Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

Фишинг

Обзор

Электронная почта в современном мире – наиболее популярный способ общения. Мы ей пользуемся не только для работы, но и для общения с друзьями и членами семьи. Кроме того, электронная почта необходима для онлайн покупок или электронных банковских платежей. Огромное количество людей во всем мире зависит от электронной почты. Это делает её очень привлекательной для атак кибер мошенников. В этом выпуске мы поговорим о таком явлении как фишинг – наиболее распространенном методе атак через электронную почту, и возможных способах защиты электронной почты.

Об авторе

Доктор Ланс Хэйден – Управляющий Директор компании Berkeley Research Group. Ланс глубоко знаком с культурой и поведенческими аспектами информационной безопасности. Он написал книгу People-Centric Security: Transforming Your Enterprise Security Culture (издательство McGraw-Hill). У Ланса есть страничка **www.linkedin.com/in/drhayden**.

Фишинг

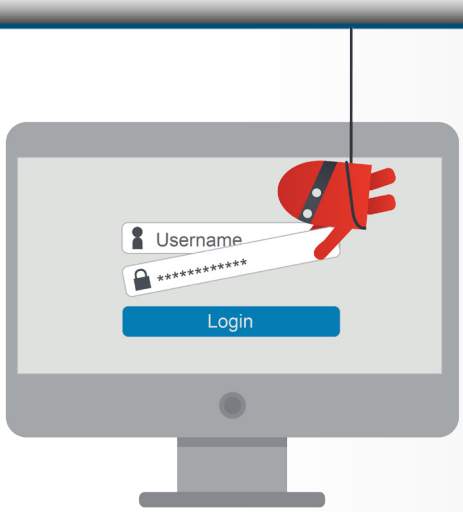
Под фишингом понимаются различные атаки через электронную почту или мессенджер, которые обманным путем заставляют вас совершить действие, например, открыть вложение или перейти по ссылке. Целью подобных атак является кража конфиденциальной информации или заражение компьютера вирусами. Мошенники прикладывают много усилий для создания правдоподобных писем. Например, письмо может быть отправлено от имени кого-то или чего-то знакомого вам, например, от имени вашего друга или компании, услугами которой вы пользуетесь. Они даже могут использовать известный логотип банка или подделать адрес отправителя, что делает письмо очень правдоподобным. Злоумышленники рассылают эти письма миллионам людей. Они не знают, кто станет их жертвой, но они знают, что чем больше писем отправят, тем больше у них шансов на успех. Фишинг подобен ловле рыбы сетью: вы не можете знать, сколько рыбы поймаете, но чем больше у вас сеть, тем больше улов. Вот некоторые виды атак:

- **Сбор информации**: Целью мошенников является сбор данных, таких, как пароли, номера кредитных карт или детали банковских счетов. Поэтому такие письма содержат ссылку на фальшивый сайт, который очень достоверно выглядит. На сайте вас просят ввести пароль и логин аккаунта или другие конфиденциальные данные. Помните, что сайт фальшивый и все данные попадают к мошенникам.
- **Инфицированные ссылки**: Кибер мошенники хотят получить контроль над вашим устройством.

Фишинг

Чтобы его получить, они отправляют письмо, содержащее ссылку. Если вы по ней перейдёте, то попадёте на сайт, который начнет атаковать ваше устройство и заразит вирусами.

- **Инфицированные вложения**: Цель мошенников такая же, заразить устройство вирусами и получить над ним контроль. Но в отличие от предыдущего способа атака производится с помощью вложения, а не ссылки, например, документа Word. Если вы откроете вложение, то преступники получат контроль над вашей системой.
- **Афёра**: Некоторые письма просто попытка мошенников обмануть вас виртуально. Вам говорят, что вы выиграли в лотерею, просят сделать пожертвования или помочь обналичить миллион долларов. Если вы поведётесь на один из этих трюков, то следующим шагом будет указание оплатить услугу или сообщить реквизиты банковского счета для перевода денег, то есть вы лишитесь своих сбережений.



Ваша лучшая защита – здравый смысл. Если письмо или сообщение странное, подозрительное или слишком хорошее, чтобы быть правдой, то, скорее всего, это фишинг атака.

Способы защиты

Во всех перечисленных способах чтение электронного письма или сообщения не представляет опасности. Чтобы фишинг атака сработала, необходимо произвести какое-либо действие. К счастью, есть ряд признаков, по которым легко распознать фишинг атаку, вот некоторые из них:

- Письмо требует незамедлительных действий, иначе что-то случится, например, ваш аккаунт закроют. Злоумышленники используют «ситуацию срочности» чтобы вы совершили ошибку, и у вас не было времени на размышление.
- Вы получили письмо с вложениями, которое не ждали или вас просят открыть это вложение. Например, в письме может говориться о том, что это детали вашего увольнения, повышения заработной платы или это штраф из налоговой инспекции.
- В письме не указывается ваше имя, а используется общее обращение «Уважаемый Клиент». Большинство ваших друзей или компаний-партнёров знают ваше имя и фамилию.
- В письме запрашивается конфиденциальная информация, например, пароль или номер кредитной карты.

Фишинг

- Письмо приходит от имени известной компании, но текст письма примитивный, с грамматическими ошибками или указан электронный адрес бесплатных почтовых серверов, например, @gmail.com, @yahoo.com, @hotmail.com.
- Ссылки в письме могут выглядеть правдоподобно или нет, но в любом случае стоит навести курсор и посмотреть во всплывающем окне, куда в действительности они ведут. Если адрес не совпадает, не переходите по этой ссылке. В мобильных устройствах следует подержать палец на ссылке, и вы увидите реальный адрес ссылки. Другой безопасный способ: скопировать ссылку и вставить в окно браузера или ввести адрес вручную.
- Вы получили письмо от своего знакомого, но текст или смысл письма очень странный, вызывает подозрения, что ваш друг не мог такое написать. Следует позвонить и уточнить, действительно ли он это написал. Ведь для мошенников наиболее простой способ обмана написать письмо от имени друга или коллеги.

Если у вас есть подозрения, что письмо или сообщение является фишинг атакой, просто удалите его. Это и есть самый лучший способ защиты.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Ресурсы

Социальная инженерия:	https://www.securingthehuman.org/ouch/2014#november2014
Пять шагов к безопасности:	https://www.securingthehuman.org/ouch/2014#october2014
Меня взломали, что делать?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
Ежедневные советы Института SANS:	https://www.sans.org/tip_of_the_day.php

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова