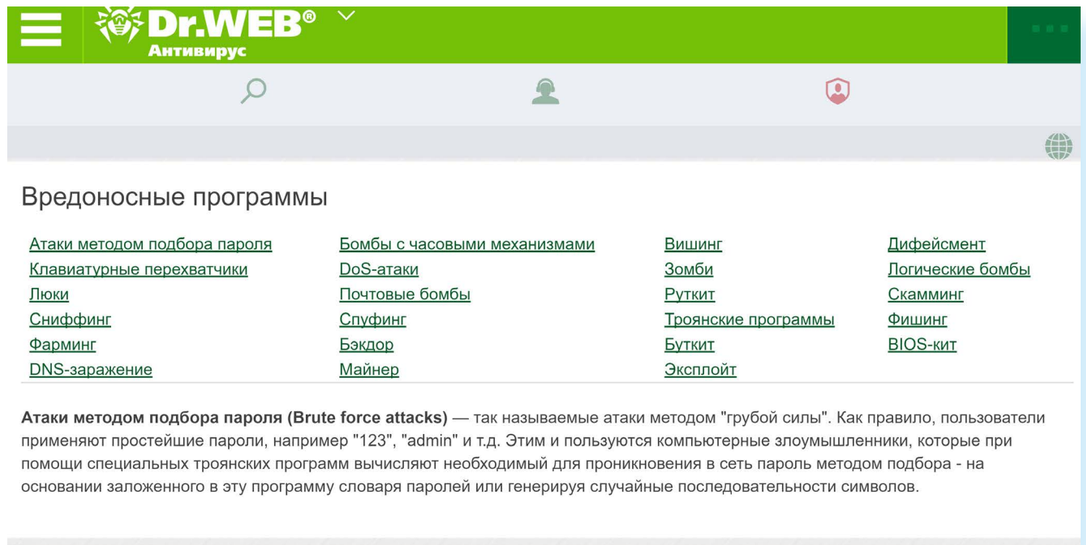
# Как действуют мошенники в интернете, способы защиты

3 ГЛАВА

Мошенники в интернете преследуют главную цель – получить деньги либо заработав на продаже личных данных, либо просто украв ваши деньги. Для этого есть технологические способы, когда, используя уязвимость вашего устройства, мошенники с помощью вредоносных программ получают доступ к вашим данным и счетам, а есть то, что называют «социальной инженерией», когда используют психологические способы влияния на пользователей для кражи личных средств.

## Вредоносные программы

Один из самых распространенных способов перехватить у вас информацию – запуск на ваше устройство вредоносных программ. Развиваются цифровые технологии, совершенствуются шпионские IT-инструменты. Вот, например, какой список вредоносных программ можно увидеть на сайте антивирусной программы «Доктор Web» 3.1. 3.1



Остановимся на основных разновидностях.

**Вирус** – это программа, которая внедряется в установленные программы и приложения на компьютере. Вирус начинает работать тогда, когда вы запускаете данную программу или приложение.

Подцепить вирус можно на зараженном сайте, нажав на ссылку или файл в подозрительном сообщении или письме, или кликнув на всплывающие окно, призывающее вас обязательно перейти на какой-то ресурс.

Правда, сейчас вирусов становится меньше. Их быстро распознают и блокируют и настройки браузера, и операционной системы, и антивирусной программы.

**Червь** – тоже вирус, но действует по-другому: распространяет сам себя по компьютеру. Его также можно «занести» через ссылки или файлы в переписке.

**Руткит** – это особая часть вредоносных программ, которая разработана так, чтобы скрыть свое присутствие в операционной системе от защитного программного обеспечения.

Однако сложные современные антивирусные программы в состоянии обнаружить и обезвредить практически все существующие разновидности руткитов.

**Троян**, как правило, загружается на устройство под видом законного приложения, но на самом деле делает то, что нужно злоумышленникам. Это одна из распространенных вредоносных программ.

С годами трояны становятся все сложнее: есть трояны-бэкдоры, которые пытаются взять на себя управление компьютером, трояны-загрузчики, устанавливающие вредоносные коды, или трояны-вымогатели.

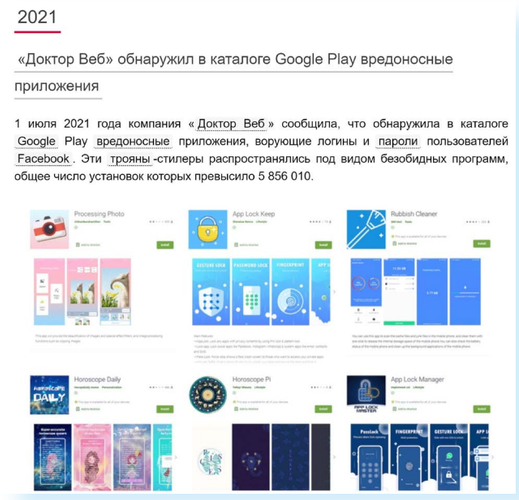
Подцепить трояна можно легко при скачивании программ, приложений или даже просто картинок.

Вот как действовал «скайповский» троян. Он отправлял слово «Привет» всем пользователям в списке контактов жертвы каждый раз, когда она выходила в онлайн. На самом деле троян вместе с «приветом» отправлял еще и фишинговую ссылку (ссылку, которая вела на подставной сайт).

Достаточно много троянов антивирусные программы находят и в мобильных приложениях, в том числе даже в тех, которые можно найти в официальном магазине Google Play 3.2.



3.2




Один из самых опасных троянов – вымогатель, или шифровальщик. «Поселившись» в устройстве, он шифрует файлы, а иногда и всю систему, и требует деньги за расшифровку.

Даже если вы найдете и удалите с помощью антивирусной программы вредоносного шифровальщика, файлы могут так и остаться зашифрованными.

Чтобы не стать жертвой вредоносного программного обеспечения, нужно соблюдать простые правила:

- не открывать подозрительные письма или сообщения от незнакомых пользователей в электронной почте и мессенджерах;
- не переходить по рекламным баннерам, сулящим выигрыши или слишком дешевые предложения покупки;

Например, мошенники часто ловят пользователей на любопытстве. Вы можете увидеть громкие сообщения типа «Секретные подробности из жизни Аллы Пугачевой». Вы нажимаете на ссылку, а там вас просят скачать последнюю версию Adobe Flash, но вместо программы Adobe Flash вы получаете вредоносную программу на ваш компьютер.

- устанавливать программы и приложения только с официальных сайтов;
- обращать внимание на настройки безопасности в мобильных приложениях, ограничивать доступ приложения к вашим данным;
- проверять на безопасность подключенные к вашему устройству переносные USB-накопители;
- по возможности делать резервные копии данных со своего компьютера.

**Как могут быть занесены вредоносные программы на устройство?**

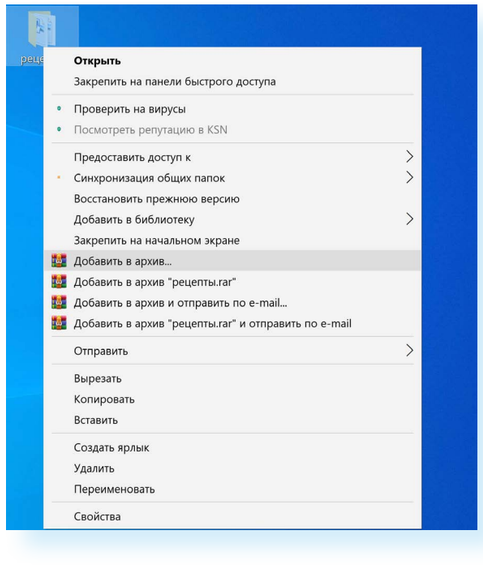
- Через ссылки и файлы, присланные в подозрительных письмах или сообщениях.
- При нажатии на рекламный баннер, обещающий большой выигрыш или выгодную покупку.
- Через USB-накопитель.
- При установке программы или приложения с неофициального сайта.

Например, копии важных файлов можно хранить на USB-накопителях или в облачном хранилище.

Чтобы разместить папку с фотографиями в облачном хранилище Яндекс. Диска, нужно:

**1.** Подготовить папку с фотографиями. Вы можете ее сжать, тогда она займет меньше места в облачном хранилище. Наведите на нее курсор и кликните правой кнопкой мыши. В открывшемся меню выберите программу для архивирования файлов. В нашем примере WinRAR 3.3.

3.3



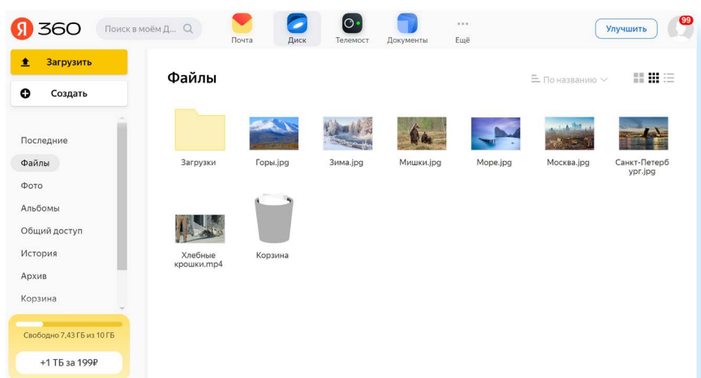

**2.** Завести аккаунт в системе Яндекс. Можно просто зарегистрировать электронную почту на Яндексе.

*Подробнее как завести электронную почту можно увидеть в главе 7 «Электронная почта» базового курса «Азбука интернета».*

**3.** Затем зайдите в свою электронную почту, выберите вверху вкладку «Диск».

**4.** Выберите «Загрузить файлы» 3.4.

3.4






**5.** В открывшемся окне найдите на компьютере вашу заархивированную (сжатую) папку. Выделите ее. Нажмите «Открыть». Папка загрузится.

Теперь папка будет храниться в облачном хранилище, которое привязано к вашей Яндекс.Почте. Зная логин и пароль от электронной почты, вы всегда сможете получить доступ к данной папке с любого компьютера. А, значит, восстановить ваши фотографии, если вдруг они будут удалены на компьютере трояном.

## Как выбрать антивирус

Самой надежной защитой для компьютера, конечно, станет установка антивирусной программы.

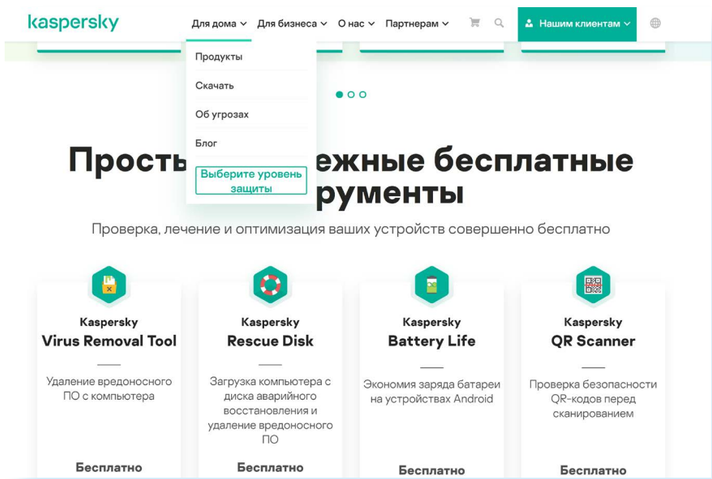
**Если на компьютере не установлена антивирусная программа, мы не советуем выходить в интернет, так как в этом случае очень высок риск заражения устройства вредоносными программами.**

Антивирусные программы могут быть бесплатными и платными. Как правило, в бесплатных версиях их функционал ограничен.

Но часто крупные известные компании именно бесплатно предоставляют доступ к небольшим программам, которые сканируют и помогают удалить различные зловредные программы в ситуации, когда вы видите, что компьютер, скорее всего, «заражен».

Например, на сайте Лаборатории Касперского, чтобы скачать такую программу (утилиту), нужно вверху выбрать раздел «Для Дома», а затем нажать на пункт «Скачать». Откроется страница, где внизу вы найдете блок «Простые и надежные бесплатные инструменты». Как видите, две из них для мобильных телефонов, в том числе на проверку QR-кодов, которые тоже могут перенаправлять на вредоносные ссылки, и две программы для компьютеров с возможностью «лечения» компьютера 3.5.

3.5



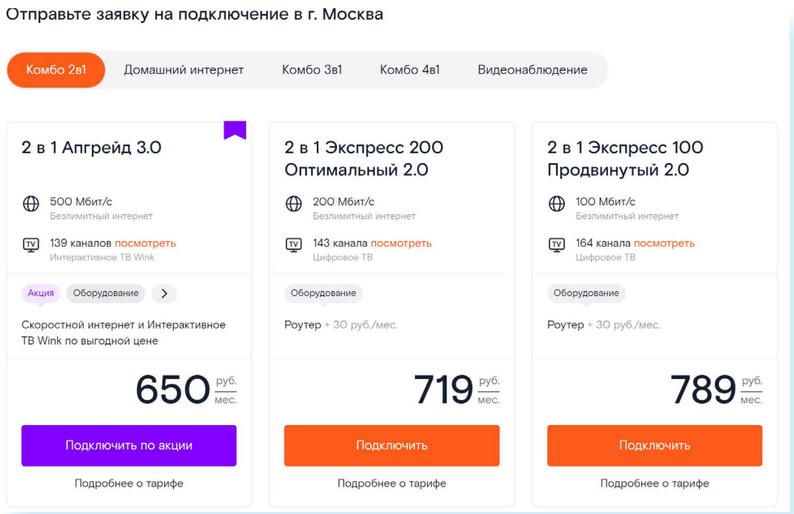

**Как установить антивирусные программы?**

- С официального сайта разработчика программы.
- Включить услугу установки антивирусной программы в тариф интернет-провайдера.

Они абсолютно бесплатны и, если вы не уверены в защите своего устройства, можно скачать такую программу и периодически ее запускать. Сама она не отслеживает вашу активность в отличие от серьезных антивирусных программ.

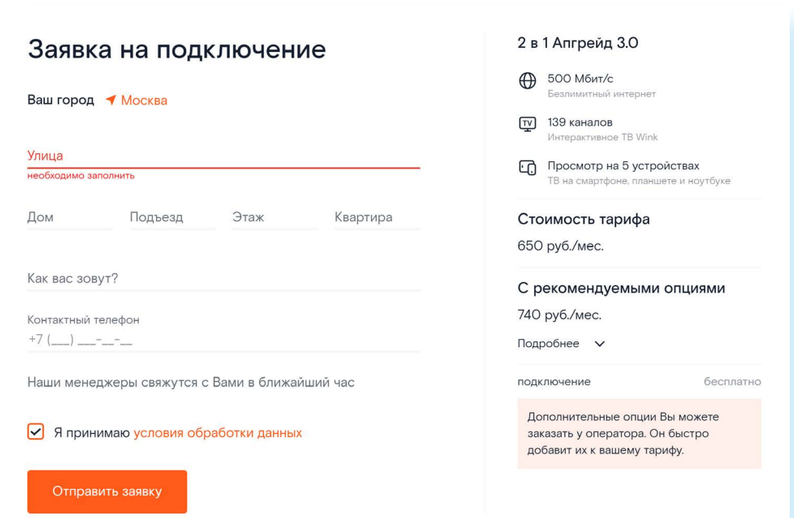
Обратите внимание, что антивирусы часто предлагают и провайдеры при подключении вас к интернету. Они могут входить в пакетное предложение. Можно сразу выбрать эту услугу, подключая интернет и выбирая тариф. Так, на сайте «Ростелекома», если мы перейдем к предлагаемым тарифам и нажмем около любого предложения строчку «Подробнее о тарифе», откроется список услуг, который входит в тариф 3.6.

3.6




Здесь есть и дополнительные услуги, которые можно добавить к тарифу, в том числе, подключение антивирусной программы. Можно выбрать приемлемую стоимость и подключить, заполнив ниже заявку 3.7.

3.7






Все крупные производители антивирусных программ обычно предлагают качественные продукты.

Сравнивайте их по стоимости и по функционалу, можно также установить антивирус сразу на несколько устройств. Как правило, программу скачивают на компьютер и затем оплачивают онлайн ее стоимость.

Скачивайте антивирусные программы с официальных сайтов производителей или включайте данную услугу в тарифах интернет-провайдеров.

## Социальная инженерия. Примеры мошеннических схем

Слабое звено любой системы защиты – это люди. Для мошенников иногда бывает проще использовать психологическое воздействие, чем какие-то сложные технологические решения.

**Фишинг** – один из самых распространенных методов обмана. Главная задача мошенника заставить пользователя перейти на поддельный сайт. Поддельный сайт выглядит также, как настоящий официальный, но вот в адресе может быть изменена всего одна буква. Например, это может быть заново созданная страница оплаты якобы какой-то крупной сети, где вы совершаете покупку.

Переход на такой сайт предполагает оплату покупки. Ввод пароля, логина и затем данных банковской карты для оплаты. Таким образом, деньги получает мошенник и в придачу ваши личные данные, которые вы используете для онлайн оплаты покупок.

В 2021 году аналитики «Доктор Веб» обнаружили множество фишинговых сайтов. В числе прочего злоумышленники подделывали веб-страницы магазинов бытовой техники. Например, мошеннические сайты были замаскированы под официальные ресурсы «М.Видео». После нажатия кнопки «Перейти на сайт» пользователи оказывались в фальшивом интернет-магазине. Здесь они, в надежде получить товар дешевле, активировали некий промокод и совершали покупку, вводя свои банковские данные. Зафиксированы случаи, когда для оплаты товара пользователь перенаправлялся на сайт поддельной платежной банковской системы. Там покупатель вводил данные банковской карты, подтверждал платеж, но товар не получал.

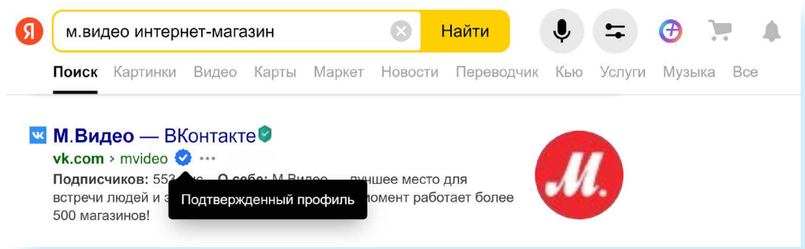
**Вишинг** – это обман по телефону. Мошенник представляется сотрудником банка, службы охраны или покупателем вашего товара и пытается узнать у вас всю информацию о платежной карте: номер, имя и фамилию владельца, код CVV и код для подтверждения транзакции.

**Помните, что для перевода средств на вашу карту не нужно сообщать все ее данные. Деньги могут быть переведены только по номеру телефона или по номеру вашей карты. Если вас просят назвать код CVV с карты или проверочный код совершенной оплаты, это 100% мошенники.**

Как пользователи попадают на фишинговые сайты?

**При поиске в интернете** конкретного товара пользователь может перейти на поддельный сайт. Всегда обращайте внимание на адрес сайта, прежде чем проводить оплату. Вас должны насторожить слишком низкие цены. На карточке настоящей компании должен быть значок (галочка на синем фоне), подтверждающий данные компании 3.8.

3.8




Это могут быть также письма, пришедшие в **электронную почту**. Среди коммерческих спам-рассылок попадаются и письма от мошенников, причем это может быть письмо якобы от известного банка с просьбой подтвердить свои данные или от известного магазина, предлагающего вам как постоянному покупателю получить большой бонус. Всегда смотрите, кто отправитель. Если это известная компания, то, прежде чем переходить по ссылке, зайдите на ее официальный сайт или свяжитесь с их службой поддержки, чтобы уточнить информацию. А подозрительное письмо удалите из своей электронной почты.

Особенно часто ссылки на фальшивые сайты мошенники присылают через **сайты объявлений или в социальных сетях и мессенджерах**. Например, на Авито покупатель может написать вам, что готов купить товар, но через другую службу доставки. Просит перейти для разговора в другой мессенджер и присылает ссылку на страницу доставки, например, Яндекс.Доставка, но это оказывается поддельная страница, на которой продавцу, чтобы получить деньги, нужно ввести все данные своей карты, в том числе срок ее действия и код CCV. В результате продавец остается без денег. Мошенники могут использовать и вишинг. Связываются с продавцом по телефону, представляются покупателем, который хочет немедленно приобрести товар. И также «выуживают» данные платежной карты.

**Никогда не переходите для общения из чата Авито в другие мессенджеры. Не переходите по присланным ссылкам. Используйте на сайтах объявлений функцию безопасной сделки.**



Схемы обмана постоянно совершенствуются. Приведем несколько примеров того, как работают мошенники.

## Безопасность на сайтах объявлений

Некоторые схемы обмана.

Продается техника по низкой цене якобы через менеджера крупного магазина. Если с ним связаться, он присылает ссылку для оплаты. Ссылка ведет на сайт, который очень похож на сайт магазина, но минимальные отличия все же есть, потому что этот сайт создали мошенники. Продавец предлагает внести залог или предоплату в 50%. В результате ни денег, ни товара.

Продавец настаивает на курьерской доставке и предлагает передать оплату курьеру. Перед приездом курьера продавец говорит, что курьеру не доверяет и просит сбросить деньги на карту. Курьер действительно приезжает. Покупатель переводит деньги, но затем оказывается, что продавец, предлагавший вам товар, не имеет никакого отношения ни к курьеру, ни к продаваемому товару. Это мошенник, который просто заказал на ваш адрес доставку нужного вам товара. В результате вы перевели деньги мошеннику, а курьер, так и не получив оплаты, товар вам не отдает.

Приходит СМС от банка, что покупатель перевел сумму за товар 2 или 3 раза. Скажем, вместо 5 тысяч переводит 20 тысяч рублей. Говорит, что это ошибка и просит вернуть деньги. Здесь большая вероятность того, что это поддельное СМС. Нужно посмотреть, с какого номера отправлено сообщение. Иногда используют, например, ненастоящий номер Сбера – девятка и две буквы «О» вместо номера 900 (девять, ноль, ноль) .

Мошенники предлагают обмен товара с доплатой, для чего нужно перейти по ссылке в сообщении. Когда продавец переходит по ней, на устройство автоматически скачивается вредоносная программа, которая может зашифровать файлы или перехватить ваши личные данные.

При сделке с техникой Apple покупатель при осмотре меняет Apple ID или ставит блокировку по отпечатку пальца/паролю и затем возвращает товар. А за разблокировку потом просит деньги с продающего товар.

В любом случае будьте внимательны на сайтах купли/продажи:

- старайтесь не переводить предоплату или залог. Если это не сайт крупной торговой сети, то в 99% случаях это мошенники;
- не переходите по ссылкам, присланным в сообщениях от незнакомцев;
- сами выбирайте службу доставки или используйте сервисы безопасной оплаты;
- если вы выступаете продавцом, внимательно проверяйте сообщения об оплате, которые пришли вам от покупателя. Перепроверьте в интернет-банкинге, точно ли ваш счет пополнился на нужную сумму;

**Как распознать поддельный сайт?**

1. Проверить адрес, сравнить его с официальным адресом магазина.
2. Сравнить цены с другими сайтами, продающими аналогичные товары; если цены значительно ниже, это может быть признаком мошеннической схемы.
3. Связаться с представителями магазина по телефону или через официальные соцсети и проверить информацию, представленную на сайте.

- никому не сообщайте все данные вашей платежной карты. Для перевода денег вам достаточно номера вашего телефона или номера карты;
- скрывайте свой номер телефона в объявлениях.

## Безопасность в социальных сетях и электронной почте

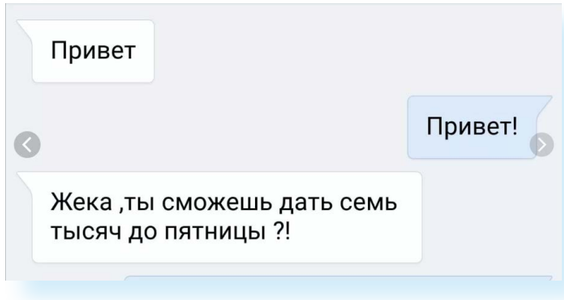
Одна из самых активных площадок для мошеннических схем – социальные сети. Многие аферы мошенников могут быть похожи, но подаются по-разному.

Например, приходит личное сообщение о раздаче бесплатных подарочных карт или о выигрыше как тысячного участника одной из групп. Мошенники предлагают перейти по ссылке. На самом деле она ведет на подставной сайт, где вас попросят ввести личные данные и данные банковской карты для перечисления выигрыша.

Мошенничество через знакомство в интернете: незнакомец входит в доверие, ведет с вами долгую переписку и затем пытается выманить деньги. Это может быть просьба оплатить какой-то подарок или его пересылку, премиум-показ фильма и т.д. В любом случае просьба невидимого собеседника о платежах должна вас насторожить. Никаких платежей делать не нужно. Должно насторожить, что новый знакомый не спешит встречаться, слишком хорошо выглядит на фотографии и тому подобные любые несоответствия в аккаунте. При знакомстве по интернету на той стороне может быть совсем другой человек, не такой, каким он вам стремится представиться.

Внезапно от знакомого вам человека приходит сообщение с просьбой выручить деньгами. Не нужно тут же переводить средства, можно предположить, что, скорее всего, его аккаунт был взломан. Нужно созвониться с ним и выяснить, действительно ли это он писал и просил о помощи. Точно такое же письмо может прийти и на электронную почту. Проще всего защититься от такого способа мошенничества, сделав телефонный звонок 3.9.

3.9




В электронную почту или соцсети могут приходить сообщения, призывающие вас перейти по некой ссылке: «Ты видела эту свою фотку?», «Тут такое про тебя написано». Ссылка ведет на поддельные сайты социальных сетей, где предложат ввести свои логин и пароль от аккаунта. Так мошенники смогут завладеть вашей страничкой.



Точно также работают и другие сообщения с предложением перейти по ссылке и «Узнать свой IQ» или «Увидеть, кто зашел на твою страничку». Это сбор данных, которые можно будет перепродать или использовать против пользователя.

На электронную почту или в смс пришла информация о том, что ваш аккаунт на Фейсбуке или платежная карта заблокирована. И нужно перейти по ссылке, чтобы подтвердить данные. Конечно, ссылка ведет на подставной сайт, а ваши личные данные получают мошенники.

Предлагают редкий товар со 100% предоплатой. Однако по указанному адресу, где можно забрать товар, живут люди, которые вообще не имеют отношения к данному предложению.

На электронную почту или сообщением в социальных сетях приходит информация о выигрыше или наследстве из-за границы. Чтобы получить солидную сумму, нужно сделать перевод или предоставить банковские данные, перейдя по ссылке. Игнорируйте такие сообщения. Это обман.

**Какие правила безопасности нужно соблюдать:**

- не переходить по подозрительным ссылкам, пришедшим от незнакомых адресатов. Даже если кажется, что информация пришла от известной компании. Если сомневаетесь, сделайте звонок, уточните информацию;
- не доверяйте и не рассказывайте все о себе в переписке с собеседниками, с которыми познакомились в интернете. Вы не можете быть уверены, что это не мошенники;
- не переводите деньги в ответ на просьбы, которые пришли в разного рода сообщениях. Сначала уточняйте ситуацию;
- периодически меняйте пароль в аккаунтах в социальных сетях;
- откорректируйте настройки безопасности. В ВКонтакте перейдите в «Настройки», в раздел «Приватность». Поставьте разрешение на отправку сообщений только своим друзьям. Вы также можете сделать вашу страничку закрытой. Аналогичная функция есть и в других социальных сетях;
- включите двухфакторную аутентификацию для входа на электронную почту. *(Подробнее в главе 5 модуля 10 «Кибербезопасность» расширенного курса «Азбука интернета»).*

## Безопасность в финансовых вопросах

Наиболее привлекательными сайтами для мошенников являются банковские и финансовые сервисы. Как правило, банки формируют надежную защиту хранящихся данных. Авантюристам проще ввести в заблуждение клиентов банка, чем взламывать существующие банковские системы защиты.

Мошенник звонит клиенту банка, представившись службой безопасности, и сообщает, что на телефоне, где установлено интернет-приложение

банка, выявлен вирус, и поэтому счет клиента под угрозой. Он предлагает немедленно установить на телефон приложение. Объясняет, как это сделать. Обманщик через установленное приложение получает удаленный доступ к устройству и снимает все деньги со счета клиента банка.

Другой вариант. Злоумышленник представляется клиенту службой безопасности банка и сообщает, что кто-то пытается снять деньги с его банковского счета. На телефон с поддельного номера действительно приходят сообщения с кодами подтверждения для проведения транзакции. Мошенник предлагает перейти к банкомату и срочно снять все деньги. Когда деньги сняты, лжесотрудник банка предлагает положить их на страховочный счет с хорошим бонусом и процентами. Это счет злоумышленника.

Еще вариант: на ваш счет приходит большая сумма денег. Звонит сотрудник банка и сообщает, что на ваше имя взят кредит. Конечно, держатель карты сообщает, что он не брал кредит. Тогда сотрудник банка предлагает срочно вернуть деньги. Для этого нужно ввести комбинацию цифр на номер 900. Деньги уходят на другой счет другого банка, то есть мошеннику. Впоследствии оказывается, что кредит на ваше имя действительно был взят. Если вы попали в такую ситуацию, не выполняйте никаких операций по переводу средств. Звоните или идите в банк и решайте вопрос с сотрудниками организации.

Мошенник звонит держателю банковской карты и, представляясь сотрудником банка, сообщает, что в ваш личный кабинет интернет-банка пытались войти из другого города. Для обеспечения безопасности необходимо подтвердить все данные платежной карты. Человек сообщает все данные, в том числе секретный код подтверждения транзакции. И деньги у мошенника.

**Какие правила безопасности нужно соблюдать:**

- никому и никогда не сообщайте все платежные данные вашей банковской карты;
- не проводите никаких платежей по просьбе якобы сотрудников банка;
- не общайтесь с мошенниками, кладите трубку и перезванивайте в банк.

## Безопасность при интернет-покупках и интернет-заработке

При выборе вариантов заработка или покупки товара в интернете нужно быть очень внимательным.

Часто в интернете предлагают заработать деньги на опросах. Как правило, это небольшие суммы. Если вы встретите подобное предложение с высокой оплатой, стоит обойти его стороной.



Чаще всего в таких случаях после прохождения опроса и сбора ваших личных данных злоумышленники просят заплатить комиссию, прежде чем заплатить вам деньги. Она небольшая по сравнению с суммой вознаграждения, поэтому человек соглашается ее заплатить. Но после оплаты обещанная за прохождение опроса сумма так и не поступит на счет пользователя, а у мошенников будут данные банковской карты, которые были введены при оплате комиссии.

Мошенники создают сайты, где предлагают медицинские услуги, информацию о лекарствах, мерах социального обеспечения. В том числе, на таких ресурсах вам могут предложить заменить полис медицинского страхования за плату или оформление услуги по получению социальных выплат. На самом деле эти услуги вы можете оформить бесплатно или дешевле. А тут просто вымогают деньги.

Нередко обманывают покупателей и интернет-магазины. Они завлекают низкими ценами. При заказе вас могут попросить внести предоплату на какой-либо электронный кошелек или банковскую карту. Затем магазин будет придумывать отговорки, почему товар не доставлен либо пришлет некачественный товар.

**На какие меры безопасности необходимо обратить внимание:**

- уточните адрес, на который вы сможете направить претензию в случае, если останетесь недовольны покупкой;
- читайте отзывы о сайтах, где вы намерены сделать покупки;
- оплачивайте товары только на проверенных сайтах известных компаний;
- если вы оформляете какие-либо документы, делайте это только на официальных сайтах ведомств или на портале «Госуслуг»;
- не вводите свои данные на сайтах, где вам предлагают получить какие-то компенсации или дополнительные социальные выплаты. Решением этих вопросов занимаются только официальные сайты государственных ведомств;
- осторожно относитесь к предложениям заработать большие суммы в интернете. За ними, скорее всего, кроются мошеннические схемы.

## Куда сообщить о мошенниках?

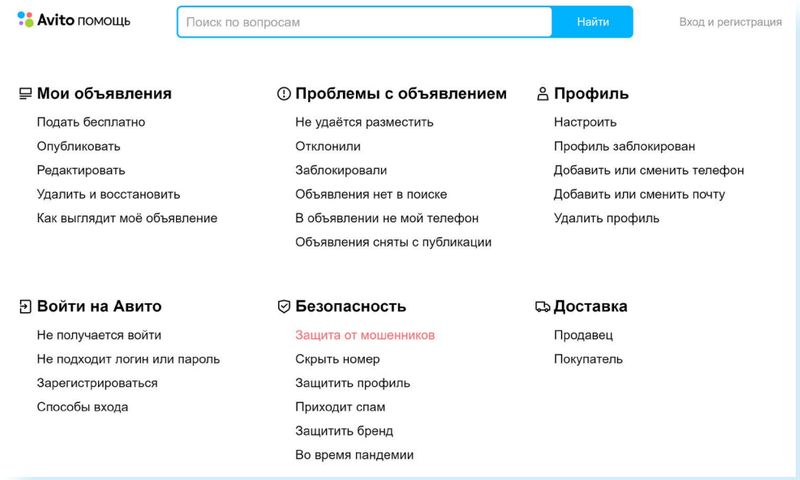
Сообщать о фактах мошенничества нужно обязательно. Можно обратиться в отделение полиции по месту жительства или отправить на сайте МВД электронное обращение.

На Авито можно сообщить о мошенниках-продавцах и покупателях. Для этого нужно перейти в раздел «Помощь». Он находится в верхнем меню сайта. Здесь есть раздел «Безопасность» и пункт «Защита от мошенников». Там можно оставить свое сообщение, если вас обманули. Также внизу есть возможность написать в службу поддержки 3.10.

**Как обезопасить себя от мошенников?**

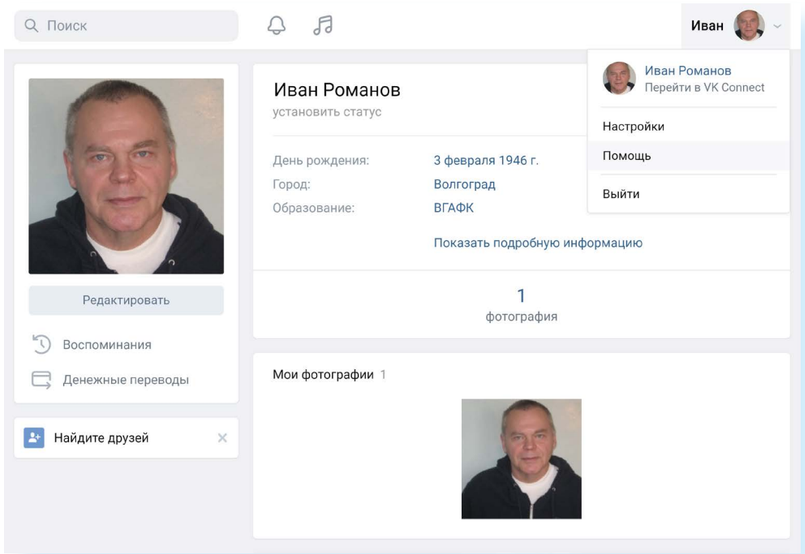
- Перепроверяйте информацию, прежде чем совершить платеж.
- Не вводите свои данные на подозрительных и незнакомых сайтах.
- Используйте безопасные сервисы оплаты.
- Не переходите по ссылкам, полученным от незнакомцев.
- Устанавливайте настройки безопасности и приватности в социальных сетях.

3.10




В социальных сетях также всегда можно пожаловаться в техподдержку на действия пользователей. Так, в ВКонтакте нажмите на значок профиля и выберите раздел «Помощь» 3.11.

3.11




Затем перейдите в раздел «Безопасность и доступ к аккаунту» либо выберите пункт «Задать вопрос» и опишите вашу ситуацию.

Если у мошенников есть сайт, то можно сообщить о нем Яндексу и Гуглу. В Яндексе для этого нужно перейти в раздел «Службы поддержки» и по данной ссылке разместить информацию о сайте злоумышленников: **https://yandex.ru/support/search/troubleshooting/delspam.html**

Можно ли вернуть украденные деньги? По закону «О национальной платежной системе» банк должен вернуть деньги, если клиент сообщил



об интернет-мошенниках в течение суток. После обращения банк заблокирует счет и начнет проводить проверку. По закону на расследование у него есть 30 дней.

Однако нужно принять во внимание, что если проблема на стороне банка, то есть был взлом системы, то деньги вернут. А вот если вы сами сообщили мошенникам данные или сами перевели им деньги, будет гораздо сложнее их вернуть.

## Риски публичных Wi-Fi сетей

К работе в публичных Wi-Fi сетях также стоит относиться осторожно. Дело в том, что именно в таких сетях злоумышленники могут увидеть ваши пароли, данные вашей платежной карты и т.п. И тем более не стоит пользоваться незапароленными сетями. Хакеры в этом случае часто создают поддельную точку доступа. И, соответственно, могут видеть все данные тех, кто к ней подключился. Но и закрытые сети могут быть поддельными, ведь мошенникам несложно узнать пароль от Wi-Fi в кафе или отеле и также создать фальшивую одноименную сеть с таким же паролем 3.12.

3.12


Не проводите платежи, не заходите на личные страницы в социальных сетях в зоне Wi-Fi с публичным доступом.. Старайтесь выключать Wi-Fi, если не пользуетесь им. Отключите функцию автоматического подключения к Wi-Fi в вашем телефоне или планшете.

Дело в том, что у сетей Wi-Fi есть возможность следить за вами. Когда вы заходите в торговый центр, телефон автоматически начинает искать точку Wi-Fi. При этом он транслирует свой собственный уникальный адрес. Эти данные заносятся в журнал приемника, и по ним маркетолог может следить, как клиент перемещается по отделам, и показывать вам соответствующую вашим интересам рекламу.

Альтернативой может стать подключение по виртуальной сети VPN. Можно поискать подобные приложения и даже найти бесплатные варианты у ProXPN,  Cyber Ghost, Your Freedom или HotSpot Shield. Они, возможно, будут работать чуть медленнее, зато безопаснее.

## Внешние носители

30% вредоносных программ распространяется через съемные накопители: карты памяти и USB-флешки. В 2012 году были обнаружены компьютерные вирусы на двух американских электростанциях, которые были отключены от сети интернет. Причиной стали флешки, которые принес из дома один из рабочих и подключил к рабочим компьютерам.

Съемные накопители отлично переносят из компьютера в компьютер нежелательные программы. Когда флешка вставляется в зараженный компьютер, активный вирус может просто самозаписаться на нее 3.13.

3.13

Более того, известны случаи, когда инфицированные флешки намеренно оставляли в тех или иных организациях в людных местах с какой-нибудь привлекающей внимание подписью: «Зарплата сотрудников», «Планы по ротации персонала» и т.д. И всегда находились те, кто не мог сдержать любопытство и подключал флешку к рабочему компьютеру, провоцируя таким образом хакерскую атаку на всю корпоративную систему.

Поэтому старайтесь перед тем, как начать работать, проверять USB-накопители антивирусной программой. Разделяйте флешки на те, что хранят ваши архивы, и те, которые можно использовать для переноса информации из других источников.

**Также имейте в виду, что зарядка телефонов через USB в общественных местах может быть чревата последствиями. USB-разъем также может передавать информацию о вашем телефоне и приложениях на нем. Поэтому, если есть необходимость зарядить мобильное устройство в общественном месте через USB-разъем, не работайте на нем, пока идет зарядка.**



## Какую информацию нельзя доверять интернету

Поскольку из сети невозможно полностью удалить все следы своего присутствия, нужно внимательно относиться к тому, что вы делаете в интернете.

Не стоит размещать в публичном доступе свои личные данные, в том числе сканы паспортов или других документов.

Сообщая данные своего паспорта, обращайте внимание, что за ресурс их запрашивает. Если это действительно необходимо, то не присылайте скан паспорта, а просто перепишите данные в текстовом виде.

Если все же нужно выслать скан паспорта, прикройте при сканировании вашу подпись. Так будет сложнее воспользоваться вашими паспортными данными.

Не делитесь публично своими финансовыми планами, информацией о ваших платежных картах. Никому не высылайте фотографии банковской карты. Они не нужны для проведения финансовых операций. Достаточно сообщить номер карты или номер телефона, к которому карта привязана.

Не размещайте на страничках в социальных сетях номер своего мобильного телефона и адрес электронной почты.

Проверяйте сайты, на которых вы проводите оплату. Если что-то вас насторожило, лучше откажитесь от оплаты и найдите другой способ покупки товара или услуги.

### Контрольные вопросы

1. Как работают вредоносные программы?
2. Откуда может появиться вредоносная программа на устройстве?
3. Что такое социальная инженерия?
4. Какие варианты и схемы мошенничества вам известны?
5. Какие действия нужно предпринять, если вам звонит сотрудник банка и просит сообщить данные банковской карты?
6. Каким сообщениям не стоит доверять в социальных сетях?
7. Почему стоит осторожно относиться к съемным USB-носителям?