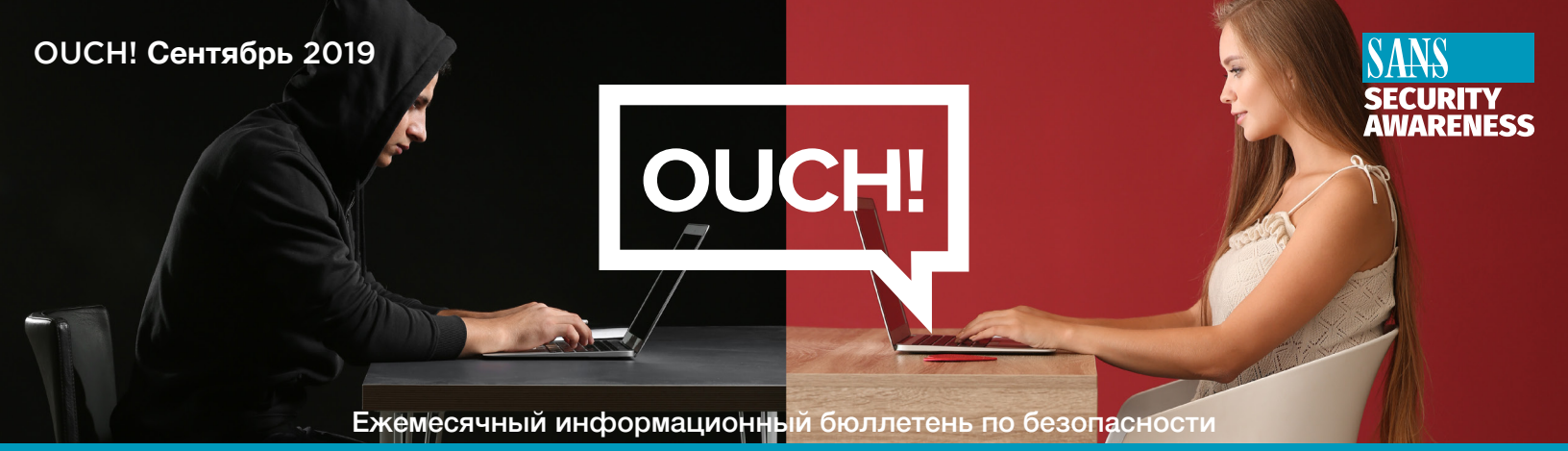
OUCH! Сентябрь 2019



Ежемесячный информационный бюллетень по безопасности

Мошенничество в социальных сетях

Обзор

Многие из нас подвергались фишинговым атакам по электронной почте, как на работе, так и дома. Это электронные письма, которые выглядят законно, например, от вашего банка, начальника или любимого интернет-магазина. Однако это атака, попытка заставить вас спешить выполнить действие, которое вы не должны делать, например, открыть зараженное вложение электронной почты, поделиться своим паролем или перевести деньги. Задача состоит в том, чем сложнее мы обнаруживаем и предотвращаем подобные атаки по электронной почте, тем больше киберпреступников пытаются использовать другие способы связи и обмана людей.

Попытки мошененечества или обмана могут случиться практически при любой форме общения, которую вы используете, от Skype, WhatsApp и Slack до Twitter, Facebook, Snapchat, Instagram или даже игровых приложений. Общение через эти платформы или каналы может показаться более неформальным или заслуживающим доверия, именно поэтому злоумышленники используют их, чтобы обмануть других. Кроме того, с современными технологиями для любого злоумышленника в любой точке мира стало намного легче притворяться кем угодно. Важно помнить, что любые сообщения, которые встречаются на вашем пути, могут быть не такими, какими они кажутся, и что люди не всегда являются теми за кого себя выдают.

Основные выводы

Вот наиболее распространенные примеры, сообщение которое вы только что получили, или сообщение, которое вы только что прочитали, могут быть атакой.

Срочность: сообщение, в котором есть чувство срочности, требующее немедленных действий до того, как произойдет что-то плохое, например, с угрозой закрыть аккаунт или отправить вас в тюрьму. Атакующий пытается торопить вас чтобы вы совершили ошибку.

Давление: заставляет вас обходить или игнорировать политику или процедуры на работе.

Любопытство: сильное чувство любопытства или что-то слишком хорошее, чтобы быть правдой. Нет, вы не выиграли в лотерею.

Конфиденциальность : запрос на получение конфиденциальной информации, такой как номер вашей кредитной карты или пароль, или любой информации, которой вы просто не можете поделиться.

Официальные сообщения: В сообщении говорится, что оно исходит от официальной организации, но имеет плохую грамматику или орфографию. Большинство государственных организаций не будут использовать социальные сети для общения с вами напрямую. Если вы не уверены, является ли сообщение легитимным, перезвоните в организацию, но используйте проверенный номер телефона, такой как номер на их веб-сайте.

Перевоплощение: вы получаете сообщение от друга или коллеги, но тон или формулировка просто не похожи на него. Если у вас есть подозрения, позвоните отправителю по телефону, чтобы убедиться, что он отправил сообщение. Кибер-злоумышленнику легко создавать сообщения от кого-то, кого вы знаете. В некоторых случаях они могут взять одну из учетных записей вашего друга, а затем притвориться вашим другом и связаться с вами. Будьте особенно бдительны о текстовых сообщениях, Twitter и других форматах коротких сообщений, которые сложнее определить личность отправителя

Вы - лучшая защита против мошенничества, обмана в подобных атак. Если почта или сообщение кажутся странными или подозрительными, просто проигнорируйте или удалите их, или если оно принадлежит кому-то, кого вы лично знаете, позвоните человеку по телефону, чтобы подтвердить, действительно ли они его отправили.

Приглашенный

Доктор Джессика Баркер *(@drjessicabarker) является лидером в области кибербезопасности. Она является со-генеральным директором Cygenta, где её задачей является следит за поведением и культурой во всем мире и положительно влиять на осведомленность о кибербезопасности. Она является председателем ClubCISO и популярным основным докладчиком.*

Ресурсы

Социальный инжиниринг:	https://www.sans.org/u/Uz6
Мошенничество по телефону:	https://www.sans.org/u/Uzb
Остановить вредоносное ПО:	https://www.sans.org/u/Uzg
Персональные атаки:	https://www.sans.org/u/Uzl