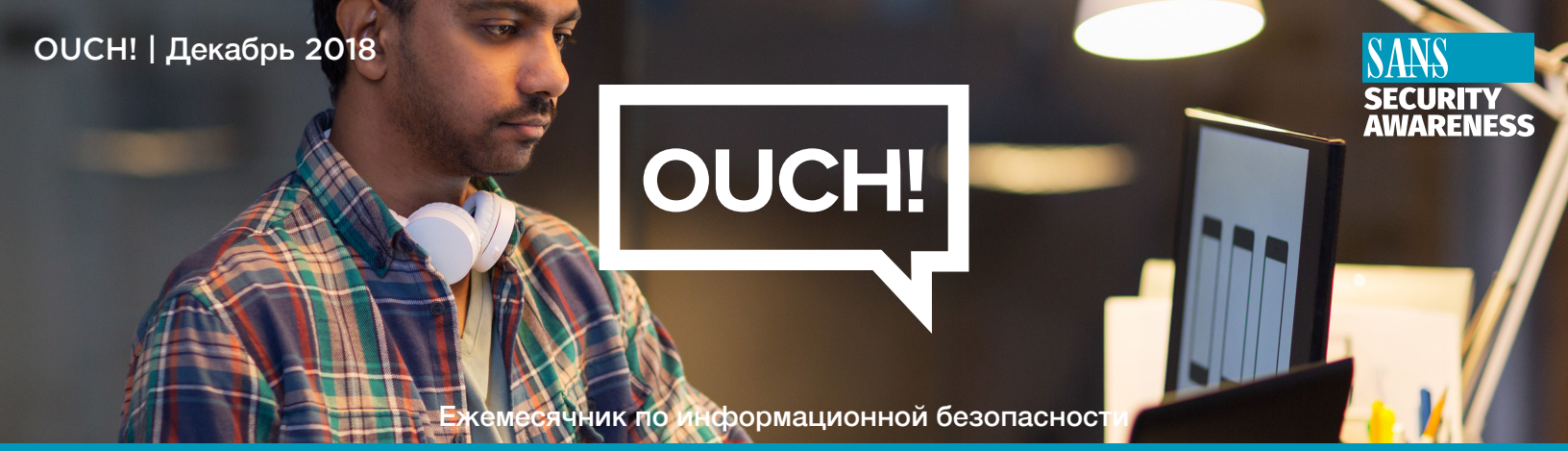

OUCH!

SANS SECURITY AWARENESS

Ежемесячник по информационной безопасности

Да, вы под прицелом

Обзор

Большинство людей ошибочно считают, что не представляют интереса для кибер мошенников, полагая, что их системы или аккаунты никому не нужны. Но такая точка зрения далека от реальности. Если вы используете технологии - неважно, дома или на работе - вы уже являетесь целью для злоумышленников. Но вам повезло. У вас есть лучшая защита от их атак – вы сами.

Почему вы являетесь целью

В наше время в интернете огромное количество мошенников, и у них могут быть разные мотивации. Почему они будут атаковать именно вас? Потому что с помощью взлома они достигают своих целей. Приведём два типичных примера киберпреступников и объясним причины, почему они интересуются вами.

⚠ **Кибер преступники:** эти парни стараются получить как можно больше денег. Интернет позволяет атаковать цель в любой точке мира простым нажатием кнопки. Существует ОГРОМНОЕ количество способов заработать на вас. Примеров много: кража денег с банковского или пенсионного счета, открытие кредитной карты на ваше имя (платить по счетам придется вам), взлом других компьютеров с помощью вашего, взлом аккаунтов социальных сетей или игровых аккаунтов и продажа этой информации другим мошенникам. Список мошеннических способов почти бесконечен. Сотни тысяч плохих парней просыпаются каждое утро с целью взломать как можно больше систем, включая вашу.

☆ **Целевое мошенничество:** это высоко квалифицированные мошенники, которые работают на правительства, преступные группировки, или на конкурентов. Вы можете думать, что ваша работа никому не интересна, но вас удивит следующее:

- **Информация, с которой вы работаете, может заинтересовать большое количество организаций или некоторые правительства.**

- **Вы можете стать целью преступников не потому, что они хотят взломать именно вас, а потому, что им нужен ваш коллега или другая система.**
- **Вы можете заинтересовать этих преступников, потому что сотрудничаете с определёнными компаниями или людьми.**

Если у меня есть антивирус, то я в безопасности

Хорошо, я являюсь целью - не проблема! Мне нужно всего лишь установить на компьютер антивирус и межсетевой экран (firewall) и я буду под их защитой, верно? Нет, не верно. Многие люди считают, что если они установят на компьютер ряд программ безопасности, то этого вполне достаточно. Это не совсем так. Кибер мошенники продолжают совершенствоваться и многие атаки могут легко преодолеть современные технологии. Например, они могут запустить вирус, который ваш антивирус не сможет обнаружить. Вашу электронную почту могут атаковать с помощью целевого фишинга или вас могут обмануть по телефону и получить номер кредитной карты, деньги или пароль. Технологии играют важную роль в защите, но лучшая защита – это вы.

К счастью, обезопаситься довольно просто: чувство здравого смысла и некоторые простые привычки - ваша лучшая защита. Если вы получили странные или подозрительные электронные письма, сообщения или звонки, которые требуют срочных действий, то это может быть атакой. Убедитесь, что ваш компьютер и устройства безопасны, используются последние версии с автоматическим обновлением. Используйте сильный и надежный пароль для каждого аккаунта. Будьте в курсе последних новостей компьютерной безопасности. Не знаете, с чего начать? Подпишитесь на ежемесячные статьи OUCH на сайте sans.org/ouch

Об авторе

Мэтт Бромили *(@mbromileyDFIR) более 8 лет занимается расследованиями киберпреступлений и координирует реагирование на кибератаки. Мэтт сотрудничает с организациями по всему миру. Он также ведёт курсы Института SANS FOR508 и FOR 572 по цифровой форенсике и реагированию на кибератаки.*

Ресурсы

Защита от вирусов:	https://www.sans.org/u/L1J
Социальная Инженерия:	https://www.sans.org/u/L1O
Телефонные атаки и мошенничество:	https://www.sans.org/u/L1T
Парольные фразы:	https://www.sans.org/u/L1Y
Ты – Цель (плакат):	https://www.sans.org/u/L23

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:* www.sans.org/security-awareness/ouch-newsletter. *Редакция: Уолт Скривенс, Фил Хоффман, Алэн Вэггонер, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова*