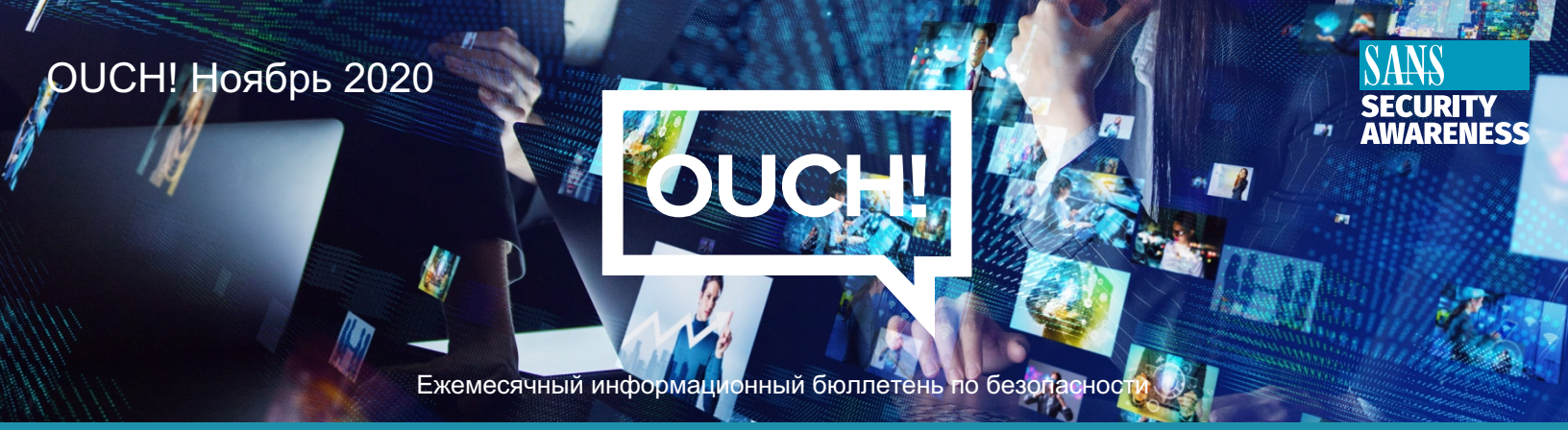
OUCH! Ноябрь 2020



Ежемесячный информационный бюллетень по безопасности

Атаки социальной инженерии

Обзор

Распространенное заблуждение о кибератаках состоит в том, что они используют только передовые инструменты и методы для взлома компьютеров или учетных записей. Кибер-злоумышленники знают, что самый простой способ украсть вашу информацию, взломать ваши учетные записи или заразить ваши системы, обманом заставляют вас сделать это за них с помощью техники, называемой социальной инженерией. Давайте узнаем, как работают эти атаки и что вы можете сделать, чтобы защитить себя.

Что такое социальная инженерия

Социальная инженерия - это психологическая атака, при которой злоумышленник обманом заставляет вас сделать то, что вы не должны делать, с помощью различных техник манипуляции. Например злоумышленник или мошенник. Кроме того современные технологии позволяют любому злоумышленнику из любой точки мира притвориться кем угодно и нацелиться на кого угодно по всему миру, включая вас. Давайте посмотрим на два реальных примера:

Вам звонит кто-то из государственной службы и сообщает, что ваши налоги просрочены и что, если вы не заплатите их сразу, вас оштрафуют или арестуют. Затем они предлагают вам заплатить по телефону кредитной картой, подарочной картой или банковским переводом, предупреждая вас, что, если вы не заплатите, вас могут посадить в тюрьму. Звонящий на самом деле не государственный служащий, а злоумышленник, пытающийся обманом заставить вас дать им деньги.

Другой пример - электронная атака, называемая фишингом. Это когда злоумышленники создают электронное письмо, которое пытается заставить вас совершить действие, например открыть зараженное вложение в электронном письме, щелкнуть вредоносную ссылку или предоставить конфиденциальную информацию. Иногда фишинговые письма носят общий характер, и их легко обнаружить, например, якобы отправленные из банка. В других случаях фишинговые электронные письма могут быть настроены и нацелены, поскольку злоумышленники сначала исследуют свои цели, например, фишинговое письмо, которое якобы отправлено вашим начальником или коллегой.

Имейте в виду, что подобные атаки социальной инженерии не ограничиваются телефонными звонками или электронной почтой; они могут происходить в любой форме, включая текстовые

сообщения, в социальных сетях или даже лично. Главное - знать, на какие признаки нужно обращать внимание.

Общие признаки атаки социальной инженерии

Здравый смысл часто является вашей лучшей защитой. Если что-то кажется подозрительным или неправильным, это может быть атакой. Наиболее частые признаки включают:

- Огромное чувство срочности. Атакующий пытается торопить вас чтобы вы совершили ошибку. Чем сильнее ощущение срочности, тем больше вероятность нападения.
- Принуждение к обходу или игнорированию политик или процедур безопасности, которым вы должны следовать на работе.
- Запросы конфиденциальной информации, к которой они не должны иметь доступа, например номера ваших счетов.
- Электронное письмо или сообщение от друга или коллеги, которого вы знаете, но сообщение не похоже на них - возможно, странная формулировка или неправильная подпись.
- Электронное письмо, которое, похоже, принадлежит коллеге или законной компании, но оно отправлено с использованием личного адреса электронной почты, например @ gmail.com.
- Игра на своем любопытстве или на чем-то слишком хорошем, чтобы быть правдой. Например, вы получаете уведомление о том, что ваша посылка был задержана, даже если вы никогда её не заказывали или что вы выиграли приз в конкурсе, в котором никогда не участвовали.

Если вы подозреваете, что кто-то пытается вас обмануть, перестаньте общаться с этим человеком. Здравый смысл часто является вашей лучшей защитой.

Приглашенный редактор

Кристиан Николсон (@GuardianCosmos) - инструктор SANS для SANS SEC560 и SANS SEC504, а также партнер/кибер-лидер в Indelible (https://indelible.global). Кристиан специализируется на безопасности приложений, Purple Teaming и автоматизации для безопасной интеграции, программирования и разработки.

Ресурсы

Мошенничество по телефону: https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams
Остановить вредоносное ПО: https://www.sans.org/security-awareness-training/resources/stop-phish
CEO Fraud / BEC: https://www.sans.org/security-awareness-training/resources/ceo-fraudbec
Персональные атаки: https://www.sans.org/security-awareness-training/resources/personalized-scams

Переведено для сообщества: Роман Поляков