Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

Четыре ступени безопасности

Обзор

По мере того, как технология занимает всё более важное место в нашей жизни, она становится всё сложнее. Учитывая, как быстро меняется технология, становится всё труднее уследить за новейшими рекомендациями по информационной безопасности. Каждый день появляются новые советы. Однако, хотя детали того, как обеспечить безопасность, могут меняться со временем, существуют фундаментальные вещи, которые помогут вам защитить себя. Какую бы технологию вы не использовали и где бы вы не использовали её, мы рекомендуем следующие четыре шага. Дополнительную информацию о каждом из шагов, описанных ниже, вы можете получить из статей, указанных в секции Ресурсы в конце этого выпуска.

Об авторе

Райан Джонсон – эксперт, помогающий организациям подготовиться к неизбежным инцидентам информационной безопасности. Он преподает курс Advanced Network Forensics в Институте SANS. Райан активно публикуется в Twitter как **@ForensicRJ**.

1. **Вы**: Первое и самое главное, запомните: технология сама по себе никогда не сможет полностью обезопасить вас. Злоумышленники поняли, что самый лёгкий путь обойти даже самые изощрённые технологические защиты – атаковать вас. Если им нужен ваш пароль, номер кредитной карты или ваши персональные данные, простейший способ получить эту информацию – спровоцировать вас на передачу им этой информации. Например, они могут позвонить вам и представиться сотрудниками службы поддержки компании Microsoft. Они будут уверять вас, что ваш компьютер заражен. В действительности, они являются кибер преступниками, которые хотят, чтобы вы дали им доступ к вашему компьютеру. В другом варианте, они посылают вам сообщение электронной почты, информирующее вас о том, что посылка не могла быть вам доставлена и вам необходимо подтвердить ваш почтовый адрес, перейдя по ссылке в сообщении. Сссылка перенаправит вас на инфицированный сайт, который попытается заразить ваш компьютер. Это типичный сценарий начала многих типов атак, таких как Ransomware и афера «Руководитель». Самая надёжная защита от нападения – это вы сами. Будьте начеку. Используя здравый смысл, вы сможете обнаружить и остановить большинство атак.

2. **Пароли**: Следующий шаг по обеспчению своей защиты заключается в использовании сильных, уникальных паролей для каждого из ваших устройств и учетных записей. Ключевые слова здесь – сильный и уникальный. Сильный пароль – это пароль, который не может быть легко подобран хакерами или их программами. Устали

© SANS Institute 2016

Четыре ступени безопасности

от сложных паролей, которые трудно запомнить и неудобно печатать? Попробуйте вместо них использовать парольные фразы. Вместо одного слова, используйте последовательность слов, которую легко запомнить, напроимер, «Где мой кофе?». Чем длиннее ваша парольная фраза, тем она сильнее. Уникальный пароль означает использование различных паролей для каждого из ваших гаджетов и учётных записей. В этом случае, если один из паролей скомпроментирован, вы можете быть уверены, что все остальные ваши учётные записи и гаджеты в безопасности. Вы не можете запомнить все эти сильные, уникальные пароли? Я тоже. Вот почему мы рекомендуем использовать менеджер паролей – специальную программу для вашего смартфона или компьютера, которая может надёжно и безопасно хранить все ваши пароли в зашифрованном виде.

Эти четыре шага помогут вам защить себя и позволят вам использовать новейшие технологии.

Наконец, один из самых надёжных шагов, которые вы можете предпринять для защиты любой учётной записи – включить двухступенчатую верификацию. Пароли сами по себе уже не достаточны для надёжной защиты учётных записей; нужна более сильная защита. Двухступенчатая верификация значительно сильнее. Она использует ваш пароль, но дополняет его вторым шагом, проверяя либо одну из ваших личных физических особенностей (биометрия), либо что-то, что у вас есть (например, код, высланный на ваш смартфон или приложение на вашем смартфоне, которое генерирует код для вас). Включите эту функцию на каждой учётной записи, которая поддерживает двухступенчатую верификацию – включая менеджер паролей, если возможно.

3. **Обновления**: Позаботьтесь о том, чтобы ваши компьютеры, мобильные устройства, приложения и всё остальное, подключённое к интернету, использовали последнюю версию программного обеспечения. Кибер преступники постоянно ищут новые уязвимости в программах. Как только они обнаруживают уязвимости, они используют специальные программы, позволяющие использовать эти уязвимости и взломать ваши устройства. В то же время, компании-производители программ интенсивно работают над устранением уязвимостей – они делают это, выпуская обновления. Устанавливая обновления на ваши компьютеры и мобильные устройства, вы значительно усложняете задачу тем, кто пытается взломать вас. Чтобы всегда иметь новейшие обновления, просто включите функцию автоматических обновлений везде, где это возможно. Этот совет применим почти к любой технике, подключённой к интернету, включая смарт телевизоры, детские мониторы, домашние роутеры,

© SANS Institute 2016

Четыре ступени безопасности

игровые консоли, и, в недалёком будущем, даже ваш автомобиль. Если ваши операционные системы или устройства достаточно старые и производитель не предоставляет обновлений безопасности, мы рекомендуем вам заменить их на новые, имеющие поддержку производителя.

4. **Резервные копии**: Иногда, несмотря на все предосторожности, ваши системы могут взломать. В этом случае, единственным способом, гарантирующим очистку вашего компьютера или мобильного устройства от вредоносных программ, будет полное стирание данных и переустановка системы. Кибер преступники могут даже закрыть вам доступ к вашим личным файлам, фотографиям и другой информации, хранящейся на взломанной системе. Зачастую, единственный способ спасти вашу личную информацию – восстановление из резервной копии. Периодически делайте резервные копии любой важной информации и проверяйте возможность восстановления данных из резервных копий. Большинство операционных систем и мобильных устройств поддерживают автоматическое резервное копирование. И ещё: мы рекомендуем вам хранить ваши резервные копии либо на Облаке или без подключения к сети – это защитит их от кибер преступников.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте securingthehuman.sans.org/ouch/archives.

Ресурсы

Фишинг:	https://securingthehuman.sans.org/ouch/2015#december2015
Менеджеры паролей:	https://securingthehuman.sans.org/ouch/2015#october2015
Двухступенчатая верификация:	https://securingthehuman.sans.org/ouch/2015#september2015
Паролевые фразы:	https://securingthehuman.sans.org/ouch/2015#april2015
Резервное копирование и восстановление данных:	https://securingthehuman.sans.org/ouch/2015#august2015

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис, Шерил Конли
Русский перевод: Александр Котков, Ирина Коткова

© SANS Institute 2016