Фишинг и как не попасть на удочку кибермошенников

Фишинг (англ. *phishing*, от *fishing* — рыбная ловля, выуживание) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Причины могут называться различные. Это может быть утеря данных, поломка в системе и прочее.

Атаки фишеров становятся все более продуманными, применяются методы социальной инженерии. Но в любом случае клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении («если вы не сообщите ваши данные в течение недели, ваш счет будет заблокирован»). Забавно, но часто в качестве причины, по которой пользователь якобы должен выдать конфиденциальную информацию, фишеры называют необходимость улучшить антифишинговые системы («если хотите обезопасить себя от фишинга, пройдите по этой ссылке и введите свой логин и пароль»).

Фишинговые сайты, как правило, живут недолго (в среднем — 5 дней). Так как антифишинговые фильтры довольно быстро получают информацию о новых угрозах, фишерам приходится регистрировать все новые и новые сайты. Внешний же вид их остается неизменен — он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники.

Зайдя на поддельный сайт, пользователь вводит в соответствующие строки свой логин и пароль, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, в худшем — к электронному счету. Но не все фишеры сами обналичивают счета жертв. Дело в том, что обналичивание счетов сложно осуществить практически, к тому же человека, который занимается обналичиванием, легче засечь и привлечь мошенников к ответственности. Поэтому, добыв персональные данные, некоторые фишеры продают их другим мошенникам, у которых, в свою очередь, есть отработанные схемы снятия денег со счетов.

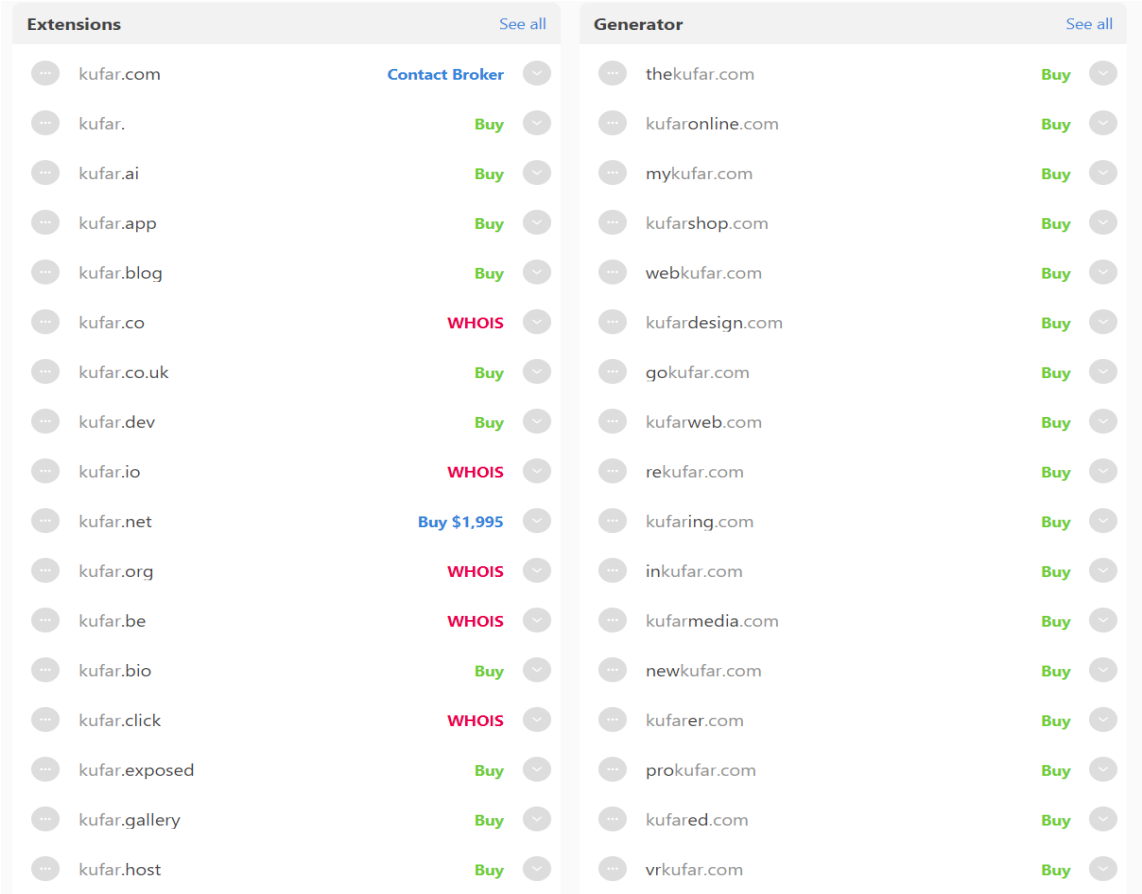
Наиболее частые жертвы фишинга — банки, электронные платежные системы, аукционы. То есть мошенников интересуют те персональные данные, которые дают доступ к деньгам. Но не только. Также популярна кража личных данных от электронной почты — эти данные могут пригодиться тем, кто рассылает вирусы или создает зомби-сети (ботнет).

Характерной особенностью фишинговых писем является очень высокое качество подделки. Адресат получает письмо с логотипами банка / сайта / провайдера, выглядящее в точности так же, как настоящее. Ничего не подозревающий пользователь переходит по ссылке наподобие «Перейти на сайт и авторизоваться»,

но попадает на самом деле не на официальный сайт, а на фишерский его аналог, выполненный с высочайшей точностью.

Еще одной хитростью фишеров являются ссылки, очень похожие на URL оригинальных сайтов. Ведь достаточно наблюдательный пользователь может обратить внимание на то, что в командной строке браузера высвечивается ссылка, совершенно либо частично отличная от легитимного сайта. Такие «левые» ссылки тоже встречаются, но рассчитаны они на менее искушенного пользователя. Иногда они начинаются с IP-адреса, хотя известно, что настоящие солидные компании давно не используют подобные ссылки.

Поэтому фишинговые URL часто похожи на настоящие. Они могут включать в себя название настоящего URL, дополненное другими словами (например, вместо www.somelink.com стоит www.login-somelink.com). Также в последнее время популярный фишинговый прием — ссылка с точками вместо слешей, внешне очень похожая на настоящую (вместо www.somelink.com/aut/login стоит www.somelink.com.aut.login). Можно привести еще такой фишерский вариант: www.somelink.com-aut.login.

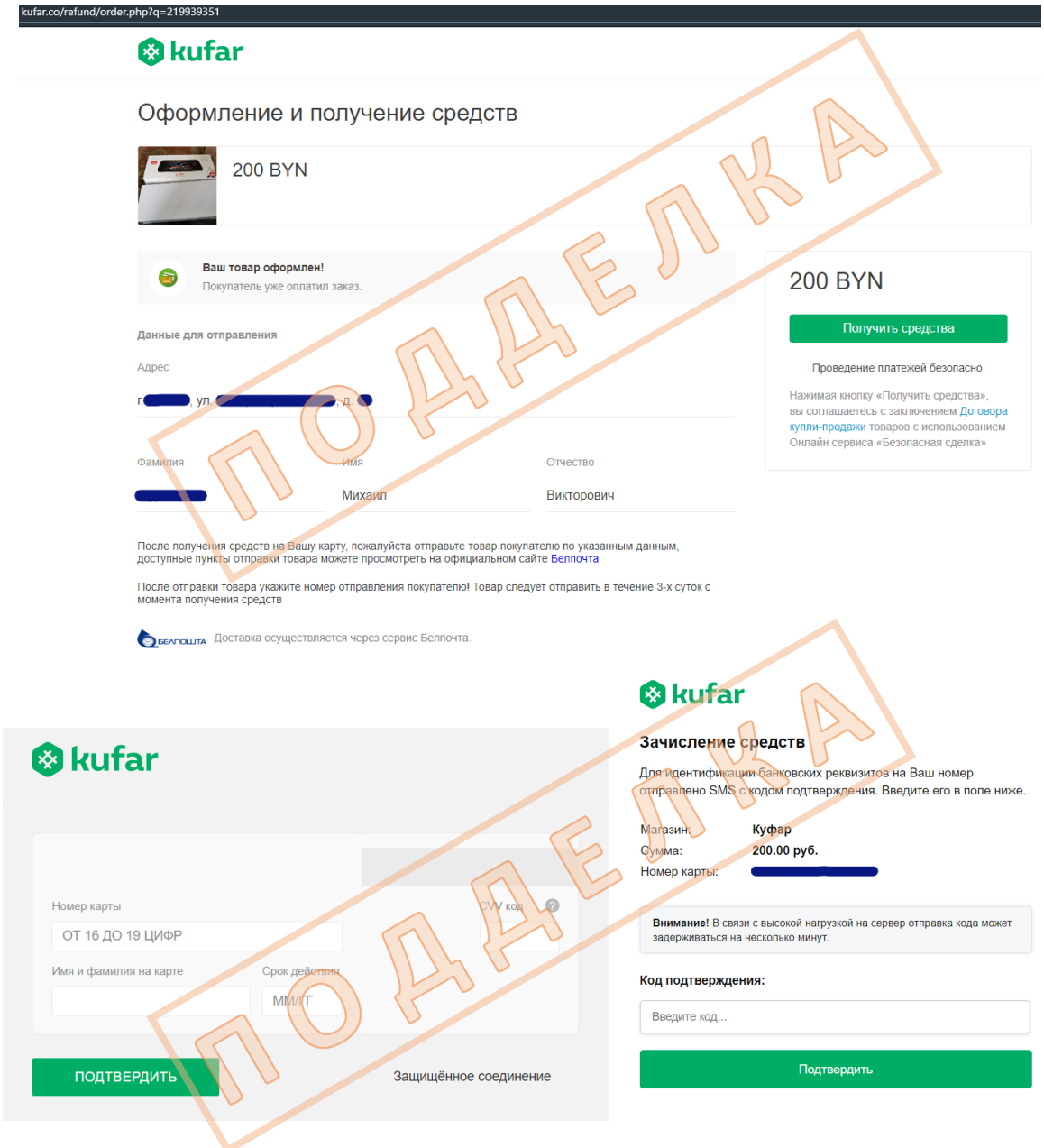


Также в самом теле письма может высвечиваться ссылка на легитимный сайт, но реальный URL, на который она ссылается, будет другим. Бдительность пользователя притупляется еще тем, что в письме может быть несколько второстепенных ссылок, ведущих на официальный сайт, но основная ссылка, по которой пользователю надо пройти и залогиниться, ведет на сайт мошенников.

Иногда личные данные предлагается ввести прямо в письме. Надо помнить, что никакой банк (либо другая организация, запрашивающая конфиденциальную информацию) не будет этого делать подобным образом.

Технологии фишеров совершенствуются. Так, появилось сопряженное с фишингом понятие — фарминг. Это тоже мошенничество, ставящее целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNS цифровые адреса легитимных веб-сайтов на адреса поддельных, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид мошенничества еще опасней, так как заметить подделку практически невозможно.

Наиболее популярные фишерские мишени — аукционы, торговые площадки, финансовые и платежные системы. Также страдают различные банки по всему миру. Атаки фишеров бывают случайными и целевыми. В первом случае атака производится «наобум». Атакуются наиболее крупные и популярные объекты — такие как торговые площадки — так как вероятность того, что случайный получатель имеет там учетную запись, довольно высока. Во втором случае мошенники узнают, каким именно банком, платежной системой, провайдером, сайтом пользуется адресат. Этот способ более сложен и затратен для фишеров, зато больше шансов, что жертва купится на провокацию.



Воровство конфиденциальных данных — не единственная опасность, поджидающая пользователя при нажатии на фишерскую ссылку. Зачастую, следуя по ней, можно получить программу-шпиона, кейлоггер или троян. Так что, если даже у вас нет счета, которым мошенники могли бы воспользоваться, нельзя чувствовать себя в полной безопасности.

Успеху фишинг-афер способствует низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. И хотя на многих сайтах, требующих конфиденциальной информации, опубликованы специальные предупреждения о том, что они никогда не просят сообщать свои конфиденциальные данные в письмах, пользователи продолжают слать свои пароли мошенникам. Пока же основной защитой от фишинга остаются спам-фильтры и личная цифровая осведомленность граждан.

Рассмотрим основные ошибки пользователей, которые способствуют совершению киберпреступлений.

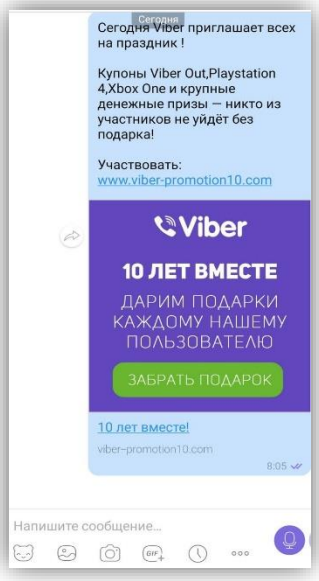
Ошибка № 1: не использовать антивирусную защиту

Хороший антивирусный пакет включает защиту от спама и фишинговых писем. Он сам распознает подозрительных адресатов. Кроме того, антивирус защитит от программ, которые воруют данные карт, получают доступ к онлайн- и мобильным банкам, перехватывают СМС и push-сообщения с секретными кодами. Это еще опаснее, чем фишинг, — ваш счет могут обнулить, а вы об этом даже не сразу узнаете. Важно регулярно обновлять защиту.

Кибермошенники изобретают новые вирусы и способы фишинга буквально каждый день.

Ошибка № 2: переходить по ссылкам из сообщений от незнакомых адресатов

Мошенники регистрируют адрес почты, похожий на адрес реального интернет-магазина, банка или другой легальной организации. Например, вместо настоящего адреса магазина mail@someshop.ru используют mail@somesshop.ru.



Иногда обманщики даже не заморачиваются с похожим адресом, так как зачастую он скрыт от глаз пользователя. Просто указывают название магазина как имя отправителя — именно его и видит получатель. Подмену проверить легко, но не все обращают внимание на такие детали.

Мошенники заманивают людей на фишинговые сайты не только через электронную почту, но и через мессенджеры и социальные сети. Вам может прийти сообщение от знакомого, который предлагает перейти по ссылке. Но может оказаться, что его аккаунт взломали.

Иногда преступники даже не стараются мимикрировать под кого-то другого. Вместо этого они запускают свой собственный бизнес-проект. И создают видимость, что проводят викторины с гарантированным выигрышем, анкетирование за вознаграждение или рассылают видео для взрослых. В текст письма или сообщения они добавляют ссылку, которая вместо обещанных викторин и видео ведет на фишинговый сайт. Его создают специально для этой аферы, чтобы собирать личные

и платежные данные пользователей. В некоторых случаях при переходе по ссылке загружается вирус, который ворует данные с вашего устройства.

Обманщики подбирают тему письма, на которую получатель должен среагировать. Что-то пугающее: «Ваш аккаунт будет заблокирован», «Срочное сообщение от Службы безопасности». Или завлекающее: «Вам начислено 500 бонусов», «Возврат платежа на 5 000 рублей». Или интригующее: «Привет! Шлю тебе фотки с последней вечеринки». Мошенники умеют играть на эмоциях.

Всегда тщательно проверяйте адрес, с которого пришло письмо. Если он хотя бы одним символом отличается от привычного адреса магазина, банка, авиакомпании или другой реальной организации, такое письмо не стоит даже открывать. Если же адрес вам вообще не знаком и вы не ждете сообщений от новых адресатов, то можете смело его удалять. Когда откроете письмо, обратите внимание на то, как оно написано и оформлено. Орфографические ошибки и ужасный дизайн — явный признак поддельного письма. Но в последнее время мошенники научились очень точно повторять фирменный стиль известных компаний. Так что стоит быть внимательным, даже если все выглядит идеально.

Если непонятную ссылку прислал друг или знакомый, лучше перезвонить и удостовериться, что это сообщение точно от него.

Ошибка № 3: не проверять адресную строку сайта

Обязательно нужно проверять при переходе на сайт его адрес. Лучше всего сохранять адреса банков, госорганов, любимых интернет-магазинов и других онлайн-сервисов в закладках. Можно вбивать адрес вручную, но нужно быть внимательным — иногда ошибка даже в одном символе приведет вас на фишинговый сайт-двойник.

Всегда проверяйте адресную строку браузера. Иногда можно попасть на фишинговый сайт даже при переходе с одной страницы известного вам портала на другую.

Безопасность соединения, несомненно, важный аспект. Если вы хотите ввести персональную информацию или данные карты, сделать покупку через сайт, то перед его адресом обязательно должно стоять https и значок закрытого замка. Буква s и закрытый замок означают, что соединение защищено: когда вы вводите на сайте данные, они автоматически шифруются и их не могут перехватить.

Защищенное соединение — требование обязательное, но не достаточное. Хакеры не могут подключиться к такому сайту и узнать ваши данные. Но это не гарантия того, что сам сайт создан законопослушной компанией. В последнее время и преступники умудряются получать сертификаты безопасности для своих сайтов.

Также стоит обратить внимание и на дизайн. Даже если вы проморгали лишнюю букву в адресе, а преступники организовали защищенное соединение, плохой дизайн сайта должен броситься в глаза. Преступники создают онлайн-ресурсы с простой целью — собрать конфиденциальные данные. Поэтому в большинстве случаев они не мудрят со структурой и дизайном сайта. Небрежная верстка, орфографические ошибки, неработающие разделы и ссылки — явные признаки фальшивки.

Но если у мошенников большие амбиции, они могут вложиться в создание сайта, который максимально точно повторяет интернет-ресурс известной организации. Или создать красивый и качественный сайт своего собственного «проекта». Так что только на дизайн тоже ориентироваться нельзя.

Ошибка № 4: платить через небезопасные страницы

После ввода реквизитов карты сайт магазина должен перекинуть вас на шлюз платежной системы вашей карты. Это отдельная безопасная страница, интернет-магазин не может получить доступ к информации, которую вы там введете.

Платежные шлюзы соединяют владельца карты с его банком при проведении платежа. Банк присылает клиенту в СМС-сообщении одноразовый код для подтверждения операции. И только после того, как покупатель его вводит, проходит платеж.

Никому не сообщайте секретные коды от банка — проверьте, совпадают ли данные из СМС с деталями операции. Если все в порядке, вбейте код в специальное поле на странице оплаты. Если нет — позвоните в банк.

Безопасные шлюзы есть у всех платежных систем. Ищите их логотипы на странице оплаты: Visa Secure, MasterCard SecureCode и т.п. Причем логотипы должны быть активными ссылками, которые ведут на сайты платежных систем. На страницах мошенников эти логотипы — просто картинки.

Ошибка № 5: использовать одну и ту же карту для всех платежей

Для онлайн-покупок и оплаты услуг через интернет лучше завести отдельную карту. Стоит переводить на нее деньги прямо перед платежом и пополнить на ровно ту сумму, которую собираетесь перечислить.

Некоторые банки и системы электронных платежей (электронные кошельки) предлагают заводить виртуальные карты — у них есть реквизиты, но в виде пластика они не существуют. Иногда можно даже создавать виртуальные карты, которые действительны лишь для одной онлайн-покупки.