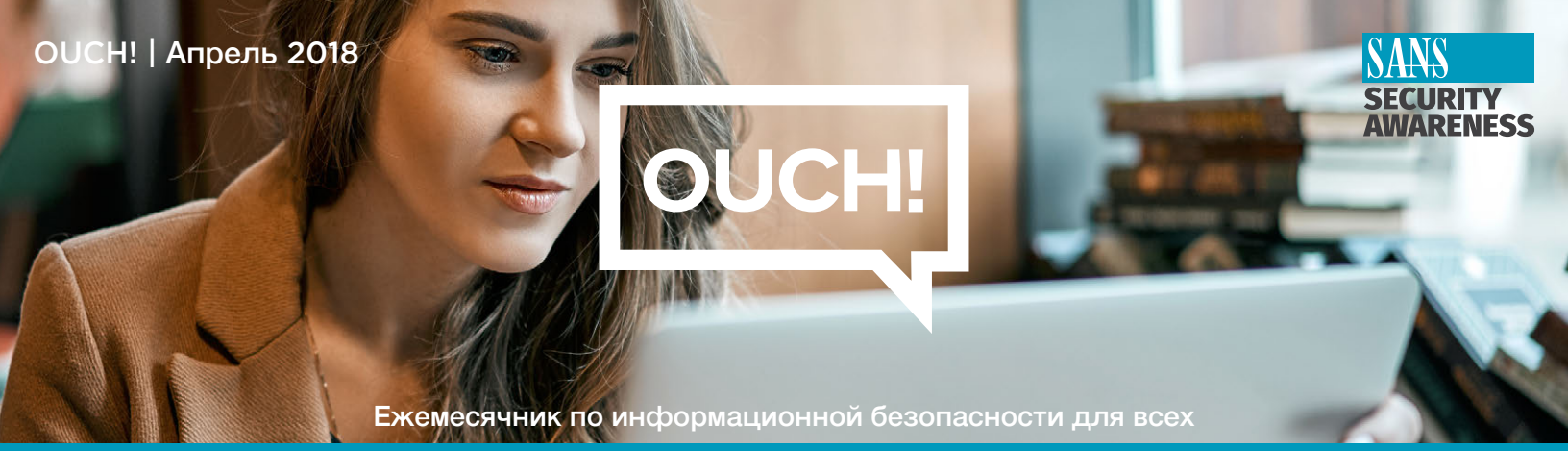

Ежемесячник по информационной безопасности для всех

Осторожно, фишинг!

Обзор

Электронная почта и службы мгновенных сообщений (например, Skype, Twitter или Snapchat) – одни из самых популярных видов связи. Мы не только используем их для работы, но и для общения с друзьями и родными. Учитывая, какое количество людей во всем мире используют данные технологии, злоумышленники направляют свои атаки именно на них, с помощью атаки «Фишинг». Давайте поговорим о том, что такое фишинг, как его распознать и остановить, независимо от того, где это происходит, на работе или дома.

Что такое фишинг

Фишинг – тип атаки пользователей через электронную почту, службы мгновенных сообщений или социальные сети, вынуждающие выполнить опасное действие обманным путём, например, перейти по заражённой ссылке, ввести свой пароль или открыть вложение с вирусами. Мошенники тщательно готовятся к атаке, стараясь задействовать ваши эмоции для достижения цели, например, создавая ощущение срочности или необычности происходящего. Они создают письма от имени чего-то или кого-то, кому вы доверяете, например, друзей или компании, с которой сотрудничаете. Злоумышленники даже могут воспользоваться логотипом вашего банка или подделать адрес отправителя для большей достоверности. Такие письма рассылаются миллионам людей. Поэтому мошенники даже и не догадываются, кто именно клюнет на наживку, просто чем больше писем они рассылают, тем больше вероятность найти жертву.

Как защитить себя

В большинстве случаев вполне безопасно открыть письмо или сообщение и просто его прочитать. Для того, чтобы атака удалась, мошенники обманным путём будут вынуждать вас к какому-либо действию. Есть несколько признаков, помогающих распознать сообщения, используемые для атаки:

- Сообщение пытается создать ситуацию чрезвычайной срочности и требует совершения действия для предотвращения нежелательного события. Например, вам могут угрожать закрытием аккаунта или тюремным заключением. Атакующие пытаются спровоцировать вас к неверному действию.
- Вас вынуждают нарушить правила или игнорировать рабочие политики и процедуры.
- Ситуация необычности, слишком хорошая новость, чтобы быть правдой (нет, вы не выиграли в лотерею).

- В письме используется общее приветствие, например, «Уважаемый клиент». Большинство компаний и друзья обращаются обычно по имени.
- У вас запрашивают слишком конфиденциальные данные, такие, как номер кредитной карты, пароли или иную информацию, которую настоящий отправитель должен знать.
- Письмо отправлено от имени официальной организации, но написано с ошибками или примитивным языком, или используется адрес бесплатных почтовых сервисов, таких как @gmail.com.
- Письмо отправлено с корпоративного адреса электронной почты (например, от имени вашего начальника), но при выборе функции «Ответить» в окне появляется адрес чьего-то личного аккаунта.
- Вы получили письмо от своего знакомого, но стиль или содержание письма совсем не похоже на отправителя. Если у вас возникли подозрения, свяжитесь с человеком, отправившим письмо, уточните, писал ли он вам. Для мошенников не составляет труда подделать письмо от друга или коллеги.

Самая лучшая защита – ваш здравый смысл. Если письмо или сообщение кажется вам странным, подозрительным или слишком хорошим, чтобы быть правдой, то, вероятней всего, вас атакуют.

Об авторе

Тоня Дадли разрабатывает и координирует программы по осведомлённости в области информационной безопасности (Security Awareness) с 2011 года, в том числе заслужившую признание программу тренинга по предотвращению фишинга. Тоню можно найти здесь: www.linkedIn.com/in/toniadudley.

Ресурсы

Социальная Инженерия:	https://www.sans.org/u/Cb1
Помощь близким – залог вашей безопасности:	https://www.sans.org/u/Cb6
Электронная почта: что нужно делать и чего делать не стоит:	https://www.sans.org/u/Cbg
Афера «Руководитель»:	https://www.sans.org/u/Cbl
OUCH! Переводы и архивы:	https://www.sans.org/u/Cbq

Лицензия

Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова