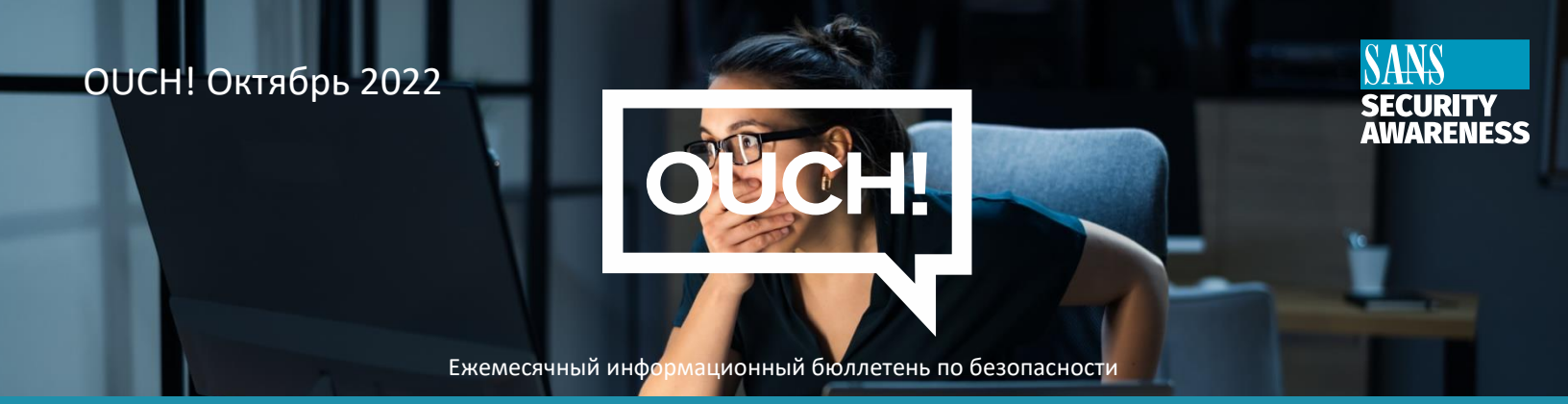
OUCH! Октябрь 2022



Ежемесячный информационный бюллетень по безопасности

Эмоциональные триггеры — как вас обманывают кибер-злоумышленники

Обзор

Кибер-злоумышленники постоянно изобретают новые способы, чтобы заставить нас делать то, что мы не должны делать, например переходить по вредоносным ссылкам, открывать зараженные вложения электронной почты, покупать подарочные карты или раскрывать наши пароли. Кроме того, они часто используют различные технологии или платформы, чтобы обмануть нас, такие как электронная почта, телефонные звонки, обмен текстовыми сообщениями или социальные сети. Хотя все это может показаться чрезвычайно, большинство этих атак объединяет одно и то же: эмоции. Зная эмоциональные триггеры, которые используют кибер-злоумышленники, вы часто можете обнаружить их атаки независимо от того, какой метод они используют.

Все дело в эмоциях

Все начинается с эмоций. Мы, люди, слишком часто принимаем решения, основываясь на эмоциях, а не на фактах. На самом деле существует целая область изучения этой концепции под названием «поведенческая экономика», возглавляемая такими исследователями, как Дэниел Ханеман, Ричард Талер и Касс Санстейн. К счастью для нас, если мы знаем, какие эмоциональные триггеры искать, мы можем успешно обнаружить и остановить большинство атак. Ниже перечислены наиболее распространенные эмоциональные триггеры, за которыми стоит следить. Иногда кибер-злоумышленники используют комбинацию этих разных эмоций в одном и том же электронном письме, текстовом сообщении, публикации в социальной сети или телефонном звонке, что делает их гораздо более эффективными.

Срочность: является одним из наиболее распространенных эмоциональных триггеров, поскольку она очень эффективна. Кибер-злоумышленники часто используют страх, тревогу, дефицит или запугивание, чтобы подтолкнуть вас к совершению ошибки. Возьмем, к примеру, срочное электронное письмо от вашего босса с требованием немедленно отправить ей конфиденциальные документы, когда на самом деле это кибер-злоумышленник, притворяющийся вашим боссом. Или, возможно, вы получаете текстовое сообщение от кибер-злоумышленника, притворяющегося правительством, информирующего вас о том, что ваши налоги просрочены, и вы должны заплатить сейчас, иначе вы попадете в тюрьму.

Гнев: вы получаете сообщение о политической, экологической или социальной проблеме, которой вы очень увлечены — что-то вроде «вы не поверите, что делает эта политическая группа или корпоративная компания!»

Сюрприз / **Любопытство**: Иногда атаки, которые являются наиболее успешными, меньше всего об этом говорят. Любопытство вызывает удивление; мы хотим узнать больше. Это реакция на что-то неожиданное. Например, кибер-злоумышленник отправляет вам сообщение о том, что посылка не доставлена, и чтобы перейти по ссылке, чтобы узнать больше, даже если вы ничего не заказывали в Интернете. Мы заинтересованы в том, чтобы узнать больше! К сожалению, посылки нет, только злой

умысел на другой стороне этой ссылки.

Доверие: злоумышленники используют имя или бренд, которым вы доверяете, чтобы убедить вас совершить действие. Например, сообщение, якобы отправленное вашим банком, известной благотворительной организацией, доверенной государственной организацией или даже человеком, которого вы знаете. Тот факт, что в электронном письме или текстовом сообщении используется название известной вам организации и ее логотип, не означает, что сообщение действительно исходит от них.

Волнение: вы получаете текстовое сообщение от вашего банка или поставщика услуг с благодарностью за своевременные платежи. Затем в текстовом сообщении содержится ссылка, по которой вы можете получить награду — новый iPad, как здорово! Ссылка ведет на веб-сайт, который выглядит официальным, но запрашивает всю вашу личную информацию или говорит, что вам необходимо предоставить информацию о кредитной карте для покрытия небольших расходов на доставку/обработку. Это кибер-злоумышленник, который просто крадет ваши деньги или вашу личную информацию.

Эмпатия / Сострадание: Кибер-злоумышленники пользуются вашей доброй волей. Например, после того, как в новостях появится информация о стихийном бедствии, они рассылают миллионы поддельных электронных писем, изображая из себя благотворительную организацию, которая помогает пострадавшим и просит у вас денег.

Лучше поняв эти эмоциональные триггеры, вы будете гораздо лучше подготовлены к обнаружению и остановке кибератак, независимо от приманки, технологии или платформы, которую они используют.

Приглашенный редактор

Май-Нгок Нгуен — генеральный директор/руководитель Secured IT Solutions. Имея 20-летний опыт работы, она имеет большой опыт управления и усовершенствования программ кибербезопасности и управления рисками как для федерального правительства, так и для частного сектора. Она привносит этот опыт в качестве сертифицированного инструктора, регулярно обучая MGT512. https://www.linkedin.com/in/menop, My-Ngoc Nguyen | SANS Institute @MenopN.

Ресурсы

Социальный инжиниринг: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Вишинг: - атаки на телефонные звонки и мошенничество: https://www.sans.org/newsletters/ouch/vishing/
Мошенничество в социальных сетях: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Текстовые сообщения /SMS фишинг: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Фишинговые атаки: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Роман Полаков