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 запрашивалипоследних.

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.

Что бы обезопасить себя и повысить уровень цифровой грамотности, рассмотрим самые распространенные на текущий момент схемы мошенничества:

1. **«Звонок из Банка»**

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка.

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber, WhatsApp и Telegram. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка. У мошенников есть возможность звонить с номеров, похожих (реже – полностью совпадающих) на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя».

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (зачастую сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код). Это нужно якобы «для сохранности ваших денег».

Как мошенник пытается вас убедить:

- *«Мы звоним с официального номера, проверьте на сайте».*
- *«В целях конфиденциальности я включаю робота, который защитит ваши данные».*
- Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
- Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
- Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

Важно! Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать!

Еще один из способов получить доступ к Вашим денежным средствам, используя методы социальной инженерии, побудить клиентов банковских учреждений установить сторонние мобильные приложения для удаленного доступа в мобильное устройство потенциальной жертвы. Для примера, одним из таких приложений является "AnyDesk - удаленное управление" из сервисов GooglePlay/AppStore.

Звонки осуществляются, как правило, на мобильные телефоны из указанных выше мессенджеров. При этом мошенники представляются сотрудниками банка, сообщают о якобы зафиксированных попытках совершения подозрительных операций на внушительные суммы, предлагают подтвердить их легитимность. В ходе разговора, с целью скорейшего вхождения в доверие, опрашивают клиента, задавая вопросы общего характера: «Передавалась ли БПК третьим лицам», «Доставляются ли СМС-оповещения» и т.п. Сообщают о блокировке сомнительных операций и счета клиента. Для повышения степени защищенности Интернет-банкинга и восстановления доступа к счету клиенту настоятельно рекомендуют установить приложение «AnyDesk - удаленное управление» из сервисов GooglePlay/AppStore. В случае согласия пострадавшего, конечно же, оказывают помощь и консультацию в установке.Установленное приложение позволяет злоумышленникам получить удалённый доступ к вашему устройству.

2. «Потенциальный покупатель»

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети Интернет. По каким-то причинам «покупатель» не может сегодня привезти или

перечислить деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Важно! Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии– только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в Интернете путем обычного поиска.

Запомните! Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

3. «Сообщения в социальных сетях»

Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям.

Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.

При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

4. «Розыгрыши/раздачи/опросы от Банка или иных организаций»

Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» либо для зачисления денежных средств в честь юбилейной даты со дня образования того или иного финансового учреждения. Цель опроса — изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение.Однако, по окончанию опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения или ввести персональные данные Вашей карты для зачисления на нее денежных средств.

Данный кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

Важно! Посетите официальную страницу организации, а не ресурс, ссылку на который прислал мошенник или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.

5. «Фишинг и новшества в различных платежах»

Дополнительно хотим рассказать о новой мошеннической схеме, которая в текущее время широко распространена на территории Российской Федерации и, к сожалению, может быть актуальна для граждан Республики Беларусь.

Злоумышленниками по электронной почте рассылаются фальшивые уведомления об оплате долгов за жилищно-коммунальные услуги, которые возникли за время самоизоляции. В письмах сообщается о задолженности и просьбой оплатить поддельные квитанции онлайн, либо предоставить сведения об уже совершенной оплате. В случае, если клиент начинал производить оплату и вводить реквизиты карточки на сайте, куда его привели ссылки из письма, мошенники получали доступ к его счету. В случае игнорирования клиентом подобных сообщений, ему звонили от лица управляющей компании и убеждали в наличии «долга по квартплате». При этом мошенники пытались выяснить способы оплаты и реквизиты карточки, по которой проводился платёж, и предлагали совершить «тестовую транзакцию для проверки», а также сообщить им код из SMS.

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!