Миллионы людей во всем мире используют сайты и приложения онлайн-знакомств, и есть множество счастливых историй, когда люди находили в интернете любовь и близкие отношения. Но наряду со счастливыми историями, в области онлайн-знакомств также имеет место мошенничество, и оно происходит все чаще.

Мошенничество в сфере онлайн-знакомств происходит, когда одна сторона считает, что удалось найти пару на сайте или в приложении для онлайн-знакомств, а вторая сторона на самом деле является мошенником, использующим поддельный профиль. Мошенник манипулирует или оказывает собеседнику знаки внимания, чтобы со временем завоевать его доверие. Однако конечная цель мошенника – либо попросить деньги, либо получить личную информацию для кражи персональных данных.

Пандемия коронавируса, препятствовавшая личному общению и вынудившая людей проводить больше времени в интернете, создала условия, которыми могли воспользоваться мошенники на сайтах онлайн-знакомств.

Хотя жертвой мошенничества на сайтах онлайн-знакомств может стать каждый, люди в возрасте часто несут более тяжелые финансовые потери. Они интересуют мошенников, поскольку с большей вероятностью обладают активами, пенсионными накоплениям или недвижимостью, заполучить которые становятся целью злоумышленников. Считается, что [приблизительно две трети жертв мошенничества на сайтах онлайн-знакомств – это женщины](https://www.bbc.co.uk/news/business-47176539), средний возраст которых около 50 лет.

Мошенничество в сфере онлайн-знакомств совершается с особой жестокостью, поскольку подразумевает игру на чувствах людей.

В этой статье дается краткий обзор мошенничества, совершаемого при онлайн-знакомствах, признаки такого мошенничества, как о нем сообщить, а также приведены рекомендации, как избежать недобропорядочных «претендентов на ваше сердце».

 **Распространенные виды мошенничества при онлайн-знакомствах**

Мошенничество при онлайн-знакомствах обычно начинается невинно. Мошенники создают «фейковые» профили, которые при этом максимально привлекательны, и жду т, когда найдутся желающие познакомиться с ними. Они также могут первыми начать общение, упоминая общие интересы или утверждая, что они каким-то образом знакомы с жертвой. После того, как жертва «попалась на крючок», возможности мошенника неограниченны, но при этом существуют наиболее распространенные схемы, описанные ниже.

**Знакомство с солдатом**

Для онлайн-знакомства с военным мошенники могут использовать данные реально существующего человека, или создать полностью фиктивный профиль. Они рассылают письма, которые внешне не вызывают сомнений, где рассказывают, что скоро выходят на пенсию; обычно у них «есть взрослые дети», и они «потеряли жену при трагических обстоятельствах». Сообщения насыщены военным жаргоном, воинскими званиями, названиями военных баз – все это производит впечатление на жертву. У жертвы возникает эмоциональная привязанность, однако, перед возможным личным знакомством солдату «приходит приказ на передислокацию».

После этого начинаются просьбы переслать деньги, чтобы оплатить интернет, купить билеты домой, расширить военную медицинскую страховку, оплатить лечение или пенсионное обеспечение. В большинстве случаев мошенник работает с соучастниками, которые выступают в роли докторов и юристов – таким образом мошенники стараются обеспечить постоянный приток денег от жертвы. Часто такое «военное» мошенничество продолжается месяцы или даже годы, и только затем жертва начинает что-то подозревать.

**Откровенные разговоры**

При этой мошеннической схеме на контакт с жертвой выходят потенциальные «поклонники», живущие за границей. Они добавляются в друзья в нескольких социальных сетях. После периода активного ухаживания, мошенник приглашает жертву поговорить по веб-камере. У мошенника камера «случайно» оказывается сломанной, при этом он осыпает жертву комплиментами и, сочетая лесть с настойчивостью, убеждают жертву частично раздеться или выполнить другие откровенные действия. После этого мошенник раскрывает свою истинную сущность, говорит, что сделал видеозапись разговора, и угрожает, что поделится ею с общими друзьями в социальных сетях или опубликует ее в интернете. Единственный способ избежать этого – заплатить. Как только жертва соглашается, требуемые суммы начинают увеличиваться до тех пор, пока жертва не откажется пересылать деньги.

**Поддельные сайты знакомств**

Мошеннические сервисы знакомств несколько отличаются от обычных [мошеннических веб-сайтов](https://www.kaspersky.ru/resource-center/preemptive-safety/scam-websites). Они якобы предлагаю добропорядочные знакомства, однако на них крайне мало зарегистрированных пользователей и очень много мошенников. Некоторые мошеннические сайты используют созданные профили специально для получения информации о пользователях. Следует остерегаться, если в анкете, заполняемой при регистрации, запрашивается мало личных данных, но при этом много вопросов про личные финансы или таких вопросов, как девичья фамилия матери или номер вашей первой школы (это общие вопросы безопасности).

Некоторые бесплатные сайты знакомств на первый взгляд кажутся легальными, но после определенного времени использования становится понятно их настоящее предназначение. Например, на них предлагается заполнить анкету с вопросами, аналогичными используемым для банковских операций, в обмен на бесплатное премиум-членство или другие эксклюзивные привилегии. Никогда не следует сообщать информацию, которая может быть использована для доступа к личным или финансовым данным, независимо от предлагаемого вознаграждения.

Также следует быть осторожным, если сразу после создания ваш профиль привлекает избыточное внимание. Если в вашем профиле лишь несколько строк текста, нет фото и не установлено предпочтений, и при этом вы начинаете получать от потенциальных поклонников одно сообщение за другим, велика вероятность того, что вы попали на поддельный сайт знакомств.

**Проверка учетной записи**

Это один из распространенных видов мошенничества в Tinder, в рамках которого выполняется рассылка электронных писем или текстовых сообщений с просьбой подтвердить свою учетную запись Tinder. В сообщении утверждается, что Tinder обновляет записи, и содержится просьба подтвердить вашу учетную запись. Другой вид мошенничества – запрос на верификацию со стороны совпавшей пары в Tinder, для того, чтобы начать общение.

В этих примерах мошенники вынуждают перейти по сторонней ссылке для подтверждения учетной записи. После перехода по ссылке требуется ввести личные данные, такие как имя, адрес, номер телефона, адрес электронной почты, номер полиса социального страхования, дату рождения и даже данные банковского счета или кредитной карты.

В Tinder существуют проверенные учетные записи, но их проверка делается исключительно внутри Tinder. Чтобы получить синий флажок рядом с именем, пользователям необходимо сделать серию селфи, которые затем сравниваются с фотографиями в их профиле для проверки соответствия. Поэтому будьте очень внимательны, если предлагается воспользоваться другими средствами проверки.

**Вредоносные программы**

[Вредоносные программы](https://www.kaspersky.ru/resource-center/threats/malware-protection) являются распространенной угрозой в интернете, в том числе на сайтах знакомств. Например, в Tinder, после обмена несколькими сообщениями, собеседник может предложить посмотреть его личную веб-страницу или поддельные профили Facebook или Instagram.

Это мошеннические страницы, и в результате вы будете перенаправлены на веб-страницу, содержащую вредоносные программы и спам, используемые злоумышленниками для кражи ваших личных данных, что может привести к возможному финансовому мошенничеству. Как правило, если ваш собеседник на сайте знакомств пытается перенаправить вас на другой сайт, это следует рассматривать как потенциальную опасность.

**Мошенничество с фотографиями**

В этом случае мошенник пытается выудить у жертвы контактные данные в обмен на свои интимные фотографии. Для этого может использоваться даже специальный [мошеннический бот](https://www.kaspersky.ru/resource-center/definitions/what-are-bots), который играет на чувствах и эмоциях (предлагая показать фотографии) жертвы, чтобы получить доступ к данным, которые затем могут быть использованы для финансового мошенничества.

**Мошенничество с наследством**

В этом случае мошенница (обычно, молодая женщина) заявляет, что ей нужно выйти замуж, чтобы унаследовать миллионы долларов золотом, оставленные отцом, дядей или дедом. Предполагается, что брак является обязательным условием получения наследства со стороны родственника-мужчины. С жертвой связывается молодая женщина и объясняет, что она не может вывезти золото из своей страны, поскольку не может заплатить пошлину или налоги на заключение брака.

Как только с жертвой устанавливаются достаточно доверительные отношения, она просит денег, чтобы доставить золото в страну жертвы. Мошенница также предлагает прилететь в страну жертвы, чтобы доказать свое реальное существование, и жертва отправляет ей деньги на перелет. Излишне говорить, что мошенница так никогда не прилетит.

**Варианты мошенничества при онлайн-знакомствах**

Некоторые истории могут показаться неправдоподобными, однако важно помнить, что потенциальные жертвы часто одиноки и уязвимы. Мошенники очень хорошо умеют играть на эмоциях и красиво ухаживать. Вот типичные виды мошенничества в сфере онлайн-знакомств:

Мошенник просит жертву отправить ему деньги для оплаты авиабилетов (или паспорта) для посещения страны жертвы.

Мошенник просит жертву оплатить его счета за телефон или купить ему новый ноутбук, чтобы они могли продолжить общение.

Мошеннику нужны деньги для оплаты лечения: своего или близкого родственника.

Мошенник утверждает, что владеет драгоценностями, конфискованными таможней, и чтобы вернуть эти драгоценности нужно заплатить налог. После этого он сможет приехать к жертве.

Мошенник рассказывает, что получил зарплату почтовым денежным переводом, и просит жертву обналичить поддельные денежные переводы, а затем перечислить ему деньги. В итоге банк отменяет почтовый денежный перевод, но не банковский перевод.

Мошеннику нужны деньги, чтобы завершить обучение, и тогда он сможет посетить жертву.

Термин кэтфишинг часто используется в контексте мошенничества в сфере онлайн-знакомств. Кэтфишинг – это создание вымышленной или поддельной личности в социальных сетях или на сайтах знакомств с целью охоты на конкретную жертву. Помимо получения финансовой выгоды, кэтфишинг может использоваться для причинения жертве страданий или ущерба, а возможно, злоумышленник хочет таким образом реализовать свои фантазии.

**Признаки мошенничества при онлайн-знакомствах: на что обращать внимание**

Независимо от платформы или приложения: кэтфишинг в Facebook, мошеннические знакомства в Instagram и прочих местах – существуют следующие сигналы, предупреждающие о мошенничестве с онлайн-знакомствами.

Мошенники пытаются быстро перейти с сайта или приложения для знакомств

Это связано с тем, что в приложениях для онлайн-знакомств часто существуют группы обслуживания клиентов, которые отслеживают странное поведение. Если они заметят, что кто-то отправляет одно и то же сообщение множеству пользователей, или другую необычную активность, они могут расценить ее как подозрительную. Чтобы этого избежать, мошенники пытаются перевести общение на другую платформу, например, в WhatsApp или аналогичный мессенджер. Они могут использовать следующие оправдания: «Мое членство скоро истечет», «Мне не нравится заходить сюда каждый день» или «В WhatsApp удобнее общаться, чем здесь».

Общение очень быстро сводится к романтическому

Часто при мошенничестве с использованием поддельного профиля злоумышленник очень быстро становится серьезным: может засыпать экстравагантными комплиментами, утверждать, что влюбился, убеждать в возникновении особой связи, о родстве душ, и что никогда раньше ни к кому так не относился. Жертвы обычно сообщают, что это происходит на ранней стадии общения.

Мошенник задает много личных вопросов

Причина такого поведения: чем больше он знает о вас, тем легче ему будет вами манипулировать. Мошенник тоже рассказывает о себе и даже может предложить пообщаться по телефону. Этот этап может длиться неделями и даже месяцами.

**Противоречивый рассказ о себе**

Когда кто-то лжет, он может забыть, что именно рассказывал раньше. Кроме того, мошенники иногда действуют в команде, и за одной личностью могут скрываться разные люди. Так что, если ваш собеседник кажется непоследовательным, обратите на это внимание. Если что-то в его историях не соответствуют рассказанному раньше, это может быть признаком обмана.

**Фото в профиле похоже на модельное**

При мошенничестве с использованием поддельного профиля часто используют красивые модельные фото, чтобы привлечь жертву. Это могут быть фотографии актеров или моделей, или даже стоковые изображения. Если фото профиля выглядит слишком красивым, несложно проверить, является ли оно настоящим. [Обратный поиск по фотографии](https://support.google.com/websearch/answer/1325808?hl=en) покажет, встречается ли это фото профиля где-либо еще в интернете.

**Отсутствие цифрового следа**

Некоторые люди не используют социальные сети и стараются свести к минимуму доступную в интернете личную информацию о себе, однако если не удается найти вообще никаких следов человека в интернете, это выглядит подозрительно.

**Использование чужого текста**

Зачастую мошенники не утруждаются написанием в своем профиле оригинального текста, а берут его с других веб-сайтов или из профилей на сайтах знакомств. Имеет смысл поискать подозрительный текст в поисковике. Если он найдется в других местах, не следует отвечать этому человеку.

**Уклонение от общения по Скайпу, видеосвязи и личных встреч**

Собеседник всегда находит причину, по которой личное или видео-общение невозможно. Жертвы мошенничества обычно сообщают, что их собеседник постоянно извинялся и избегал появляться перед камерой. Очевидная причина этого – он не похож на фото профиля, а также хочет избежать идентификации с дальнейшим отслеживанием.

**Жизнь как мыльная опера**

Мошенники, использующие поддельные профили, часто рассказывают истории, связанные с болезнями, семейными трагедиями, несчастными случаями, чтобы вызывать сочувствие и отложить личную встречу. Если история жизни вашего потенциального избранника кажется невероятной, возможно, это афера.

**Отношения на расстоянии**

Мошенники пытаются завязать отношения на расстоянии, поскольку это позволяет уклоняться от личной встречи, а также дает время на ухаживания и попытки завоевать доверие. В рассказах таких мошенников всегда находится причина, объясняющая сложность личной встречи. Если же они договариваются о встрече, то потом отменяют ее в последний момент.

**Просьбы денег**

Основной признак того, что вы имеете дело с мошенником – это просьбы денег. Все ухаживания и манипуляции, которые могут длиться неделями или даже месяцами, заканчиваются просьбами денег. Вам могут приводить различные причины, но, разумеется, на такие просьбы следует отвечать отказом.

**Как сообщить о мошенничестве на сайтах онлайн-знакомств**

Если вы стали жертвой мошенничества на сайте знакомств, не стесняйтесь об этом говорить. Жертвы такого мошенничества стараются не афишировать случившееся, поскольку им может быть стыдно или неприятно рассказывать об этом, особенно когда они осознали, что их обманули.

Также стоит сообщить о мошенничестве на самом сайте или в приложении. Отправьте имя пользователя-мошенника и как можно больше связанной с мошенничеством информации, включая диалоги и транзакции, чтобы модераторы сайта могли принять меры для защиты других пользователей.

В случае денежных потерь, как можно скорее свяжитесь с банком и объясните им ситуацию.

**Советы по безопасности: как защититься от мошенников на сайтах знакомств**

Ниже приведено 12 советов, как избежать мошенничества при онлайн-знакомствах:

Не принимайте предложения дружбы от незнакомцев в социальных сетях.

Не раскрывайте слишком много личной информации в профиле на сайте знакомств или человеку, с которым вы общались только в интернете. Мошенники могут использовать вашу фамилию или данные о месте работы для манипуляций или кражи личных данных.

Используйте известные сайты знакомств и общайтесь посредством их службы обмена сообщениями. Мошенники быстро захотят перейти на текстовые сообщения, общение в социальных сетях или по телефону, чтобы на сайте знакомств не осталось свидетельств того, что они просят у вас денег.

Не торопитесь. Задавайте собеседнику вопросы и следите за возможными несоответствиями в его ответах. Это поможет выявить мошенника.

Остерегайтесь излишне льстивых сообщений. Вставьте текст сообщения в поисковик и посмотрите, находятся ли такие же фразы на веб-сайтах, посвященных разоблачению мошенничества при онлайн-знакомствах.

Не испытывайте ложного чувства безопасности из-за того, что это вы инициировали общение. В приложениях и на сайтах знакомств полно мошенников с поддельными профилями, ожидающих жертв.

Не отправляйте незнакомцам компрометирующие фотографии, которые впоследствии могут быть использованы для вымогательства.

Немедленно прекратите общение, если возникнет подозрение, что вы ведете диалог с мошенником. Уведомьте администрацию сайта знакомств или приложения, на котором вы встретили мошенника.

Не переходите по ссылкам в профилях пользователей и в полученных сообщениях, если кажется, что они не имеют отношения к диалогу.

Если вы решили встретиться с потенциальным партнером лично, сообщите родным и друзьям, куда вы собираетесь, и назначьте встречу в общественном месте. Не рекомендуется ехать за границу, чтобы встретиться с тем, кого вы никогда раньше не видели.

Никогда не отправляйте деньги или подарочные карты, а также не разглашайте свои банковские реквизиты тем, с кем вы знакомы только по интернету.

Для обеспечения безопасности в интернете важно использовать комплексное антивирусное решение, способное защитить вас от злоумышленников, вирусов и вредоносных программ.

Жертвами мошенничества на сайтах онлайн-знакомств часто становятся уязвимые пользователи. Однако, умея определять распространенные виды мошенничества с использованием поддельных профилей и зная, как избежать такого мошенничества, можно обойти опасности и найти настоящую любовь.