SANS SECURITY AWARENESS

OUCH!

Ежемесячник по информационной безопасности для всех

Телефонные атаки и мошенничество

Обзор

Когда вы думаете о киберпреступниках, вы вероятно представляете себе злого гения, сидящего за компьютером и запускающего изощренные атаки через интернет. Действительно, многие современные киберпреступники активно используют технологии, такие как электронная почта или мгновенные сообщения. Однако, преступники также часто используют телефон, чтобы обмануть своих жертв. Использование телефона даёт два преимущества. Во-первых, в отличие от электронной почты, существует меньше технических возможностей для мониторинга телефонных звонков, обнаружения и предотвращения атак. Во-вторых, по телефону значительно легче передать эмоции – это даёт дополнительные возможности для манипуляций. Давайте рассмотрим, как обнаружить и остановить эти атаки.

Как работают телефонные атаки?

Прежде всего, вам надо понять мотивацию атакующих. Обычно им нужны ваши деньги, информация или доступ к вашему компьютеру. Они добиваются своей цели путем манипуляции и убеждают вас сделать то, что им нужно. Преступники звонят людям, создавая ситуации, которые кажутся очень срочными. Они пытаются вывести вас из равновесия запугиванием, так, чтобы вы не могли спокойно анализировать ситуацию. Затем они торопят вас совершить какое-либо действие, которое навредит вам. Несколько типичных примеров:

Звонящий представляется сотрудником правительственной налоговой службы и сообщает что у вас есть задолженность по налогам. Они объясняют, если вы не заплатите налоги прямо сейчас, вас посадят в тюрьму. После этого, они вынуждают вас заплатить вашу задолженность по налогам вашей кредитной картой, по телефону. Это мошенничество. Налоговые службы никогда не звонят людям и не посылают им сообщения электронной почты. Все официальные уведомления о налоговой задолженности присылаются по почте.

Мошенники могут представиться сотрудниками Службы Технической Поддержки компании Microsoft. Они заявляют, что ваш компьютер заражен. Как только им удаётся убедить вас, что ваш компьютер заражен, они склоняют вас к покупке их антивирусной программы или к предоставлению им удалённого доступа к вашему компьютеру. Компания Microsoft никогда не будет звонить вам домой.

Вы можете получить автоматическое сообщение голосовой почты, сообщающее что ваш банковский счёт был заблокирован и вам следует перезвонить, чтобы разблокировать его. Когда вы позвоните, автоматическая система попросит вас подтвердить вашу личность и начнёт спрашивать большое количество личных вопросов. На самом деле, это не банк; они просто записывают всю вашу информацию с целью «кражи личности».

Как защитить себя

Самая лучшая защита против телефонных атак – это вы сами. Имейте в виды следующее:

Каждый раз, когда кто-то звонит и пытается создать ситуацию срочности, вынуждая вас что-либо сделать, будьте очень осторожны. Даже если телефонный звонок поначалу выглядит нормально, но затем становится подозрительным, вы в любой момент можете остановиться и сказать «Нет».

Если вы думаете, что телефонный звонок является атакой, просто повесьте трубку. Если вы хотите удостовериться, что звонок был легитимным, откройте веб страничку этой организации (например, вашего банка), найдите телефон службы поддержки клиентов и позвоните им сами. Таким образом, вы будете уверены в том, что вы говорите с настоящей организацией.

Никогда не доверяйтесь информации, предоставляемой функцией определения номера телефона (Caller ID) – преступники часто имитируют номер звонящего, так, что он выглядит как номер настоящей организации или имеет тот же код города, как и ваш телефонный номер.

Никогда не позволяйте звонящему осуществлять удалённое подключение к вашему компьютеру или склонить вас к загрузке и установке каких-либо программ. Это позволит преступникам инфицировать ваш компьютер.

Если звонящий вам не известен лично, дайте им возможность оставить сообщение голосовой почты. В этом случае, вы сможете прослушать звонки от незнакомцев в удобное для вас время. Если ваш телефон имеете функцию «Не беспокоить» (Do Not Disturb), используйте её для предотвращения нежелательных звонков.

Количество мошеннических схем и телефонных атак растёт. Вы и только вы являетесь лучшей защитой от них.

Об авторе

Джен Фокс ((Jen Fox) *работает старшим консультантом по информационной безопасности компании All Covered. Она занимается оценкой рисков, а также вопросами противодействия атакам, использующим социальную инженерию. Джен ведет страничку Twitter @j_fox.*

Ресурсы

Информация для потребителей: Личность, приватность и безопасность в интернете:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security

Сообщите о телефонном мошенничестве (США):	https://www.ftccomplaintassistant.gov/#crnt
Социальная инженерия:	https://www.sans.org/u/Fi5
Телефонные аферы:	http://www.vseafery.ru/telefonnye-afery/blog
Мошенничества и аферы с сотовыми телефонами:	http://www.aferizm.ru/moshen/m_sotovye.htm

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. *Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь:* www.sans.org/security-awareness/ouch-newsletter. *Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова*