Фишинговые атаки становятся все более изощренными

Фишинговые атаки стали наиболее распространенным методом, который кибер-злоумышленники используют для атаки на людей на работе и дома. Фишинговые атаки традиционно представляли собой электронные письма, отправляемые кибер-злоумышленниками, чтобы заставить вас сделать то, что вы не должны делать, например, открыть зараженное вложение электронной почты, щелкнуть вредоносную ссылку или поделиться своим паролем. В то время как традиционные фишинговые атаки продолжаются и сегодня, многие кибер-злоумышленники создают расширенные фишинговые электронные письма, которые более персонализированы и их труднее обнаружить. Также они используют чтобы привлечь и обмануть вас такие технологии, как обмен текстовыми сообщениями, социальные сети и даже телефонные звонки. Вот их последние уловки и как их обнаружить.

Кибер-злоумышленники проводят свои исследования

Раньше фишинговые электронные письма было легче обнаружить, потому что они были общими сообщениями, рассылаемыми миллионам случайных людей. Кибер-злоумышленники понятия не имели, кто станет жертвой; они просто знали, что чем больше писем они отправят, тем больше людей смогут обмануть. Мы часто могли обнаруживать эти атаки, получая странные электронные письма со словами «Уважаемый клиент» в начале, орфографические ошибки или сообщения, которые были слишком хороши, чтобы быть правдой, например, нигерийские принцы предлагали вам миллионы долларов.

Сегодняшние кибер-злоумышленники гораздо более изощренны. Теперь они исследуют своих предполагаемых жертв, чтобы создать более индивидуализированную атаку. Вместо того, чтобы рассылать обычные фишинговые электронные письма, пяти миллионам человек отправленные корпорациями, они могут отправить их всего пяти людям и настроить атаку таким образом, чтобы она выглядела отправленной кем-то, кого мы знаем. Кибер-злоумышленники делают это следующим образом:

- изучая наши профили в LinkedIn, то, что мы публикуем в социальных сетях, или используя информацию, которая является общедоступной или найденной в Даркнете.
- создание сообщений, которые, как кажется, исходят от руководства, коллег или поставщиков, которых вы знаете и с которыми работаете.
- узнать, каковы ваши хобби, и отправить вам сообщение, притворяясь кем-то, кто разделяет взаимный интерес.
- установить, что вы были на недавней конференции или только что вернулись из поездки, а затем создать электронное письмо со ссылкой на ваши путешествия.

Кибер-злоумышленники активно используют другие методы для отправление одних и тех же сообщений, например, отправлять вам текстовые сообщения или даже звонить вам напрямую по телефону.

Как обнаружить эти более сложные фишинговые атаки

Поскольку кибер-злоумышленники не торопятся и изучают своих предполагаемых жертв, обнаружить эти атаки может быть труднее. Хорошей новостью является то, что вы все еще можете обнаружить их, если знаете, что ищете. Задайте себе следующие вопросы, прежде чем предпринимать какие-либо действия в отношении подозрительного сообщения:

1. Создает ли сообщение повышенное чувство срочности? Принуждают ли вас обходить политики безопасности вашей организации? Атакующий пытается торопить вас чтобы вы совершили ошибку. Чем сильнее ощущение срочности, тем больше вероятность нападения.
2. Имеет ли электронное письмо или сообщение смысл? Будет ли генеральный директор вашей компании срочно писать вам с просьбой о помощи? Действительно ли вашему руководителю нужно, чтобы вы купили подарочные карты? Зачем вашему банку или компании-эмитенту кредитных карт запрашивать личную информацию о вас, которая у них уже должна быть? Если сообщение кажется странным или неуместным, это может быть атакой.
3. Вы получаете связанное с работой электронное письмо от надежного коллеги или, возможно, вашего руководителя, но в электронном письме используется личный адрес электронной почты, такой как @gmail.com?
4. Вы получили электронное письмо или сообщение от кого-то, кого вы знаете, но формулировка, тон голоса или подпись в сообщении неверны и необычны?

Если сообщение кажется странным или подозрительным, это может быть атака. Если вы хотите подтвердить, является ли электронное письмо или сообщение законным, один из вариантов — позвонить человеку или организации, отправившей вам сообщение, на проверенный номером телефона..

Вы, безусловно, лучшая защита. Используй здравый смысл.

Приглашенный редактор

Фил Хоффман — ИТ-консультант на пенсии с 40-летним опытом работы в области инфраструктуры и безопасности. Он многолетний участник и редактор OUCH!, увлекается технологиями, ездой на велосипеде и фотографией.

Ресурсы

Социальный инжиниринг: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Три главных мошенничества: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Текстовые сообщения /SMS фишинг: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Вишинг - атаки на телефонные звонки и мошенничество: https://www.sans.org/newsletters/ouch/vishing/
Разведка с открытым исходным кодом: https://www.sans.org/newsletters/ouch/search-yourself-online/

Роман Полаков
OUCH! Публикуется SANS Security Awareness и распространяется под лицензией Creative Commons BY-NC-ND 4.0 . Вы можете делиться или распространять этот информационный бюллетень, если вы не продаете и не модифицируете его. Редакционная коллегия: Уолтер Скривенс, Фил Хоффман, Алан Ваггонер, Лесли Ридаут, Принцесса Янг