Сетевое мошенничество

С развитием сети интернет его стали осваивать и мошенники.

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги и получить личные и конфиденциальные данные: к таким данным относятся логины и пароли от различных сервисов, в том числе банковских, номера и пин-коды банковских карт и другие персональные данные.

Сетевое мошенничество имеет множество методов.

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) предполагает за счет использования различных методов заманивания пользователя на поддельный сайт, например, через ссылку в письме, баннер или ссылку в тексте.

Иногда вредоносная ссылка маскируется под правильную ссылку – так злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение с помощью опечатки в адресе сайта, или сайты, копирующие интерфейс известных ресурсов. Примеры: http://www.sberbank.ru/ и http://www.sbenbank.ru/ либо www.yandex.ru и www.yadndex.ru.

На подобных сайтах пользователю предлагается ввести логин и пароль или данные счета, после чего зачастую происходит перенаправление на реальный сайт, но данные уже попадают в руки мошенников.

Вишинг является разновидностью фишинга, в которой используется телефон. Мошенник может позвонить и представиться сотрудником банка или платежного сервиса и попросить продиктовать какие-либо платежные данные, например, пароль или код, пришедший на телефон. Его цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька. Часто дополнительно присылается СМС со ссылкой, которая ведет на фишинговый сайт.

Фарминг или скрытое перенаправление является также разновидностью фишинга, но направляет пользователя вирус или взломанная программа на поддельный сайт, являющийся полной копией официального ресурса.

Сетевое мошенничество имеет также множество видов, в частности:

1. Липовые акции и фальшивые выигрыши в лотереи. Пользователь может получить сообщение (по телефону, почте или SMS), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет. Признаки фальшивой лотереи: пользователь никогда не принимал участие в лотерее; пользователь никогда не оставлял своих личных данных на этом ресурсе; почтовый адрес отправителя – общедоступный почтовый сервис, например, gmail.com, mail.ru, yandex.ru;

2. Просьба «друзей» сообщить пароль, когда знакомый в социальной сети сообщает о потере телефона, просит напомнить ваш номер, вам приходит SMS с неким кодом, а тот же друг в социальной сети сообщает, что заказывает товар или регистрируется на сайте и случайно указал ваш телефон вместо своего. Он просит сообщить пришедший код. Таким образом, ваш номер будет подключен к платной подписке и с вас начнут списывать деньги;

3. Ложная блокировка аккаунта в социальной сети: на баннере подробно расписан вариант «спасения» от блокирования страницы в социальный сети, который включает отправку SMS на «короткий» номер или введение кода подтверждения. В первом случае происходит разовое списание денег, а во втором оформляется ежедневная подписка на какую-либо платную услугу;

4. Рекламные сообщения и баннеры о необходимости обновления браузера имеют риск подписаться на платную загрузку или получить вирус с архивом платной программы;

5. Бесплатное скачивание файлов и просмотр каких-либо файлов с подпиской по номеру телефона, после чего включится подписка и с указанного номера могут начать списываться деньги;

6. Пользователю предлагается бесплатный антивирус, под видом которого на устройство попадет вредоносная программа, либо создается иллюзия, что компьютер уже заражен и для уничтожения угрозы нужно воспользоваться специальным антивирусом, который, опять же, окажется вирусом. Примером является появление надписи на экране компьютера о блокировке операционной системы, устранить которую можно только при отправке SMS с кодом, пришедшим на телефон при подтверждении, – после чего запускается сам вирус;

7. Предложения очень выгодных покупок, реклама больших скидок или анонс распродаж, которые размещаются на сайтах, в социальных сетях и присылаются смс или на электронную почту. Такие предложения обычно предполагают перевод денег на банковскую карту, электронный кошелек или мобильный номер. В настоящее время стала актуальна следующая разновидность данной угрозы – пользователям рассылаются на оплату мобильного телефона, домашнего интернета, ЖКХ и т.д. Зачастую мошенники направляют поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать свои платежи;

8. Мошенник может попросить денег в долг под видом знакомого, например, через взломанный аккаунт в социальных сетях. При этом перевести деньги он может попросить любым удобным способом – на электронный кошелек, банковскую карту, через интернет-банк.

Фишинговые сообщения могут содержать:

1. сведения, вызывающие тревогу, или угрозы, например, закрытие ваших банковских счетов;

2. обещания большой денежной выгоды с минимальными усилиями или вовсе без них;

3. сведения о сделках, которые слишком хороши для того, чтобы быть правдой;

4. запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;

5. и другую информацию.

Отдельным подвидом необходимо рассматривать мобильное мошенничество, которое в частности предполагает получение смс-сообщений с незнакомых номеров, которые могут содержать:

1. ссылки на фишинговые или зараженные ресурсы;

2. информацию о выигрышах, которых не существует;

3. ложные просьбы о помощи;

4. о переводе денег на сотовый, прямые просьбы о переводе денег;

5. SMS из несуществующего банка;

6. просьбы перезвонить на платный номер;

7. требования выкупа;

8. просьбы отправить СМС, которые активируют платные услуги;

9. и другую информацию.

Мобильное мошенничество также часто встречается в формах:

1. Wangiri («Очень дорогой звонок») – когда человек звонит с неизвестного номера, но, как только человек берет трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги;

2. Требования выкупа – когда кто-то звонит вам с неизвестного номера, но, как только вы берете трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги. Когда вам позвонили или прислали SMS с неизвестного номера с просьбой о помощи близкому человеку: не впадайте в панику, не торопитесь переводить деньги. Перезвоните родным и узнайте, все ли у них в порядке. Уточните, где находятся близкие.

Мобильное мошенничество имеет примеры смежных технологий: пользователю может прийти SMS от банка или платежного сервиса с паролем для совершения платежа, а сразу после этого может позвонить человек, который скажет, что ввел этот номер мобильного телефона по ошибке и попросит сообщить код из SMS, которое только что пришло пользователю. На самом деле код из SMS — это пароль не к счету незнакомца, а к счету пользователя, с помощью которого злоумышленник может поменять настройки кошелька или интернет-банка, украсть деньги и т.д.

Особо актуальной проблемой в сфере сетевого мошенничества стало стремление злоумышленников получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов. Мошенники могут получить доступ к учётной записи жертвы следующими способами:

1. Заставить жертву ввести свои данные на поддельном сайте;

2. Подобрать пароль жертвы, если он не является сложным;

3. Восстановить пароль жертвы с использованием “секретного вопроса” или введенного ящика электронной почты;

4. Перехватить пароль жертвы при передаче по незащищенным каналам связи.

Какие меры помогут бороться с мошенничеством в сети?

1. Внимательно проверять доменное имя сайта и особенно доменные имена сайтов, на которых вводятся учетные данные.

2. Использовать проверенные и безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем. Использовать закладки в браузере часто посещаемых сайтов.

3. При переходе по ссылке из сомнительных источников, в частности e-mail, форумы, сообщения в социальных сетях и всплывающие окна, вы рискуете попасть на «фишинговый сайт».

4. Помнить, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте, а также никогда не просят сообщать – ни по почте, ни по телефону – пароль, пин-код или код из SMS. Нельзя переходить по ссылкам из таких писем и вводить свои пароли на посторонних сайтах, даже если они очень похожи на сайт банка или платежного сервиса.

5. Не указывать свой мобильный номер на незнакомых сайтах.

6. Не переходить по ссылкам в сообщениях электронной почты и сообщениях из социальной сети.

7. Не размещать личную информацию в интернете. Даже маленькие кусочки личных данных могут быть использованы в преступных целях.

8. Никому не сообщать не сообщать пароли, пин-коды и коды из SMS, которые приходят на мобильный номер от банков, платежных сервисов, мобильных операторов и других организаций.

9. Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.

10. Не открывать файлы и другие вложения в письмах, даже если они пришли от друзей и знакомых. Необходимо уточнить у них, отправляли ли они эти файлы.

11. Не доверять объявлениям о подозрительно дешевых товарах, акциях и распродажах на малознакомых сайтах. Перед покупкой необходимо прочитать отзывы в интернете о сайте или частном продавце, а в случае их отсутствия отказаться от покупки.

12. Проверять реквизиты, указанные в платеже перед оплатой. Если они не совпадают с заявленными ранее, то отказаться от покупки.

13. Настроить онлайн-платежи на заранее проверенные реквизиты (авто-платежи).

14. В случае просьб от друзей и знакомых о деньгах необходимо лично перезвонить и уточнить необходимость в помощи, а в случае отсутствия возможности позвонить, задать какой-либо проверочный вопрос, ответ на который может знать только данный человек.

Что делать если уже возникли проблемы?

1. Если СМС-подписка была оформлена, то необходимо обратиться по телефону в службу поддержки оператора и попросить отключить её.

2. Если аккаунт был взломан, то необходимо заблокировать аккаунт, сообщить администрации сайта о взломе, поменять пароль к сайту, а также предупредить всех своих знакомых о том, что произошел взлом и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты.

3. Если деньги или другие важные данные вашей банковой карты были предоставлены неизвестным лицам, то необходимо как можно