит вас создать пароль, вместо этого создайте надежную и уникальную фразу-пароль. Парольная фраза - это тип пароля, который использует ряд слов, которые легко запомнить, например, «пчелиный мед бурбоновый дождь». Чем длиннее парольная фраза, тем надежнее. Используйте разные парольные фразы в сети для каждого устройства или учетной записи. Таким образом, если одна парольная фраза будет взломана, остальные ваши учетные записи и устройства будут в безопасности. Не можете запомнить парольные фразы? Используйте менеджер паролей, который представляет собой специализированную программу, которая надежно хранит все парольные фразы в зашифрованном формате (а также предлагает множество других функций).

Наконец, включите двухэтапную проверку (также называемую двухфакторной или многофакторной аутентификацией). Он использует ваш пароль, но также добавляет второй шаг, например, ввод кода, отправленного на ваш смартфон или из приложения, которое генерирует для вас код. Включение двухэтапной проверки, является наиболее важным шагом, который вы можете предпринять для защиты своих учетных записей в Интернете, и это проще, чем вы думаете.

3. Обновление: убедитесь, что на каждом из ваших компьютеров, мобильных устройств, программ и приложений установлена последняя версия программного обеспечения. Кибер взломщики постоянно ищут новые уязвимости в программном обеспечении, используемом вашими устройствами. Когда они обнаруживают уязвимости, они используют специальные программы, чтобы взломать и использовать их в своих целях. Между тем компании, создавшие программное обеспечение для этих устройств, усердно работают над устранением уязвимостей путем выпуска обновлений. Обеспечивая своевременную установку обновлений на ваших компьютерах и мобильных устройствах, им будет намного сложнее взломать вас. Для того, чтобы оставаться защищенным, включите автоматическое обновление. Это правило применяется практически ко всем технологиям, подключенным к сети, включая телевизоры, подключенные к Интернету, радионяни, камеры видеонаблюдения, домашние маршрутизаторы, игровые приставки или даже ваш автомобиль.

4. Резервное копирование и восстановление: Независимо от того, насколько вы осторожны, вас все равно могут взломать. Если это так, то единственным способом восстановить всю вашу личную информацию является резервное копирование. Убедитесь что вы регулярно делаете резервные копии любой важной информации и проверяйте, можете ли вы восстановить из них свои данные. Большинство операционных систем и мобильных устройств поддерживают автоматическое резервное копирование на внешние диски или на Cloud.

Приглашенный

Сертифицированный инструктор SANS ***Стив Энсон*** *улучшает уровень безопасности и предоставляет рекомендации для групп ИТ-безопасности и правительств по всему миру. Стив является автором новой книги Applied Incident Response и предоставляет бесплатные ресурсы для специалистов по ИТ-безопасности на* AppliedIncidentResponse.com.

Ресурсы

Социальная инженерия:	https://www.sans.org/u/Uz6
Персонализированные мошенничества:	https://www.sans.org/u/Uzb
Простые пароли:	https://www.sans.org/u/Uzg
Резервные копии:	https://www.sans.org/u/Uzl