Фишинг (от англ. выуживать, ловить) – это вид получения секретной информации, при котором злоумышленник обманом заставляет клиента открыть свои личные данные. Например, отправляет сообщение в мессенджер или в соцсетях с просьбой сказать номер и код банковской карты, номер телефона, логин и пароль от какого-либо сервиса и т. д.

Вишинг – одна из разновидностей фишинга, при которой используются методы социальной инженерии. Как правило, телефон. Вам звонят из банка и просят подтвердить перевод денег, который вы, естественно, не совершали. В итоге вы сами, добровольно сообщаете свои данные карты, CVV-код и иные сведения, с помощью которых потом можно провести реальную операцию по снятию и переводу наличных.

В чём заключается фишинг?

Мошенники создают страницу, которая визуально очень похожа на страницу реально существующей компании или вовсе идентична ей. Размещают её на сайте, название которого визуально тоже очень похоже на название реальной компании и имеет лишь незначительные различия. Отправив такую ссылку пользователю, они ждут, когда он введёт на такой странице свои данные. Как только он это сделает, данные окажутся в руках мошенников, и они смогут их использовать по своему усмотрению.

Вот, например, как выглядит фишинговая страница, которая маскируется под торговую интернет-площадку. Обратите внимание, внешний вид абсолютно идентичен оригиналу, выдаёт обман только адрес страницы (вместо .by указано .store):

Под каким предлогом могут выслать ссылку на фишинговую страницу?

Вот актуальные схемы, которыми мошенники завлекают людей:

1. Фишинговая страница, которая выглядит как интернет-банк.

Мошенник под видом покупателя пишет продавцу о желании приобрести товар, а также сообщает, что прямо сейчас забрать его не может. Чтобы продавец гарантированно его оставил, предлагает перевести деньги продавцу немедленно, а для этого спрашивает, какой у него банк и номер карты. После чего сообщает, что нужно подтвердить перевод, высылает ссылку на поддельную страницу, выглядящую как интернет-банк, где пользователю предлагается ввести свои данные для входа в интернет-банк, а затем ввести код из смс. Если пользователь введёт свои данные, то мошенник сможет от его имени зайти в интернет-банк и перевести деньги куда угодно.

2. Фишинговая страница, которая выглядит как оригинал сайта.

Мошенник размещает объявление о дорогостоящем товаре по привлекательной цене. Пишет в объявлении, что связь только через мессенджер (Viber, WhatsApp, Telegram), после чего получает телефоны заинтересованных пользователей в личные сообщения.

Пишет им в мессенджере, что готов продать товар, но так как находится в другом городе, то вышлет вещь через Доставку. После чего высылает ссылку на страницу, которая выглядит совершенно так же, как оригинал торговой интернет-площадки, и на которой предлагается ввести свои данные карты для оплаты за товар. Если доверчивый пользователь вводит свои данные, то мошенник с их помощью переводит деньги с карты пользователя на свой счёт.

Как узнать, что страница настоящая?

Адресная строка.

Поищите официальный сайт компании в Гугле или Яндексе и сравните написание этого сайта с тем, которое вы видите на странице, которую вам кто-то выслал. Например, skrynka.by — это реальное название. А skrynka.be, skrynka.store, skrynka.swf.com, skrynka.aa.by названиями не являются.

Другие элементы страницы.

Они могут выглядеть как настоящие, но на самом деле такими не являются. Например, при нажатии на кнопку ничего не происходит; в меню ни один пункт никуда не ведёт.

Особенности текста.

Даже одна единственная странность может указывать на то, что страница не настоящая.

Как ещё можно себя обезопасить?

Ведите переписку только на официальной торговой интернет-площадке.

На многих торговых интернет-площадках заблокирована возможность отправлять ссылки на сторонние сайты, и это сделано специально для того, чтобы оградить добросовестных покупателей и продавцов от попыток недобросовестных пользователей увести на мошенническую страницу. Если кто-то хочет отправить вам ссылку на объявление с сайта, то в личных сообщениях это можно сделать. Однако, если это фишинговая страница (т.е. выглядит как торговая интернет-площадка, но на самом деле таковой не является), то отправить ссылку на неё в личных сообщениях не получится.

Если нужно перевести деньги на другую карту, то пользуйтесь мобильным приложением от вашего банка, либо же самостоятельно заходите на страницу интернет-банка вашего банка, сохраните себе её в закладки.

Не переходите по ссылкам, которые вам высылают посторонние люди.

Не сообщайте никому информацию, размещенную на вашей банковской платежной карте (на обеих сторонах): номер, дату, код, цифровые или буквенные коды, паспортные данные.