Как не стать жертвой «фишера». Рекомендации по борьбе с кибермошенниками

Внимательно проверяйте электронные письма

Получив любое письмо, не спешите отвечать или выполнять инструкции из него: сначала обратите внимание на важные детали. Что Вас должно насторожить?

Броская тема. Крупные переводы, денежные компенсации, взлом или блокировка учетной записи, мошеннические операции. Злоумышленники стараются завладеть вниманием, играя на чувствах жертвы, особенно часто — на жадности или страхе.

Нагнетание обстановки. Фразы вроде «срочно!» и «у вас осталось всего 3 часа», обилие восклицательных знаков — тоже уловки из арсенала мошенников, которые любыми способами пытаются заставить вас торопиться, паниковать и от этого потерять бдительность.

Ошибки, опечатки и странные символы в тексте. Некоторые преступники и правда безграмотны, но иногда злоумышленники специально пишут слова с ошибками, например «розыгрышь призов», или меняют часть букв на похожие латинские. Так они пытаются обойти спам-фильтры.

Странный адрес отправителя. Нагромождение случайных букв и цифр или «левый» домен в адресе отправителя письма, якобы пришедшего от крупной организации, — верный признак подделки.

Ссылка в письме, если она там есть. Точнее, адрес сайта, на который она ведет. Чтобы увидеть его, нужно навести мышку на ссылку и внимательно проверить адрес. Часто в расчете на невнимательность жертв преступники вставляют в сообщения ссылки на сайты с именами известных компаний или брендов с небольшим изменением, например sumsung.com или qoogle.com, поэтому проверять ссылку надо очень внимательно.

В большинстве случаев такой проверки хватит, чтобы опознать фишинговое письмо массовой рассылки. Но, к сожалению, имя и адрес отправителя можно подделать, а ссылку сократить до нечитаемого вида или настроить цепочку автоматических переходов с менее подозрительных адресов на сам фишинговый сайт.

Поэтому по возможности вообще не переходите по ссылкам из писем, если вы их не запрашивали. Например, уведомление из банка или от онлайн-магазина можно проверить, позвонив по телефону из договора. В социальную сеть — зайти, набрав адрес вручную. Информацию о розыгрыше проверить на официальном сайте проводящей его компании, который вы найдете через поисковик. И так далее.

Не теряйте бдительность в мессенджерах и социальных сетях

Внимательными надо быть не только с письмами в почте, но и с сообщениями в мессенджерах. А также в соцсетях: ссылка-приманка может

содержаться в посте знакомого на Facebook, ВКонтакте, в ответе фейковых представителей бренда в Twitter, личном сообщении в Discord и т.п.

Также стоит с подозрением относиться к баннерам — картинка на них может не иметь ничего общего с сайтом, на который вас перекинет. Ресурсы, где размещены баннеры, как правило, не могут контролировать, что именно увидит и куда перейдет пользователь. Так что даже с вполне респектабельного сайта по баннеру вы можете перейти на фишинговую страницу.

Как и в случае с почтой, нужно очень внимательно проверять все ссылки, а лучше вообще не переходить по ним, если вы не запрашивали последних.

Перед вводом номера карты остановитесь!

Данные банковских карт — особенно чувствительная персональная информация. Они открывают прямой доступ к вашим деньгам. Поэтому, как бы вы ни попали на сайт — по ссылке, баннеру, из поисковой выдачи или набрав адрес вручную, — прежде чем вводить реквизиты карты, еще раз остановитесь и проверьте, где вы находитесь.

Во-первых, присмотритесь к адресной строке. Признаки опасности все те же — опечатки, цифры вместо букв, дефисы в неожиданных местах и странные домены. Увидели один из них — покиньте сайт и попробуйте ввести его адрес заново.

Во-вторых, в той же адресной строке нажмите на замочек слева. Сам по себе он не гарантирует безопасность, но по клику появится предложение узнать больше о владельце сайта. Нажимайте на кнопки «Подробнее» и «Больше информации», пока не увидите название организации, которой принадлежит сайт.

Если вы часто совершаете покупки через Интернет, в том числе у небольших компаний и частных продавцов, мы рекомендуем завести для этого отдельную карту, хранить на ней незначительные суммы и пополнять непосредственно перед тем, как соберетесь что-то оплатить. Даже если данные этой карты утекут в результате фишинга, вы не потеряете больших денег.

Используйте разные пароли

Если вы используете для разных аккаунтов одинаковый пароль, пусть даже очень надежный, и однажды введете его на фишинговом сайте, то рискуете потерять все свои учетные записи. Поэтому важно, чтобы пароль был уникальным для каждого сайта и приложения.

Если вам трудно придумывать и запоминать десятки паролей для каждого интернет-ресурса: социальной сети, онлайн-магазина, интернет-банкинга и др., вам поможет менеджер паролей.

С таким решением вам нужно будет запомнить только один уникальный мастер-пароль, который откроет доступ ко всем остальным. Их, в свою очередь, приложение будет подставлять само на нужные сайты. Кстати, это работает и как дополнительная проверка на фишинг: если

приложение не подставило логин и пароль автоматически, то, скорее всего, вы находитесь на поддельной странице. Для человека она выглядит похоже, но адрес у нее другой, поэтому менеджер паролей и не подставляет на ней учетные данные. Кроме того, менеджеры паролей сами генерируют сложные для взлома комбинации.

Включите двухфакторную аутентификацию для защиты аккаунтов

Многие фишинговые атаки нацелены на угон учетной записи. Однако можно сделать так, чтобы у злоумышленников не получилось войти в аккаунт, даже если они получат логин и пароль. Настройте двухфакторную аутентификацию во всех возможных сервисах — и для авторизации будет нужен дополнительный временный код, который придет вам по почте, в SMS или в специальном приложении-аутентификаторе. Таким образом, злоумышленнику, чтобы войти в ваш аккаунт придется заполучить еще и специальный код подтверждения.

Однако надо помнить о том, что особенно тщательные фишеры могут подделывать и окошко для ввода одноразового кода двухфакторной аутентификации, поэтому бдительность не стоит терять на всех этапах проведения транзакции.

Стоит помнить, что мошенники идут в ногу со временем, а общество постоянно повышает уровень своих цифровых знаний, всё больше узнает о различных преступных методах злоумышленников, поэтому используемые сейчас последними способы и средства для хищения денежных средств в скором времени могут стать неактуальными. В любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщить третьим лицам либо ввести где-то свои персональные данные или совершить какие-либо действия по указанию мошенников. Ведь Ваша безопасность, в первую очередь, в Ваших руках!