Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Что такое Фишинг
- Способы защиты

Фишинг: атаки по электронной почте

ОБ АВТОРЕ

Питер Даникс – автор этого выпуска. Питер работает в BAE System Detica, Австралия (www.baesystemsdetica.com.au), он также является инструктором Института SANS, читает курс по выявлению взлома.

ОБЗОР

В современной жизни электронная почта является одним из приоритетных способов коммуникаций. Мы пользуемся электронной почтой не только на работе, но и для общения с друзьями и членами семьи. Кроме этого, многие компании предоставляют ряд услуг через почту, например, он-лайн покупки или электронные банковские платежи. Так как огромное количество людей зависят от электронной почты, атаки на электронную почту стали одним их излюбленных приёмов кибермошенников. В данной статье мы поговорим о наиболее распространённых видах атак и способах защиты.

ЧТО ТАКОЕ ФИШИНГ

Изначально фишингом называли попытки получить банковский счет и пароль по электронной почте. Теперь под этим термином подразумевают любые атаки по электронной почте. Фишинг атаки осуществляются с помощью социальной инженерии, при которых киберпреступники обманными способами вовлекают вас в действие. Чаще всего кибермошенники рассылают письма от имени того, кого вы знаете или чему доверяете, например, друзей, вашего банка или интернет-магазина. В этих сообщениях вас просят перейти по ссылке, открыть вложения или ответить на ряд вопросов. Такие письма выглядят очень правдоподобно, мошенники рассылают их миллионам людей по всему миру. У преступников нет определённой цели, то есть желания обмануть конкретного человека. Просто чем больше таких писем они отправят, тем выше вероятность найти жертву. Можно выделить четыре основных направления фишинга:

- **Сбор информации:** преступники обманным путём вынуждают вас перейти по ссылке. Перейдя по ней, вы попадёте на фальшивый сайт, который запрашивает логин и пароль или, как вариант, номер кредитной карты и ПИН код. Такие сайты выглядят очень правдоподобно, практически

© The SANS Institute 2013

Фишинг: атаки по электронной почте

идентичны сайту вашего банка или магазина, но созданы для сбора конфиденциальной информации.

- **Заражение вашего компьютера через вредоносную ссылку:** как и в предыдущем случае, преступники обманом вынуждают вас перейти по ссылке. Однако их не интересует конфиденциальная информация, они пытаются заразить компьютер. Если вы перейдёте по ссылке, то попадёте на сайт, который по умолчанию запустит атаку и, скорее всего, инфицирует вашу систему.
- **Заражение вашего компьютера через вредоносные вложения:** такого рода письма содержат вредоносные вложения, например, в виде зараженных PDF файлов или документов Microsoft Office. Если вы откроете эти вложения, вирусы атакуют компьютер, в результате чего преступники получат полный контроль над вашей системой.
- **Аферы:** попытки преступников обмануть вас. Классические примеры такого обмана: сообщение о выигрыше в лотерею, сбор пожертвований пострадавшим от недавней стихии, просьба помочь перевести миллионы чиновнику в вашу страну за вознаграждение. Не верьте, это обман, попытки злоумышленников получить ваши деньги.

СПОСОБЫ ЗАЩИТЫ

В большинстве случаев простое открытие письма не опасно. Для запуска большинства атак нужно произвести действие, например, открыть вложение, перейти по ссылке или сообщить требуемую информацию. Вот некоторые советы по выявлению фишинг атаки:

Если письмо кажется странным или слишком хорошим, чтобы быть правдой, то, скорее всего, вас атакуют

- Относитесь с подозрением к любым письмам, требующим незамедлительных действий или создающим иллюзию срочности. Это классическая уловка преступников, в спешке люди чаще ошибаются.
- С осторожностью относитесь к письмам, адресованным «Уважаемому клиенту» или содержащим другие общие фразы. Если это письмо от вашего банка, то они наверняка знают ваше имя.
- Грамматические ошибки тоже должны вас насторожить: серьёзные компании всегда тщательно проверяют письма перед отправкой.
- Не переходите по указанной ссылке, а скопируйте её из письма и вставьте в браузер. Или наберите имя адресата в адресной строке.

© The SANS Institute 2013

Фишинг: атаки по электронной почте

- Наведите курсор мыши на ссылку, и вы увидите, куда она ведёт на самом деле. Если адреса не совпадают, то это обман.
- Будьте осторожны с вложениями, открывайте только те, которые ждали
- То, что вы получили письмо от друга, не означает, что он действительно его отправлял. Возможно, компьютер друга заражен вирусами или его аккаунт взломали и рассылают вирусы всем из адресной книги. Если вы получили письмо от друга или коллеги, которым доверяете, позвоните им, чтобы убедиться, что они действительно отправляли письмо. Всегда звоните по номеру телефона, который есть у вас или вы можете узнать, а не указанному в письме.

Если прочитав письмо, вы понимаете, что это фишиг атака или спам, просто удалите это письмо. Использование электронной почты безопасно, если пользоваться здравым смыслом. Помните, что если что-то в письме кажется подозрительным или слишком хорошим, чтобы быть правдой, то, скорее всего, вас атакуют. Просто удалите это сообщение.

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.

Фишинг –
http://ru.wikipedia.org/wiki/Фишинг
Что такое фишинг? –
http://www.microsoft.com/ru-ru/security/online-privacy/phishing-scams.aspx
Безопасность в Интернете - Фишинг
http://www.google.com/intl/ru/goodtoknow/online-safety/phishing/
Рапознание фишинговых атак:
http://preview.tinyurl.com/3c2axs8
Услуга OpenDNS защиты от фишинга:
http://www.opendns.com/phishing-protection
OnGuard Online -
http://www.onguardonline.gov/phishing
Термины информационной безопасности:
http://preview.tinyurl.com/6wkpae5
Ежедневные советы Института SANS по информационной безопасности:
http://preview.tinyurl.com/6s2wrkp

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.

OUCH! издается в рамках программы SANS «Защита Человека» и распространяется по лицензии Creative Commons BY-NC-ND 3.0. Распространение данного журнала разрешено при следующих условиях: наличие ссылки на источник, содержание не может быть изменено и не может использоваться в коммерческих целях. Для перевода и получения дополнительной информации, пожалуйста, свяжитесь с нами: ouch@securingthehuman.org

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