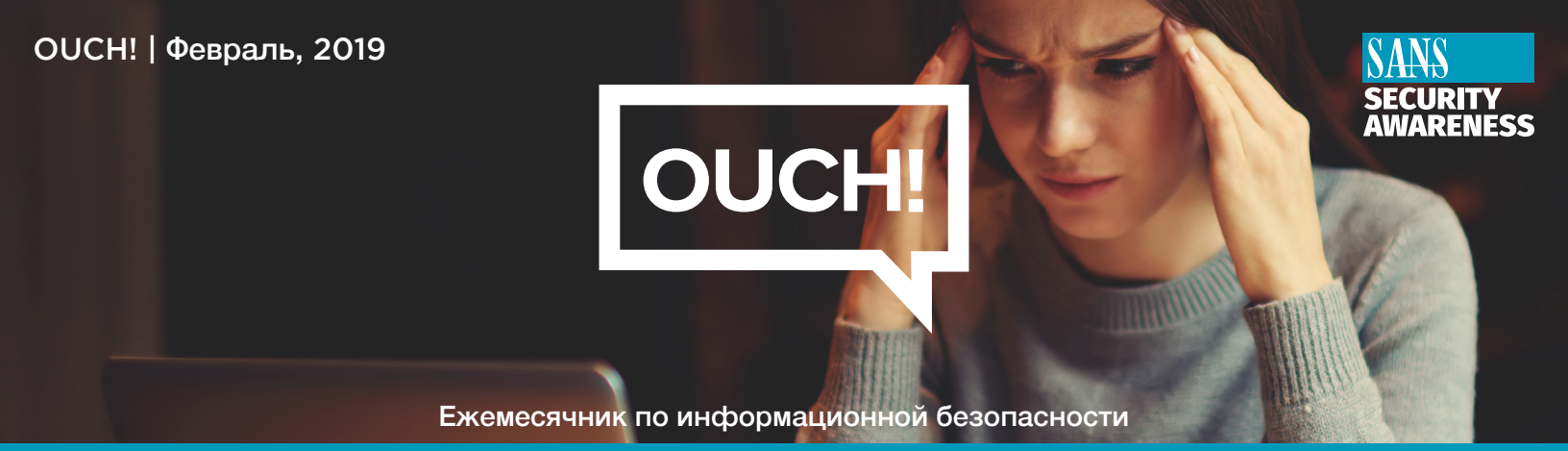
OUCH! | Февраль, 2019



Ежемесячник по информационной безопасности

Персонализированное мошенничество.

Обзор

Кибер мошенники продолжают создавать новые способы обмана людей. Растёт популярность атак нового типа: персонализированное мошенничество. Кибер преступники покупают информацию о миллионах людей, затем используют эту информацию для персонализации атак. Мы поговорим о том, как работает этот вид атак и приведём их примеры. Чем больше вы будете знать об этих атаках, тем легче будет их распознать и остановить.

Как это работает

Мошеннические письма электронной почты и телефонные звонки уже не новость, с их помощью преступники обманывают людей уже много лет. Примером могут служить письма из серии «Вы выиграли в лотерею» или «Письма от принца Нигерии». Однако, в этих традиционных видах мошенничества, кибер преступники даже не знают, кому предназначается письмо. Они просто создают шаблонное сообщение и направляют его миллионам людей. Эти попытки обмана совершенно безлики, поэтому их достаточно легко распознать. Персонализированное мошенничество отличается тем, что преступники сначала изучают своих будущих жертв, затем создают индивидуальное письмо для каждой конкретной жертвы. Они находят или покупают базы данных с именами людей, паролями, номерами телефонов или другими деталями. Все эти данные легко найти благодаря информации со взломанных сайтов. Также их можно найти в социальных сетях или государственных реестрах. Преступники затем начинают охотиться за теми, о ком они имеют достаточно информации.

Самым распространённым трюком мошенников является вымогательство денег путем запугивания или обмана. Работает это следующим образом. Они находят или покупают логины и пароли со взломанных сайтов. Затем находят в базе данных информацию о вашем аккаунте и отправляют вам (и всем остальным из этой базы данных) электронное письмо с вашими личными данными, включая пароль, который вы использовали на взломанном сайте. Мошенники отправляют вам ваш пароль как подтверждение того, что ваш компьютер или устройство взломали, что является ложью. Затем мошенники сообщают, что при взломе компьютера они поймали вас за просмотром порнографических материалов онлайн. В своем письме они вам угрожают, что распространят информацию о компрометирующей активности вашей семье или друзьям, если вы им не заплатите выкуп.

Ключевым в подобных ситуациях является то, что кибер преступники никогда не взламывали вашу систему. Они даже не знают, кто вы на самом деле и какие сайты посещали. Преступники просто пытаются использовать незначительную часть личной информации о вас, чтобы запугать и заставить поверить, что ваш компьютер или устройство взломали, и получить деньги. Помните, подобные техники преступники используют и по телефону.

Что мне делать

В первую очередь нужно рассматривать подобные письма или звонки как мошенничество. Вполне нормально чувствовать страх, если кто-то раздобыл вашу личную информацию. Но помните, что отправитель врёт. Атака является частью массовой рассылки и не нацелена конкретно на вас. В наши дни преступникам довольно легко получить или купить персональные данные, поэтому в будущем следует ожидать роста популярности подобного вида мошенничества. Ключевые признаки мошенничества:

⚠

- **Проявляйте особую осторожность с письмами или звонками, требующими немедленных действий. Если кто-то играет на чувстве страха или срочности, они подталкивают вас к совершению ошибки.**
- **Кто-то требует совершить платеж через Биткойн, подарочные карты и прочие способы, сложные для отслеживания.**
- **Если вы получили подозрительное письмо, поищите в Google отзывы других людей о подобных атаках.**

В любом случае, чувство здравого смысла - ваша лучшая защита. Следует защищать каждый свой аккаунт с помощью уникального и сложного пароля. Сложно их все запомнить? Используйте менеджер паролей. Всегда, когда это возможно, используйте двухступенчатую верификацию.

Об авторе

Ленни Зельцер *- ветеран кибербезопасности. Он создает антивирусные решения в компании Minerva Labs и читает лекции по информационной безопасности в Институте SANS. У Ленни большой опыт работы в области управляемых услуг информационной безопасности и консалтинга. Он ведёт блог zeltser.com/blog и страницу в Twitter @lennyzeltser.*

Ресурсы

Социальная Инженерия:	https://www.sans.org/u/MUU
Осторожно, фишинг!:	https://www.sans.org/u/MUZ
Что знает о тебе Интернет:	https://www.sans.org/u/MV4
Менеджер паролей:	https://www.sans.org/u/MV9

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*