Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

Мошенничество «Телефонный звонок из службы Технической Поддержки»

ОБ АВТОРЕ

Мы пригласили Ленни Зельцера написать материал для этого выпуска нашего ежемесячника. Ленни занимается защитой информационной безопасности в корпорации NCR и преподает методики борьбы с вредоносными программами в Институте SANS. Ленни ведёт записи в Twitter как @lennyzeltser и публикует блог по информационной безопасности blog.zeltser.com.

ВВЕДЕНИЕ

Многие кибер атаки, организованные преступниками, осуществляются с целью получения ваших денег или личных данных. Типичным примером этого являются мошеннические сообщения электронной почты («фишинг»), которые якобы приходят от человека или компании, вызывающим доверие, например, от вашего друга или банка. Помимо атак с использованием электронной почты, преступники совершают атаки на потенциальную жертву и с помощью телефонных звонков. В этом выпуске мы расскажем, как происходят такие телефонные аферы, в частности, мошенничество «Телефонный звонок из службы Технической Поддержки» и что вы можете предпринять для своей защиты.

МОШЕННИЧЕСТВО

Нужно помнить, что нет абсолютно идентичных афер, однако, они часто включают в себя элементы, которые мы обсудим в данной статье.

Вам звонит человек и представляется сотрудником компании, связанной с Microsoft, или другой известной компанией. Он утверждает, что у Вашего компьютера аномальная активность в сети, например, сканирование интернета. Это означает, что он заражён вирусом. Вам предлагают помочь обезвредить вирус в компьютере. Затем, используя большое количество технических терминов, Вас окончательно сбивают с толку и вынуждают приобрести их продукт.

Прежде всего, мошенники могут попросить загрузить и установить программу с их сайта или использовать интернет сервисы. Эти сервисы обеспечат возможность удалённого доступа к вашему компьютеру для диагностирования проблемы. Эти сервисы, как правило, предоставляют обычные услуги удаленного доступа, например, LogMeIn.com или ShowMyPC.com и, скорее всего, не будут замечены вашей антивирусной программой. Общаясь с Вами по телефону, мошенник будет устанавливать и настраивать различные программы на Вашем компьютере. Собеседник будет

Мошенничество «Телефонный звонок из службы Технической Поддержки»

убеждать Вас, что он или она предпринимает меры по обнаружению вирусов, которые якобы есть на вашем компьютере. Мошенник может даже начать отключать стандартные функции и программы, которые есть на всех компьютерах с Windows, утверждая, что эти программы вредоносные. Приводя Ваш компьютер в нерабочее состояние, злоумышленники пытаются запугать вас, внушить, что компьютер сильно пострадал от вирусов и только приобретение их продукции или дорогостоящая подписка на обслуживание может решить эту проблему.

Помните, все, что вам говорят эти мошенники, ложь. Не попадайтесь на такие уловки. Причина, по которой преступники используют телефон, а не электронную почту, в том, что практически не существует технологий для защиты от такого рода мошенничества. Кроме того, телефонный звонок дает преступникам больше возможностей для передачи эмоций и иллюзии срочности, увеличивая их шансы обмануть Вас.

Таким образом, лучшая защита от подобных атак не технология, а Вы сами.

Будьте предельно осторожны, если кто-либо по телефону попросит Вас предоставить удаленный доступ к Вашему компьютеру или вынуждает Вас к покупке программ защиты компьютера. Такие телефонные звонки практически всегда являются мошенничеством.

СПОСОБЫ ЗАЩИТЫ

Иногда официальные компании, услугами которых Вы пользуетесь, например, банк или кредитная компания, могут позвонить для подтверждения данных вашего счета или совершённой операции. Задача состоит в том, чтобы отличить реальный звонок от звонка мошенников. Приводим несколько ключевых правил:

- Если кто-то хочет получить от вас информацию по телефону или просит совершить какие-то действия, проявите бдительность и установите личность собеседника. Спросите про компанию, в которой они работают. Если вы никогда о такой компании не слышали, очень вероятно, что это атака. Если компания известна вам, то скажите, что Вам сейчас неудобно говорить, уточните должность, имя, фамилию сотрудника и скажите, что свяжетесь позже. Затем зайдите на сайт этой компании или используйте данные, которые у Вас уже есть и перезвоните в эту организацию.
- Если собеседник создает иллюзию срочности, и вас вынуждают действовать немедленно, то, скорее всего, это мошенничество, не верьте.

Мошенничество «Телефонный звонок из службы Технической Поддержки»

- Не полагайтесь только на определитель номера для идентификации абонента. Преступники легко могут обмануть определитель номера или сделать так, что определится номер настоящей организации, хотя реально они звонят с другого номера.
- Никогда не давайте свой пароль по телефону. Ни одна организация не имеет права запрашивать Ваш пароль.
- Никогда не предоставляйте сотрудникам организации информацию, которая у них уже есть. Например, если звонят из банка, то номер вашего счета у них уже есть.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Некоторые ссылки были сокращены для удобства чтения с помощью сервиса TinyURL. Для повышения безопасности OUCH! всегда использует функцию предварительного просмотра TinyURL, которая показывает вам настоящий адрес, на который будет переадресована ссылка и запрашивает ваше разрешение для перехода по ней.

Запись реального мошенничества «Звонок из службы Технической Поддержки»:
http://preview.tinyurl.com/cbg9kku

Microsoft о мошенничестве «Звонок из службы Технической Поддержки»:
http://preview.tinyurl.com/cxpwkc9

Symantec о мошенничестве «Звонок из службы Технической Поддержки»:
http://preview.tinyurl.com/244raev

Сообщение о мошенничестве (США):
https://www.ftccomplaintassistant.gov

Обзор ISC о мошенничествах «Звонок из службы Технической Поддержки»:
https://isc.sans.edu/reportfakecall.html

Словарь по информационной безопасности Common Security Terms:
http://preview.tinyurl.com/6wkpae5

Ежедневные советы SANS по безопасности:
http://preview.tinyurl.com/6s2wrkp

Управление К МВД России:
http://www.mvd.ru/projects/attention/

Фишинг:
http://ru.wikipedia.org/wiki/Фишинг

УЗНАЙ БОЛЬШЕ

Подпишись на ежемесячную рассылку OUCH! по вопросам компьютерной безопасности для пользователей, просмотри архивы OUCH! и узнай больше о решениях в области компьютерной безопасности SANS, посетив наш сайт:
http://www.securingthehuman.org.

Наши авторы: Билл Уайман, Уолт Скривенс, Фил Хоффман, Ланс Спицнер, Кармен Рael Харди.
Перевод: Александр Котков