Фишинг (попытка украсть пароли или другую конфиденциальную информацию, выдавая себя за заслуживающий доверия веб-сайт) сегодня является одной из самых серьезных проблем в индустрии безопасности. Эту проблему пытаются решить с помощью многих технологий обеспечения безопасности, и банки, особенно те, которые часто становятся объектами подобных атак, уделяют ей много внимания. Честно говоря, в наши дни это касается большинства банков. Конечно, у нас должно сложиться впечатление, что фишинг - это легкие деньги, и люди становятся богаче. Но недавно появился интересный отчет1ъ, в котором доказывается, почему это не так. Авторы этого отчета умело сравнивают фишинг с традиционным рыболовством (да, с буквой “f” вместо “ph”).

Чем больше рыбаков, тем меньше рыбы остается для ловли, и рыбакам приходится работать усерднее, чтобы поймать такое же количество рыбы (обычно они уходят дальше в море и работают дольше). В мире фишинга происходит то же самое, за исключением того, что есть только один вид фишей, которых можно поймать (назовем его “рыба-присоска”). Число потенциальных жертв фишинга растет не очень быстро. И после того, как люди были пойманы на крючок, не так уж много из них выбрасывается обратно в пруд (это означает, что люди, которые были пойманы на крючок раньше, как правило, более осторожны и с меньшей вероятностью попадут на крючок снова).

Если фишинг ведет много злоумышленников, это создает проблемы для всех злоумышленников. Им приходится прилагать больше усилий для поиска жертв, что означает гораздо большее количество попыток фишинга, и каждый из злоумышленников заработает меньше денег (в среднем). Неудивительно, что злоумышленники оказались в такой ситуации, потому что фишинговать исключительно легко. Не требуется особых технических навыков, чтобы создать электронное сообщение или веб-сайт, которые выглядят законно. Хорошие парни, тем временем, особенно обеспокоены этой проблемой, потому что предпринимается так много попыток фишинга. Хорошие парни считают, что это серьезная проблема и что убытки огромны. Поэтому они испробовали все возможные способы в надежде, что вы сможете определить, когда вас обманывают, а когда нет.

Например:

• Большинство электронных сообщений от людей, которые на законных основаниях владеют вашей финансовой информацией (банки, PayPal и т.д.), содержат информацию, которой вряд ли может быть у злоумышленника, например, последние четыре цифры номера вашего счета.

• Когда вы заходите на законные веб-сайты, большинство из них будут иметь какой-либо встроенный в браузер механизм, который поможет вам укрепить доверие к сайту. Например, Bank of America известен своей технологией SiteKey, которая требует, чтобы вы распознавали изображение при входе на веб-сайт. Однако это не является надежным способом.

• Некоторые финансовые сайты имеют дополнительные механизмы физической аутентификации, обычно для своих самых параноидальных клиентов. Например, пользователи E*Trade (и другие) могут получить физическое устройство, которое генерирует одноразовые номера. Пользователь должен ввести тот же номер, который отображается на устройстве в данный момент. Используя несколько иную схему, Bank of America (и другие банки) позволят вам зарегистрироваться в системе, где вы должны каждый раз вводить одноразовый пароль, который они отправляют в виде текстового сообщения на ваш телефон. Эти технологии несовершенны, часто потому, что они зависят от подкованности конечного пользователя. Однако они действительно поднимают планку, что еще больше усложняет задачу фишерам.

Если исходить из экономических соображений, то средний рыбак, вероятно, зарабатывает

очень мало. В упомянутом ранее исследовании утверждалось, что средний рыбак зарабатывает меньше, чем он мог бы зарабатывать при других доступных ему возможностях карьерного роста. Однако я не уверен, что это правда. Многие люди, занимающиеся фишингом, живут в районах с тяжелой депрессией.

Возможно, в этих районах мало других доступных рабочих мест, и им будут платить столько, сколько позволит местная экономика. Если люди смогут выманивать деньги у американцев, даже если их заработки значительно ниже, чем в США. при минимальной заработной плате они легко могли бы зарабатывать гораздо больше, чем на неквалифицированной работе (если бы смогли ее получить). В любом случае, с течением времени фишерам следует ожидать, что они будут зарабатывать все меньше и меньше денег. Те, кто хорошо зарабатывает на этом, - это те, кто способен изобрести новые методы фишинга, позволяющие обмануть людей, которые в противном случае были бы устойчивы к попыткам фишинга. Например, несмотря на отличные методы обеспечения безопасности и отличную команду специалистов по безопасности, Amazon.com на данный момент это довольно привлекательная мишень для фишеров по следующим причинам:

• Большинство Amazon.com клиентов получают множество рекламных сообщений по электронной почте с сайта.

• У получателей электронной почты нет очевидного способа подтвердить, что электронное сообщение пришло от пользователя Amazon.com. Электронное сообщение отправлено в формате HTML (это означает, что это веб-страница, и большинство почтовых программ будут отображать его как веб-страницу). Чтобы проверить подлинность сайта, вам необходимо изучить ссылки и убедиться, что они ведут в нужные места. Обычно вы можете навести курсор мыши на ссылку, чтобы увидеть пункт назначения, но мало кто это делает.

• Никто не привык получать Amazon.com фишинговые сообщения электронной почты (потому что фишеры не особо нацелены на это, если вообще нацеливаются).

• Никто не ожидает, что это будет ценный объект для фишинга, потому что вы не можете напрямую получать финансовую информацию.

• Amazon.com вам часто приходится вводить пароль, поэтому фишинговое электронное сообщение, которое ведет вас на сайт, который выглядит точно так же, как Amazon.com, и запрашивает ваш пароль, не вызовет особых подозрений.

Какова стоимость фишинговой учетной записи Amazon.com?

Если бы я был плохим парнем, я бы сделал следующее:

1. Выберите одно или два доменных имени, которые не вызовут особых подозрений. Это означает, что в нем должно быть указано “amazon” — возможно, www1-amazon.com или revalidation-amazon.com.

2. Рассылайте электронные письма, которые выглядят так, как будто они на законных основаниях получены от Amazon.com, рекламируя что-то новое, что люди действительно могли бы там купить. Сообщение электронной почты должно быть просто рекламой, а не указывать на то, что “что-то не так”, как это делают большинство фишинговых сообщений электронной почты. “Что-то не так” + отсутствие конкретной информации об учетной записи = очевидная попытка фишинга.

3. Когда жертва перейдет по ссылке в сообщении электронной почты, отправьте ее на

страницу, которая в точности похожа на предыдущую. Amazon.com страница входа в систему с заполненным адресом электронной почты, но с оставленным пустым паролем (как плохой парень, вы определенно его не знаете).

4. Как только пользователь введет пароль и нажмет на кнопку, попробуйте войти в систему. Amazon.com . Если она введет неверный пароль, покажите ей тот же экран Amazon.com было бы видно, если бы она входила в систему напрямую.

5. Отправляйте ей любые страницы Amazon.com посылает тебя. Присутствуйте при их разговоре, но позвольте пользователю делать с ними все, что он захочет. Amazon.com . То есть она отправляет информацию вам, затем вы пересылаете ее на Amazon, а затем показываете ей все веб-страницы, которые Amazon хочет, чтобы она увидела.

6. Регистрируйте все на случай, если пользователь случайно введет данные кредитной карты.

7. Через несколько дней я начинал заходить в Amazon.com учетные записи, для которых у меня есть регистрационные данные (все это будет автоматизировано). Я бы начал искать недавно размещенные заказы, которые не будут отправлены в течение дня или двух (так что Amazon.com некоторое время я не буду отправлять законные электронные письма).

8. Затем я отправлю электронное сообщение, которое выглядит точно так же, как это сообщение Amazon.com отправляется, когда ваша кредитная карта не работает и вам нужно ввести новую информацию (см. рисунок 15-2).

9. Когда пользователь нажимает на ссылку, он снова переходит на сайт плохого парня. На этот раз все немного сложнее, но, в принципе, я бы сделал так, чтобы это выглядело так, как будто я Amazon.com, записав данные ее новой кредитной карты для соответствующего заказа, но в остальном показав ей то, что она увидела бы, если бы была на реальном сайте Amazon.com.

Недавно мой банк заменил мою чековую карточку, потому что в ней была серьезная брешь, поэтому я кое-что заказал на Amazon.com не прошел. Amazon.com отправил мне электронное сообщение. Сообщение было полностью текстовым, но злоумышленнику пришлось бы оформить его в формате HTML, чтобы ссылки выглядели так, как будто они указывают на Amazon.com, хотя на самом деле они указывают на сайт злоумышленника.

По большому счету, создание всего этого с минимальным участием человека не требует больших затрат времени. Человек, обладающий достаточными техническими навыками, может легко справиться со всем этим за неделю. Более профессиональному преступнику, вероятно, потребовалось бы больше времени, чтобы убедиться, что все работает правильно, и подключить его к инфраструктуре ботнета, чтобы хорошим парням было сложнее отразить атаку, как только они поймут, что происходит (в этом случае плохой парень переместил бы плохой веб-сервер перемещаясь от взломанной машины к взломанной машине).

Это не говорит ничего плохого об Amazon. Как я уже говорил ранее, я знаю, что у него отличная программа обеспечения безопасности. Я использую ее только в качестве примера, потому что я постоянный клиент и очень хорошо ее знаю. Реальный урок заключается в том, что у злоумышленников будет много неочевидных способов заработать деньги на фишинге, и поэтому список потенциальных “фишеров” далеко не исчерпан. Прямо сейчас, по сути, существует огромное озеро, полное рыбы, и никто другой там не ловит. Итак, кто-то может заработать много денег, но его легко переловить. Как только люди пострадают от фишинговой атаки в нашем примере, их осведомленность начнет расти, особенно по мере увеличения количества попыток Amazon.com поднимается вверх.

Amazon.com скорее всего, он предпримет какие-то меры, чтобы дать понять, что его сообщения электронной почты являются законными (например, разместит очевидный заголовок, содержащий ваше настоящее имя, которое, надеюсь, вы заметите, если оно когда-нибудь исчезнет). В результате эта атака в конечном итоге перестанет работать должным образом. Люди с большим подозрением отнесутся к сообщениям электронной почты Amazon.com и будут переходить непосредственно на страницу Amazon.com вместо того, чтобы переходить по ссылкам в сообщениях электронной почты. Или, по крайней мере, мы должны на это надеяться. Но было бы неправильно говорить, что на фишинге (или ловле рыбы, если уж на то пошло) нельзя заработать. По-прежнему существует множество подобных возможностей, где злоумышленники, обладающие технологическими новшествами, могут заработать немного денег.