**Что такое фишинг?**

В современном мире достаточно много угроз сопровождает людей изо дня в день. К стихийным бедствиям, убийцам и тому подобному добавились мошенники, в том числе интернет мошенники. Каждый день сотни людей становятся жертвами их махинаций, теряют все то, что копили годами. Одной из такой угроз являются фишинг мошенники и их атаки в интернете, число которых растет с каждым днем. Сегодня я хочу подробно ознакомить Вас с этой угрозой, рассказать, как с ней бороться и как обезопасить себя и своих близких.

**Что такое фишинг? Кто такие фишинг мошенники?**

**Фишинг –** (в переводе с английского «fishing» - рыбная ловля, к чему-то принуждать, что-то узнавать) – это один из видов современного интернет-мошенничества с использованием социальной инженерии с целью получения личной информации пользователей (логинов, паролей, кодов и так далее).

**Фишинг мошенники** – интернет пользователи, которые с помощью спама, получают нужную им личную информацию от других людей.

**Спам –** это своего рода реклама, которую Вы можете получить на свою почту или в сообщении в социальной сети. Спам может быть безопасным (не несущим угрозу Вам или Вашему компьютеру) и опасным (нести в себе фишинг ссылки, вирусы).

**Какая же основная задача у фишинг мошенника?** Главной целью всех фишинг мошенников является узнать от Вас какую-то личную информацию. Самое распространенное – это логины и пароли от Вашей почты или страничек в социальных сетях. С их помощью жулики начинают рассылку (возможно даже вредоносного) спама от Вашего имени Вашим родственникам, друзьям, коллегам и т.д. Менее распространенное, но с огромными темпами набирающее популярность, - это выяснение у Вас номеров и паролей от ваших банковских счетов, номера и пин коды Ваших банковских карточек для переводов денег на свой счет. Каждый из этих случаев опасен, потому что несет за собой последствия.

**Как действуют фишинг мошенники?**

Многие люди не единожды слышали о махинациях и тем не менее попадаются на самые простые уловки. Чаще всего мошенники действуют по такой схеме:

1) Создаются сайты, которые по своему оформлению очень похожи на игровые ( например онлайн казино). Если Вы когда-то пользовались таким, то знаете, что к ним прикрепляется множество ресурсов, которые позволяют связываться с Вашими онлайн кошельками (например WebMoney Кошелёк, Яндекс Деньги), банковскими счетами и картами;

2) Есть определенная база данных, используя которую злоумышленники совершают широкомасштабную рассылку спама. В ней вы можете увидеть рекламу этого самого нового казино, которая будет привлекать не только увлекательной и затягивающей игрой, но и скорее всего очень правдоподобными подарками в виде легкодоступных бонусов или же просто некоторой суммы денежных средств;

3) Гость этого псевдо казино, как и сказано в рекламе, получает обещанный бонус и без особого труда, что должно насторожить, отыгрывает его;

4) Далее посетитель, естественно, хочет получить свой выигрыш. Он оформляет заявку на выплату выигранных им денег. Как и любой человек у него уже присутсвует чувство эйфории. Но тут он получает в ответ на свою заявку сообщение о том, что, например, сервер перезагружен и для получения денег ему нужно немного подождать;

5) Но на этом клиент казино не останавливается. Чтоб не терять время и пока фартит, он вводит новый депозит и снова, скорее всего выигрывает. Помимо этого не редко бывает так, что такие «казино» содержат ссылки на другие подобные сайты.

Вывода выигранных Вами средств не произойдет никогда. Чаще всего в мошеннических казино вообще не предусмотрена система выплат.

И главный вопрос: куда же делись ваши деньги? Ответ прост: Ваши деньги ушли в карман злоумышленника сразу после оформления депозита. Если Вы опять захотите вывести деньги, то получите все то же сообщение о том, что Вам следует немного подождать. За это врнмя мошенник успеет обналичить деньги и скрыться. Такие сайты временные. Срок их «жизни» длится от нескольких часов до нескольких недель. После удаления такого сайта найти злоумышленника практически невозможно.

Так же может использоваться рассылки от имени банков, где просят подтвердить Ваши личные данные. Или же подделка сайта (чаще всего социальные сети) – обычно подделывают только одну страницу, где нужно указать Ваши логин и пароль.

**Как защититься от фишинга и не попасть под фишинг атаку?**

И так, мы подробно разобрали что такое фишинг, фишинг мошенники и какие схемы используют для своих махинаций. В принципе ничего сложного в модели их действий нет. Но все же, лучше себя обезопасить. Вот несколько простых, незамысловатых, но очень полезных советов:

1) Лучше иметь не одну электронную почту, а две. Первая будет использоваться, как Ваша личная (для переписок с родными и близкими, коллегами и т.д.). Вторая же для регистрации на разнообразных форумах, чатах, тех же казино. Это поможет Вам, как минимум, случайно не наткнуться на вредоносный спам.

2) С осторожностью и вдумчиво читайте электронные письма. Запомните, что официальные законные организации ни в коем случае не запрашивают Ваши конфединциальные данные. Большинство банков это делают только при личном обращении клиента.

3) Не поддавайтесь манипуляции. Помните о предыдущем правиле и если чувствуете давление (например угрозу закрытия вашего счета) лучше лично позвоните на горячую линию банка или обратитесь в ближайшее отделение.

4) Что не мало важно «личное обращение», которое мошенники используют крайне редко в отличии от подлинных писем банков.

5) Никогда не переходите по ссылке, если вы не уверены в ее подлинности. Проверить это очень легко. Чаще всего они очень похожи на настоящие интернет страницы и обман можно распознать только будучи очень внимательным. Откройте новую вкладку в вашем браузере и начните вводить ссылку и проверте с той, что в Вашем письме. Отличие может быть только в одной букве (например официальный сайт vkontakte.com превращается в vkantakte.com).

6) Далее, никогда не отвечайте на спам. Большинство спамеров фиксируют Ваши ответы. Соответственно: чем больше Вы отвечаете, тем больше Вам присылают.

7) Своевременно обновляйте Ваш браузер. Будьте уверены, что на компьютере стоит последняя версия браузера и загружены и установлены все последние исправления, которые связаны с безопасностью в интернете.

8) Установите антивирус. У большинства антивирусов есть функция, которая блокирует фишинг атаки на Ваш компьютер. Проверяйте эту функцию в характеристике перед установкой.

**Что делать, если Вы обнаружили фишинговый сайт или стали его жертвой?**

**Если Вы наткнулись на фишинговый сайт, то Вам следует сделать следующее:**

1) Наткнувшись на один из таких сайтов Вы можете с легкостью обратиться к владельцу ресурса, который стараются подделать. В большинстве случаев это можно сделать через «Центр поддержки пользователей» написав письмо с жалобой и прикрепить к нему ссылку на фишинговый сайт.

2) Если же Вы наткнулись на такую ссылку в сообщении какого-то пользователя, комментарии или же на форуме, Вы можете нажать кнопку «Пожаловаться» или «Жалоба», тем самым указав причину и заблокировав пользователя и его сообщения до проверки администрацией.

3) Сообщить об угрозе фишинга можно на специальные сайты в интернет сети. Подробнее о них Вы можете узнать прочитав статьи в интернете.

**Если же Вы были недостаточно внимательны и все таки стали жертвой фишига Вам следует:**

1) Если обман произошел в социальной сети или почте поменяйте пароль или удалите свою страницу.

2) Сообщите своим друзьям о том, что злоумышленники владеют Вашим логином и паролем, чтоб они не переходили по ссылкам отправленным от Вашего имени.

3) Если Вы стали жертвой более серьезного, финансового жульничества Вас срочно нужно обратиться в банк, чтоб там заморозили Ваши счета до личного визита в отделение банка.

4) Вы можете обратиться в милицию и прокуратуру, которые обязаны принять Ваше заявление. Более подробно об этой процедуре Вы можете узнать у сотрудников правоохранительных органов.

Таким образом мы подробно рассмотрели вопрос опасности фишинга для пользователей глобальной сети интернет. Знайте, что каждый может стать жертвой, несмотря на свою осторожность и наблюдательность. Помните правила защиты от интернет мошенничества и используйте их каждый день. Так же не забывайте предупредить об этой опасности своих родственников, друзей и коллег.