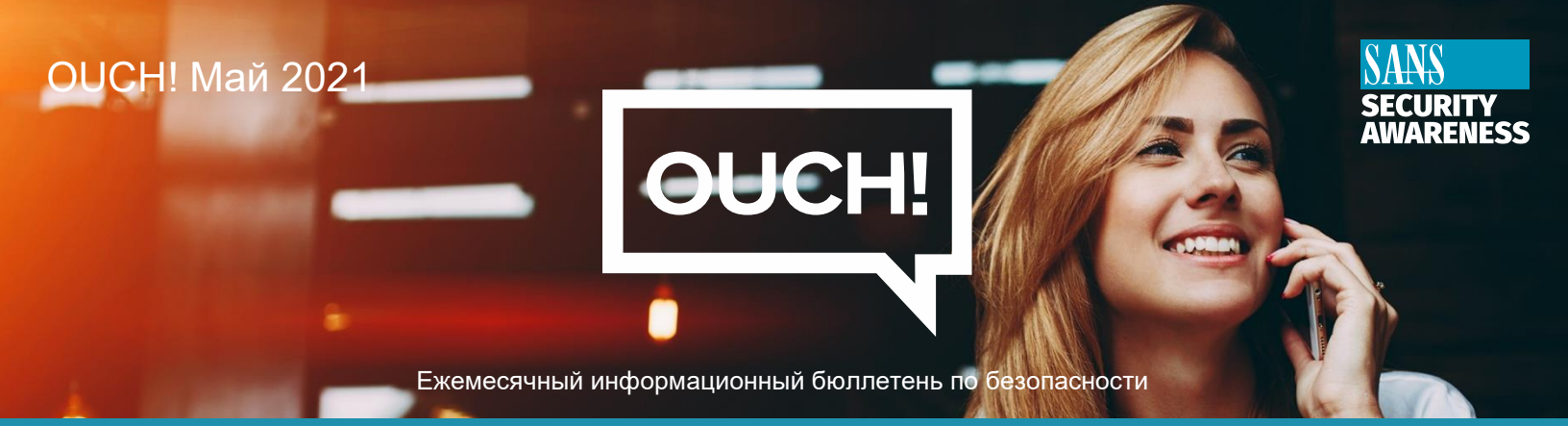
OUCH! Май 2021



Ежемесячный информационный бюллетень по безопасности

Вишинг - телефонные звонки как вид мошенничества

Обзор

Когда вы думаете о киберпреступниках, вы, вероятно, представляете себе злого вдохновителя, который сидит за компьютером и запускает изощренные атаки через Интернет. Хотя некоторые из сегодняшних киберпреступников действительно используют передовые технологии, многие просто используют телефон, чтобы обмануть своих жертв. Использование телефона дает два больших преимущества: В отличие от других атак, существует меньше технологий безопасности, которые могут обнаружить и остановить атаку по телефону; Кроме того, преступникам намного проще выражать эмоции и укреплять доверие по телефону, что упрощает обман своих жертв. Давайте узнаем, как обнаружить и остановить эти атаки.

Как работают атаки на телефонные звонки?

Во-первых, нужно понять, что преступники обычно ищут ваши деньги, информацию или доступ к вашему компьютеру (или всем трем). Они заставляют вас делать то, чего вы не должны делать, - технику под названием «социальная инженерия». Киберпреступники во время разговора часто создают ситуации, которые кажутся очень важными и реалистичными. Вот некоторые из наиболее распространенных примеров:

- Звонящий делает вид, что он представитель налоговой службы, и сообщает вам, что у вас есть неуплаченные налоги. Они объясняют, что если не заплатите налоги сразу, вы попадете в тюрьму, а затем заставляют вас заплатить налоги с помощью кредитной карты по телефону. Это мошенничество. Налоговая служба отправляет официальные уведомления только по обычной почте.
- Звонящий представляет собой представителя такой компании, как Amazon, Apple или службу технической поддержки Microsoft, и объясняет, что ваш компьютер заражен. Убедив вас, что ваш компьютер заражен, они заставят вас купить их программное обеспечение или предоставить им удаленный доступ к вашему компьютеру.
- Автоматическая голосовая почта информирует вас о том, что ваш банковский счет или кредитная карта аннулированы, и вам нужно перезвонить по номеру, чтобы повторно активировать его. Когда вы звоните, вы получаете автоматическую систему, которая просит вас подтвердить вашу личность, а также задает всевозможные личные вопросы. В действительности это не ваш банк. Они просто записывают всю вашу информацию в целях мошенничества с личными данными.

Как защитить себя?

Самая лучшая защита от атак по телефону - это вы сами. Имейте в виду следующее:

- Каждый раз, когда кто-нибудь звонит вам и вызывает сильнейшее чувство срочности или давления, будьте крайне бдительны. Они пытаются подтолкнуть вас к ошибке. Даже если сначала телефонный звонок кажется обычным, но далее начинает становиться подозрительным, вы можете остановиться и сказать «нет» в любой момент
- Будьте особенно осторожны с абонентами, которые настаивают на покупке подарочных карт или предоплаченных дебетовых карт.
- Никогда не доверяйте идентификатору вызывающего абонента. Мошенники часто подделывают номер, поэтому создается впечатление, что он исходит от законной организации или имеет тот же код города, что и ваш номер телефона.
- Никогда не позволяйте вызывающему абоненту временно контролировать ваш компьютер или заставлять вас загружать программное обеспечение. Вот так они могут заразить ваш компьютер.
- Если вы не звонили, никогда не сообщайте другой стороне информацию, которая у них уже должна быть. Например, если вам звонили из банка, они не должны спрашивать номер вашего счета.
- Если вы считаете, что телефонный звонок - это атака, просто положите трубку. Если хотите подтвердить, что телефонный звонок был законным, перейдите на веб-сайт организации (например, вашего банка) и сами позвоните по номеру телефона службы поддержки клиентов. Таким образом, вы действительно знаете, что разговариваете с реальной организацией.
- Если телефонный звонок поступает от кого-то, кого вы лично не знаете, позвольте вызову перейти непосредственно на голосовую почту. Таким образом, вы можете просматривать неизвестные звонки в удобное для вас время. Более того, на многих телефонах вы можете включить по умолчанию функцию «Не беспокоить».

Мошенничество и атаки по телефону становятся все более распространенными. Вы - лучшая защита в их обнаружении и предотвращение.

Приглашенный редактор

Джен Фокс имеет черный значок DEF CON 23 за социальную инженерию и проводит обучение по вопросам безопасности в качестве специалиста по программам безопасности в Domino’s. Найдите Джен в Twitter как @j_fox.

Ресурсы

Социальный инжиниринг: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Текстовые сообщения /SMS фишинг: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Персонализированное мошенничество: https://www.sans.org/security-awareness-training/resources/personalized-scams
Сообщить о телефонном мошенничестве (в США): https://www.reportfraud.ftc.gov

Переведено для сообщества: Роман Поляков