ЧТО ТАКОЕ ФИШИНГ И ЧЕМ ОН ОПАСЕН?

Фишинг (англ. phishing) — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логин, пароль, номер кредитной карты и другой конфиденциальной информации), а также запуск вредоносного программного обеспечения на компьютере пользователя.

Такой вид интернет-мошенничества, как правило, основан на психологической манипуляции и его цель – вывести человека на такие эмоции, как интерес, страх, жадность, злость, желание помочь. Это позволяет ослабить концентрацию человека, усыпить его бдительность.

Чтобы не стать жертвой мошенников, необходимо обратить внимание на формат поступившего сообщения, грамотность и достоверность составления текста.

Какие цели у фишинга?

Фишинговые атаки используют, чтобы украсть ценные данные: реквизиты банковских карт, логин и пароль для входа в аккаунт на каком-либо сайте (в том числе относящиеся к рабочим обязанностям ресурсы). Получив конфиденциальные данные, фишеры могут продать их другим мошенникам, самостоятельно использовать в своих целях, а также шантажировать жертв и требовать деньги в обмен на то, что не станут публиковать личные данные в Сети. В случаях, когда фишинговые атаки направлены на компании, целью киберпреступников является получение данных учетной записи какого-либо сотрудника и последующая расширенная атака на компанию.

К основным методикам и техникам фишинга относят:

Психологическое манипулирование
Представляясь представителями известных компаний, фишеры чаще всего сообщают получателям, что им нужно по какой-либо причине срочно передать или обновить персональные данные. Такое требование мотивируется утерей данных, поломкой в системе или другими причинами.
Организаторы фишинга стараются встревожить пользователя и вызвать его немедленную реакцию. Так, считается, что электронное письмо с заголовком «чтобы восстановить доступ к своему счету…» привлекает внимание и заставляет человека пройти по ссылке для получения более подробной информации.

Фишинг с обманом
Это самый распространенный тип фишинговых атак. Например, фишер присылает фальшивое письмо от имени организации с просьбой пройти по ссылке и проверить данные учетной записи.
Для кражи личных данных создаются специальные фишинговые сайты, которые размещаются по похожей ссылке и имеют схожий с оригиналом сайта дизайн.

Фишинг на конкретных персон
Чаще всего этот способ является первым этапом для преодоления средств защиты компании и проведения целевой атаки на нее. Злоумышленники в таких случаях изучают своих жертв с помощью социальных сетей и других сервисов и таким образом адаптируют сообщения и действуют более убедительно.

«Охота на китов»

Охоту за конфиденциальной информацией топ-менеджеров и других важных персон называют «охотой на китов». В этом случае фишеры тратят достаточно много времени на определение личностных качеств жертвы, чтобы подобрать подходящий момент и способы для кражи учетных данных.

Рассылка вирусов
Кроме кражи личных данных мошенники также ставят себе целью нанесение ущерба отдельным лицам или группам лиц. Ссылка фишингового письма при клике может загружать на компьютер вредоносный вирус.

Фарминг
Это новая разновидность фишинга. Этим методом фишеры получают личные данные не через письмо и переход по ссылке, а непосредственно на официальном сайте. Фармеры меняют цифровой адрес официального сайта на DNS-сервере на адрес подменного сайта, и в результате ничего не подозревающий пользователь перенаправляется на поддельный сайт. Такой фишинг опаснее традиционного, поскольку увидеть подмену невозможно. От подобных атак уже страдают аукцион Ebay, платежная система PayPal и известные мировые банки.

Вишинг
Вишинг — метод фишинга, использующий для получения информации телефонную связь. В уведомительном письме указывается номер телефона, по которому нужно перезвонить, чтобы устранить «возникшую проблему». Затем во время разговора оператор или автоответчик просит пользователя назвать идентификационные данные для решения проблемы.
Что делать при получении сомнительного электронного письма или иного сообщения?

Если вы получили сообщение, требующее взаимодействия, в том числе незамедлительного, или же такое письмо вызывает у вас любопытство, чувство страха или побуждает к действиям, например, «открой», «прочитай», «ознакомься», то задумайтесь и задайте себе следующие вопросы:

- ожидаю ли я это сообщение?
- есть ли смысл в том, что от меня требуют?
- знаю ли я автора этого сообщения?
- уверен ли я в безопасности полученного сообщения?

Если ответ хотя бы на один из озвученных выше вопросов «нет» — вероятнее всего, это кибермошенники.

В ответ на письмо с просьбой «подтверждения» учетной записи или любой другой схожей просьбой эксперты советуют пользователям связаться с компанией, от имени которой отправлено сообщение, чтобы проверить его подлинность. Кроме того, рекомендуется самостоятельно вводить URL-адрес организации в адресную строку вместо использования любых гиперссылок.

Практически все подлинные сообщения сервисов содержат в себе упоминание некой информации, недоступной для фишеров, например, упоминание имени или последние цифры номера счета. При этом подозрения должны вызвать любые письма, не содержащие какой-либо конкретной личной информации.

Следует помнить также, что фишинговые сайты могут скрываться за всплывающими окнами. На них может вести реклама. Бывают случаи, когда в графе «логин» пользователь уже видит адрес своей электронной почты и ему предлагается только ввести пароль в нижней графе. Есть вероятность увидеть ссылку на фишинговый сайт в комментариях на форумах и в социальных сетях. Ссылку может прислать вам также друг или знакомый, чей аккаунт был взломан. Если письмо или ссылка вызвали у вас подозрение, лучше не переходить по ней.

Борьба с фишерами происходит также на техническом уровне:

- Об угрозах фишинга предупреждают браузеры, большинство из них ведет собственные списки фишинговых сайтов, после сверки с ними сервисы предупреждают пользователей о переходе на опасные сайты;
- Почтовые сервисы борются с фишингом в сообщениях, совершенствуя свои спам-фильтры и анализируя фишинговые письма;
- Крупные сервисы и компании также занимаются усложнением процедуры авторизации, предлагая пользователям дополнительную защиту личных данных.

Будьте внимательны
Не спешите быстро открывать сомнительные сообщения, даже если они вызывают сильный интерес. Лучше один раз подумать и лишний раз проявить внимательность, чем потом бороться с последствиями утечки данных.