Виды мошенничества в интернете и как не стать жертвой

Интернет стал настолько привычной частью нашей жизни, что иногда мы забываем, что не все, с кем мы пересекаемся онлайн, заботятся о наших интересах. Киберпреступники вездесущи и делают все возможное, чтобы извлечь выгоду, используя для этого обычных пользователей интернета, поэтому об угрозе онлайн-мошенничества нужно помнить всегда. Лучший способ защиты от онлайн-мошенников – знать о рисках и уметь их избегать. Здесь мы рассмотрим основные формы мошенничества в интернете и узнаем, как не дать себя обмануть.

1. Мошенничество с предложением работы

Этот вид мошенничества стал особенно популярен во время пандемии COVID-19. Суть в том, что вы получаете электронное письмо от незнакомого человека с предложением работы, обычно не имеющей отношения к области ваших знаний: например, вам предлагают поработать «тайным покупателем» или что-то в этом роде. Если вы принимаете предложение, с вами расплачиваются чеком или платежным поручением на сумму, которая несколько больше заранее оговоренной. После этого вас просят вернуть разницу. Разумеется, чек или платежное поручение оказываются фальшивкой, и вы лишаетесь тех денег, которые отправили фальшивому работодателю.

Благодаря широкому распространению сайтов для обмена деловыми контактами, таких как Linkedin, неожиданные предложения от работодателей стали обычным делом, а значит каждый, кто хочет заработать, должен уметь отличать настоящие предложения от мошеннических схем.

Как не стать жертвой мошенничества с предложением работы

Если вы согласились на предложение, никогда не обналичивайте подозрительные чеки не убедившись, что они не фальшивые. Для надежности попросите ваш банк заморозить средства, пока подлинность чека или платежного поручения не будет подтверждена. Если вас просят вернуть разницу – это явный признак того, что вы имеете дело с мошенником.

2. Мошенничество с лотереей

По некоторым данным, в 2020 г. мошенничество с лотереей стало в США четвертым по популярности видом мошенничества. Вот типичная схема: вам приходит электронное письмо с сообщением, что вы выиграли крупную сумму в неизвестной лотерее, обычно в другой стране. Для получения выигрыша вам предлагают заплатить деньги. Обычно мошенники утверждают, что это страховой сбор, подоходный налог, банковская комиссия или оплата услуг курьерской доставки. Вас также просят прислать данные для подтверждения вашей личности, и вот вы уже жертва кражи персональных данных, да и деньги ваши пропали.

У этой схемы есть еще один вариант: мошенник получает доступ к аккаунту своей жертвы в соцсетях, связывается с ее друзьями и родственниками и сообщает им, что все они выиграли деньги. Затем он присылает адрес электронной почты для получения инструкций о том, как получить выигрыш. Это особенно коварная схема, поскольку мошенник спекулирует на доверии между друзьями и членами семьи, чтобы выманить у них деньги.

Как не стать жертвой мошенничества с лотереей

У лотерейного мошенничества есть несколько явных признаков:

отправитель письма – физическое лицо, а не компания;

вы не единственный в списке адресатов;

вы первый раз слышите об этой лотерее.

Если вы получили подобное письмо, попробуйте поискать информацию в интернете, подтверждающую, что вы действительно выиграли деньги (это всегда оказывается неправдой). Люди склонны верить в счастливый случай но, если вы не покупали лотерейный билет, не стоит рассчитывать на выигрыш. Никогда не отправляйте свои персональные данные по электронной почте людям, которых вы не знаете лично, и никогда не верьте тем, кто обещает вам бесплатный сыр.

3. Мошенничество с переводом денег

Вы получаете электронное письмо от человека, которому нужно быстро перевести куда-то деньги. Иногда отправитель выдает себя за лицо королевской крови (вы наверняка слышали о «нигерийском принце»), но чаще – за бизнесмена, которому нужно вывести из страны несколько миллионов, и он просит вашей помощи в обмен на процент от суммы. В письме содержится ровно столько информации, сколько нужно, чтобы предложение выглядело правдоподобно. Но перевод денег неизбежно откладывается, а вы уже на крючке и вынуждены совершать множество мелких платежей – якобы, чтобы ускорить вывод денег.

Как не стать жертвой мошенничества с переводом денег

Если вы на мели, вы легко можете пойти на такую аферу. Но есть ряд признаков, по которым можно понять, что предложение не так хорошо, как кажется. Если письмо содержит орфографические и грамматические ошибки, а адрес для обратного ответа не совпадает с адресом отправителя, это снова повод вспомнить, что бесплатный сыр бывает только в мышеловке. Особенно это справедливо для интернета.

4. Мошенничество при онлайн-знакомстве

«Романтические» аферы встречаются все чаще. Вы знакомитесь с кем-то через приложение или сайт онлайн-знакомств, начинаете ближе узнавать друг друга, и вроде бы ничто не вызывает подозрений. Но вы не знаете, кто в действительности находится по ту сторону экрана. Если ваш виртуальный знакомый обращается к вам с просьбой выслать ему деньги или переправить кому-то вещи, которые он вам пришлет, – знайте, что вы столкнулись с мошенником.

Таких мошенников иногда называют кэтфишеры (catfishers). Они часто выдают себя за реально существующих людей, чтобы их обман выглядел правдоподобно, а подробности из жизни были убедительными. Но чтобы замести следы, они присылают поддельные фотографии и контактную информацию. Мошенничество на сайтах знакомств, или «романтические» аферы, имеют ряд характерных признаков:

демонстрация сильных эмоций уже в самом начале общения;

попытка сразу перейти с сайта или из приложения для знакомств в более приватные каналы общения;

просьба выслать деньги, чтобы выручить в трудной жизненной ситуации (например, на лечение родственника или на спасение бизнеса).

Как не стать жертвой мошенничества при онлайн-знакомстве

Чтобы не стать жертвой «романтической» аферы, нужно настороженно относиться к виртуальным отношениям, которые развиваются слишком быстро. Никогда не отправляйте деньги людям, с которыми вы не поддерживаете отношения в реальной жизни. Если вы договариваетесь с кем-то о встрече за пределами киберпространства, на всякий случай сообщите близким, куда вы идете.

5. Мошенничество, связанное с благотворительностью

После масштабных стихийных бедствий и других резонансных человеческих трагедий люди хотят помочь пострадавшим чем могут, и мошенники умеют на этом наживаться. Они создают поддельные сайты для пожертвований, открывают счета, а потом с помощью эмоционально заряженных писем

организуют сбор денег, которые никогда не доходят до пострадавших. Мошенники достигают успеха, поскольку спекулируют на человеческой эмпатии, поэтому всегда нужно изучать ситуацию. Проверяйте сайты для сбора пожертвований, чтобы убедиться, что они действительно собирают деньги на заявленные цели.

Как не стать жертвой мошенничества, связанного с благотворительностью

Чтобы не попасться на удочку интернет-мошенников, действующих под видом благотворительности, никогда не делайте пожертвования через сомнительные сайты. У реально существующего благотворительного фонда должен быть информативный веб-сайт, где заявлена миссия организации и представлены документы для налогового вычета. Чтобы проверить легитимность благотворительного фонда, поищите его в официальных базах данных, например Charity Check, CharityWatch, BBB Wise Giving Alliance или Charity Navigator.

6. Мошенничество, связанное с коронавирусом

Пандемия открыла перед злоумышленниками новые возможности. Они стали изобретать новые мошеннические схемы и подавать старые под новым соусом коронавирусных реалий.

Вот несколько примеров.

Мошенники выдавали себя за несуществующие благотворительные организации, чтобы собирать пожертвования от населения.

Мошенники предлагали поддельные тесты на коронавирус, несуществующие вакцины или лекарства, а также атаковали участников программы Medicare в попытке украсть их личные данные.

Мошенники создавали поддельные веб-сайты с картами распространения вируса COVID-19 и цифрами погибших и выздоровевших по отдельным странам. На самом же деле эти веб-сайты были рассадником компьютерных вирусов, вредоносных и шпионских программ, которые заражали устройства посетителей.

Как не стать жертвой мошенничества, связанного с коронавирусом

Как и в случае любого мошенничества, связанного с благотворительностью, проверяйте легитимность благотворительной организации по официальной базе данных. Ни в коем случае не переводите деньги и не сообщайте персональную информацию, реквизиты банковских карт или учетные данные к онлайн-аккаунтам незнакомым людям. Тщательно проверяйте каждый веб-сайт, чтобы убедиться, что он не поддельный. Не переходите по ссылкам и не открывайте вложения, которые содержатся в подозрительных письмах. Дополнительную информацию о том, как избежать мошенничества, связанного с коронавирусом, вы найдете в этой статье.

7. Ложная техподдержка

Этот вид мошенничества начинается в реальном мире, но быстро переходит в онлайн. Вам звонит человек, представляется сотрудником компании Microsoft или другой крупной компании-разработчика ПО и предлагает помощь в решении какой-либо компьютерной проблемы, например медленного интернета или низкой скорости загрузки данных. Предложение выглядит полезным, поэтому когда вам присылают по электронной почте ссылку на программу для удаленного доступа, вы ее загружаете и тем самым позволяете мошенникам получить контроль над вашим компьютером и установить на него вредоносное ПО. Не все пользователи хорошо ориентируются в компьютерных технологиях, очень многие даже не знают, как устроен компьютер, и мошенникам легко их обмануть. Установив вредоносное ПО, мошенники получают доступ к файлам, персональным данным и другой личной информации.

Как не поддаться на уловку ложной техподдержки

Никогда не слушайте непрошеных советчиков и не заказывайте никакие ремонтные работы, пока не убедитесь в том, что говорящий действительно тот, за кого себя выдает. Не предоставляйте никому удаленный доступ к вашему компьютеру. Если вам звонит неизвестный, попросите его предоставить информацию, которая подтвердит его статус. Не исключено, что если вы будете задавать много вопросов, мошенник поймет, что вас не удастся обмануть.

8. Мошенничество в соцсетях

Мошенничество в соцсетях становится все более распространенным и разнообразным по форме.

Вот несколько примеров.

Вам предлагают пройти тест в соцсети: определить свой тип личности или узнать, на какую знаменитость вы похожи, или обещают заманчивый приз за победу в викторине. В условиях участия обычно содержится пункт, разрешающий продажу предоставленной вами информации третьим лицам. Кроме того, разработчик теста может получить доступ к данным вашего профиля, списку друзей и IP-адресу. Обладая всей этой информацией, мошенник может начать выдавать себя за вас в интернете.

Вам приходит запрос на дружбу в Instagram от мошенника, который выдает себя за вашего знакомого. После этого он присылает вам фишинговую ссылку, которая ведет на вредоносный веб-сайт.

Вы загружаете из соцсети приложение, которое вам кажется легальным, а на самом деле устанавливает на ваше устройство вредоносное ПО.

Как не стать жертвой мошенничества в соцсетях

Никогда не участвуйте в тестах, не нажимайте на всплывающие уведомления или окна, в которых содержится шокирующий контент или предложения, которые слишком хороши, чтобы быть правдой. Не переходите по ссылкам и не открывайте вложения, содержащиеся в письмах из неизвестных источников.

С осторожностью относитесь к сокращенным URL-адресам, которые скрывают полное местоположение веб-страницы. Такие адреса часто встречаются в сети Twitter, и, хотя обычно они безобидны и ведут на соответствующий веб-сайт, всегда есть шанс, что они перенаправят вас на сайт, зараженный вредоносным ПО.

9. Мошенничество с использованием голосовых ботов

Если вы слышите в трубке не живого человека, а записанный голос – значит, это голосовой бот. Голосовые боты иногда несут полезную информацию, например напоминают о записи на прием или сообщают об отмене рейса. Но чаще всего их используют для «холодных» маркетинговых звонков, среди которых нередко встречаются мошеннические.

Существует способов мошенничества в интернете с использованием голосовых ботов.

Звонок от имени налоговой службы с требованием оплатить несуществующую налоговую задолженность и угрозой в противном случае заблокировать номер социального страхования.

Звонок от имени крупной технологической компании, такой как Apple, с просьбой предоставить информацию, которую настоящая компания никогда бы не стала запрашивать у клиента по телефону.

Звонок с предложением бесплатной пробной версии продукта или услуги с целью выманить реквизиты вашей банковской карты.

Боитесь телефонных мошенников?

Пусть они боятся вас!

Как не стать жертвой мошенничества с помощью голосовых ботов

Лучше всего вообще не отвечать на звонок, если вы подозреваете, что звонит бот. Не всегда это можно понять заранее, поэтому если уж вы ответили на звонок, повесьте трубку сразу же, как только поймете, что это голосовой бот. Не следуйте инструкциям бота, например: «Нажмите цифру 1 для связи с оператором» и т. п. По возможности не произносите слово «да». Многие роботизированные звонки начинаются с вопроса: «Здравствуйте, вы хорошо меня слышите?», на который многие автоматически отвечают: «Да». Мошенники записывают звук, чтобы потом использовать запись в своих неблаговидных целях.

Любой ответ или позитивная реакция на такой звонок является сигналом для мошенника, что вы – перспективный объект, так что лучше всего свести взаимодействие к минимуму. В США о роботизированных звонках можно сообщать в Федеральную торговую комиссию через сайт donotcall.gov.

10. Мошеннические сообщения

Мошенники используют службы передачи сообщений и мессенджеры, такие как SMS, WhatsApp, Facebook Messenger, Viber, Skype, Google Hangouts и другие, чтобы выманивать у людей деньги. Фишинг с использованием службы SMS даже получил название «смишинг».

Существует множество мошеннических схем с использованием мессенджеров. Вот несколько примеров.

Вы получаете SMS-сообщение о том, что вам пришла посылка, для получения которой необходимо подтвердить свою личность или оплатить стоимость доставки.

Вы получаете сообщение якобы от вашего банка о том, что ваш счет будет закрыт или ваша дебетовая карта будет заблокирована, а на вас будет наложен штраф. Чтобы этого не случилось, вам нужно подтвердить свой аккаунт (разумеется, на поддельном веб-сайте).

Вы получаете сообщение о крупном выигрыше, но, чтобы получить его, вы должны сообщить свои платежные реквизиты.

Как не попасться на удочку мошеннических сообщений

Если организация, от имени которой пришло сообщение, раньше не связывалась с вами через мессенджер, это первый тревожный сигнал. Официальные организации не будут отправлять неожиданные сообщения через мессенджер с просьбой предоставить им личные или конфиденциальные данные. Проверьте, нет ли в сообщении орфографических или грамматических ошибок. Если сообщение выглядит непрофессионально – возможно, это признак онлайн-мошенничества. Если у вас возникли сомнения, не переходите по ссылкам и не сообщайте никакую персональную или финансовую информацию.

11. Поддельные интернет-магазины

Новейшие технологии позволяют создавать поддельные сайты интернет-магазинов, которые выглядят совсем как настоящие. Мошенники крадут логотипы и копируют дизайн страниц. На таких сайтах пользователям предлагают популярные бренды одежды, ювелирных изделий или электроники по низким ценам. Иногда пользователи получают оплаченный заказ, но чаще всего нет. В последнее время мошенники часто создают интернет-магазины в соцсетях. Такие магазины довольно быстро исчезают, чтобы вновь возродиться под другим названием. Дополнительную информацию о том, как безопасно совершать покупки в интернете, вы найдете в этой статье.

Как распознать поддельный интернет-магазин

Если какой-либо товар предлагают по невероятно низкой цене – это явный признак мошенничества. Еще один признак – если продавец настаивает на предоплате или оплате электронным или телеграфным переводом. Иногда вам даже предлагают приобрести ваучеры, чтобы получить доступ к распродаже или промоакции.

Как распознать поддельные веб-сайты

Важный элемент вашей интернет-безопасности – умение распознавать поддельные веб-сайты. Вот несколько советов, как избежать мошеннических веб-сайтов.

Всегда проверяйте доменное имя сайта, особенно если вы переходите на него по ссылке, содержащейся в электронном письме или на другой веб-странице. Домены мошеннических веб-сайтов часто очень похожи на домены хорошо известных брендов или организаций и могут отличаться от них всего одной буквой или лишним словом.

Если у вас возникли сомнения, поищите дополнительную информацию о домене. Сервис поиска доменов Whois Lookup domain tracker содержит информацию о том, на кого, когда и где именно зарегистрирован домен.

Полезно бывает проверить и адресную строку веб-сайта. Любой сайт, на котором вас просят ввести персональные данные, должен быть защищенным и его URL-адрес должен начинаться не с http://, а с https://. Буква «s» как раз и означает, что сайт защищен. Об этом же говорит и значок замка в адресной строке. Этот значок означает, что у сайта есть сертификат безопасности SSL.

О надежности сайта можно судить и по его содержимому. Если контент выглядит небрежно и содержит орфографические или грамматические ошибки – это тревожный сигнал. Если на сайте интернет-магазина мало информации или отсутствуют условия предоставления услуг, политика конфиденциальности или правила возврата товара, это может свидетельствовать о том, что сайт поддельный.

При покупке товара онлайн проверьте наличие безопасных способов оплаты. Легитимные веб-сайты предлагают стандартные способы оплаты – с помощью банковской карты или через сервис PayPal. Если на сайте вам предлагают оплатить покупку телеграфным переводом, с помощью платежного поручения или другим небезопасным (и невозвратным) способом, безопаснее будет воздержаться от такой покупки.

Еще одним полезным инструментом проверки веб-сайтов являются отзывы клиентов. Их нужно искать на специальных сайтах-агрегаторах отзывов. Если все отзывы кажутся до странности похожими друг на друга или оставлены совсем недавно – имейте в виду, что они могут быть заказными. Если отзывы вообще отсутствуют, это повод насторожиться.

Мошенники могут атаковать в любой момент!

Как не стать жертвой кибермошенников

Вот несколько простых профилактических рекомендаций для тех, кто не хочет стать жертвой кибермошенников.

1. С осторожностью относитесь к просьбам перевести деньги или сообщить персональную информацию

Не сообщайте реквизиты банковских карт или данные для входа в онлайн-аккаунты, не отправляйте деньги или копии личных документов незнакомым людям. Используйте только безопасные способы оплаты, которые вам известны. Не соглашайтесь на просьбу переслать кому-то деньги или вещи: отмывание денег карается законом.

2. Остерегайтесь фишинга

Фишинг – это составная часть многих мошеннических схем. Не переходите по ссылкам и не открывайте вложения, содержащиеся в письмах или сообщениях из сомнительных источников. Не реагируйте на неожиданные сообщения или звонки с просьбой предоставить личную или финансовую информацию.

3. Не реагируйте на звонки с просьбой предоставить удаленный доступ к вашему компьютеру

Если звонящий представляется сотрудником крупной телекоммуникационной или технологической компании и хочет получить доступ к вашему компьютеру, чтобы решить какую-то проблему, немедленно повесьте трубку. На самом деле ему нужен доступ к вашему компьютеру, чтобы установить на него вредоносное ПО, с помощью которого он сможет похитить ваши пароли и другие личные данные.

4. Защищайте свои мобильные устройства и компьютеры

Для защиты устройств используйте пароли и никому не предоставляйте доступ к ним (включая удаленный). Установите пароль для защиты своей беспроводной сети и не пользуйтесь общедоступными компьютерами или сетями Wi-Fi для входа в интернет-банк или для передачи персональной информации.

5. Используйте надежные пароли

Надежный пароль сложно подобрать, в идеале он должен представлять собой комбинацию заглавных и строчных букв, специальных символов и цифр. Люди часто годами не меняют пароли, что снижает их надежность. Менеджер паролей – отличный инструмент для управления вашими паролями.

6. Проверьте настройки безопасности и конфиденциальности ваших аккаунтов в соцсетях

Если вы пользуетесь социальными сетями, будьте осторожны при общении и используйте настройки конфиденциальности и безопасности, чтобы защитить себя. Если кто-то из пользователей ведет себя подозрительно, если вы открыли спам-сообщение или столкнулись с мошенником, примите меры для защиты своего аккаунта и сообщите о нарушении.

7. Не подключайтесь к стримам на незнакомых сайтах

Стриминговый контент на незнакомых и, возможно, пиратских веб-сайтах с большой вероятностью может быть источником вредоносного ПО. Киберпреступники часто предлагают пиратский контент бесплатно, чтобы заманить побольше посетителей. Пользуйтесь только хорошо известными и надежными стриминговыми платформами.

8. Игнорируйте требование действовать немедленно

Легитимные компании всегда дают время на размышление. Если кто-то начинает давить на вас и требовать заплатить деньги или сообщить персональную информацию, возможно, это мошенник.

9. Бесплатный сыр бывает только в мышеловке

Если на каком-либо сайте или при общении в интернете вам предлагают невероятно большие скидки или нереально крупные призы, будьте осторожны. Как говорится в известной пословице, бесплатный сыр бывает только в мышеловке.

В общем, будьте бдительны и с настороженностью относитесь к неожиданным электронным письмам или звонкам с требованием предоставить персональные данные. В США о случаях онлайн-мошенничества можно сообщить в Федеральную торговую комиссию. Аналогичные организации существуют и в других странах мира.

Лучший способ обезопасить себя от интернет-мошенников – установить защитное ПО на все ваши устройства и регулярно обновлять его. Остерегайтесь поддельных антивирусных программ: обычно мошенники под их видом распространяют вредоносный код. Приобретайте и скачивайте антивирусное ПО только на официальном сайте производителя.