

## Как сохранить денежные средства при осуществлении платежей банковских операций с помощью сети Интернет

не переходить по ссылкам, указанным в поступивших сообщениях, а вводить ссылку вручную на проверенном сайте в строке поиска.

Вводить адресную строку, если получен запрос на повторную авторизацию, чтобы убедиться, на том же сайте вы находитесь.

Вводить логин и пароль, убедиться, защищено ли соединение (наличие перед адресом сайта букв https говорит о защищенном соединении).

Убедиться в источнике входящих писем и адресов, он может быть неясным даже если письмо, от которого так как его могли также перехватить или взломать телефон, почту, интернет.

Не переходить в интернет-банк с чужих компьютеров или телефонов (если есть возможность это сделать, то по окончании сессии необходимо нажать Ctrl+Alt+Del и очистить кэш-память).

Не передавать без необходимости свои персональные данные, помимо логина и пароля.

Использовать сложный пароль (буквы, цифры, знаки) только в личном кабинете, а также использовать разные пароли, запрашиваемые

банками для подтверждения действий в личном кабинете.

**Оперативно** уведомлять банк при получении подозрительных сообщений на телефон, не звонить по указанным в них номерам. В случае смены номера или утраты SIM-карт информировать банк.

**Установить** пароль на телефон и не снимать блокировку с экрана при появлении посторонних лиц.

**Запретить** оператору связи замену SIM-карты по доверенности.

**До** совершения покупки в интернет-магазине необходимо собрать информацию о продавце: адрес продавца (не абонентский ящик), его телефон, отзывы в Интернете.

**Использовать** для покупок в Интернете банковскую карту с высокой степенью защиты.

**Игнорировать** сообщения о предоставлении личной или финансовой информации.

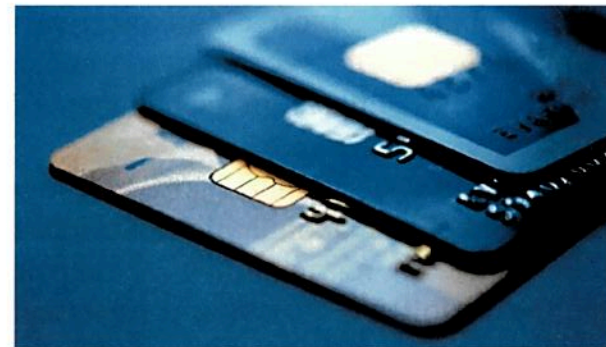
**Фальшивые** письма и сайты могут во всем повторять дизайн настоящих, но гиперссылки, скорее всего, будут неправильные, с ошибками или будут отсылать не туда. По этим признакам можно отличить фишинговое письмо от настоящего.

**В случае, если Вы все же стали жертвой мошенников, Вам необходимо обратиться с заявлением в дежурную часть ближайшего к вам отделения полиции.**



## ПРОКУРАТУРА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

**Как обезопасить себя от действий мошенников по хищению денег с банковских карт?**



г. Челябинск  
2020 г.

астоящее время довольно распространенным преступлением является мошенничество с использованием электронных средств.

Ответственность за использование средств доверия с целью завладения средствами, привязанными к банковской карте, предусматривается в ст. 159.3 Уголовного кодекса РФ.

### **Как распорядиться средствами чужой банковской карты:**

Мошенник может завладеть чужой банковской картой и ПИН-кодом к ней одним из следующих путей.

Карта может быть похищена тайно или открыто, а ПИН-код может быть украден; снят на микрокамеру, установленную рядом с банкоматом и привязанную к устройству ввода; украдена при помощи специальной клавиатуры.

Мошенник может получить информацию об имени владельца, срок окончания действия и номер платежной карты, используемой для покупок и платежей в интернете, мошенник может напечатать карты, не снабженные специальной защитой (3D-secure) в обход подтверждения транзакции с помощью СМС-сообщения.

Мошенники представляются сотрудниками банков и других финансовых компаний, по телефону

обещают своей жертве кредиты под низкий процент, сообщают якобы о выигрыше в конкурсе или о поступлении платежа, который можно получить, произведя определенные действия через банкомат.

**Н**икогда и никому, ни при каких обстоятельствах нельзя передавать логин, пароль или реквизиты вашей банковской карты (секретный код безопасности CVV2, подтверждающий подлинность карты, имя ее владельца, срок действия) и, разумеется, ПИН-код. Если банковская карта привязана к номеру сотового телефона с функцией отправки СМС-сообщений с кодом подтверждения операции с картой, нельзя сообщать данный код другим лицам.

**Н**еобходимо выбирать банкоматы, расположенные внутри офисов банков или в охраняемых точках, оборудованных системами видеонаблюдения.

**Н**еобходимо при вводе ПИН-кода закрывать клавиатуру банкомата рукой;

**П**ри возникновении проблем нельзя пользоваться советами «случайных помощников», лучше сразу позвонить в банк и заблокировать карту. Если карта осталась в банкомате необходимо позвонить в компанию, осуществляющую техническое обслуживание банкомата (номер должен быть указан на терминале).

**В** случае потери карты или при наличии

оснований полагать, что третьи лица узнали ее реквизиты, необходимо срочно обратиться в банк и заблокировать ее.

**Б**анки не рассылают сообщений о блокировке карт, а в телефонном разговоре не выспрашивают конфиденциальные сведения и коды, связанные с картами клиентов.

**Н**еобходимо незамедлительно информировать банк, эмитента карты или кредитора, если в банковских отчетах и отчетах по кредитным картам имеются транзакции, которых Вы не совершали. **Н**еобходимо отслеживать списания с карты, обращать внимание на те, которые Вы не узнаете или которые подозрительно выглядят.

**Н**е стоит принимать всерьез звонки с предложением малорискованных и высокоприбыльных инвестиций, особенно если оппонент настаивает на немедленном вложении денег, гарантирует высокие прибыли, обещает низкий или вообще отсутствующий финансовый риск.

**Н**ельзя принимать всерьез сообщения о выигрыше или о Ваших высоких шансах выиграть в лотереях или конкурсах, в которых не принимали участие, особенно, если предлагают отправить деньги на оплату «налогов», «сборов» или «таможенных платежей», прежде чем выслать Ваш выигрыш..

## ▲ Что делать, если вас обманули? ▲

Если преступник узнал информацию о вашей банковской карте, правоохранители рекомендуют обратиться в день хищения в банк с требованием вернуть деньги на карту, заблокировать счет, запретить перевод средств с него на другие счета, приостановить обслуживание счетов, на которые были перечислены ваши деньги. После получения ответа от банка с выпиской по счету написать заявление в полицию.

Фактически средства можно вернуть до зачисления перевода на счет получателя. После этого возврат возможен лишь по решению суда.



**ПРОКУРАТУРА  
ЧЕЛЯБИНСКОЙ ОБЛАСТИ**

**Как не стать жертвой  
«телефонного» мошенничества**



**г. Челябинск  
2020 г.**

«интернет-банк», «онлайн - банк», ходимо срочно связаться с банком, активировать карту и приостановить обслуживание по счетам.

Следует отметить, что владельцы интернет-сайтов обязаны проверять достоверность размещенной информации не обязаны. Какой-либо ответственности владельцы интернет-ресурсов за достоверность информации не несут. Лица, размещающие объявления в интернете при покупке или продаже товара обязаны идентифицироваться, при этом владелец интернет-сайта не обязан и просто не имеет возможности проверить достоверность личных данных и номера телефона. Зачастую кража осуществляется под именем и по сим-карте, выданной на чужое имя.

Необходимо внимательно проверять информацию в объявлении, тщательно оценивать товар и его стоимость. Не соглашайтесь на предоплату. Не сообщайте данные паспорта, банковской карты, телефон и любую персональную информацию. Не переходите по подозрительным ссылкам в сообщениях. Наилучший вариант - личная встреча и покупка товара после его осмотра.

практически каждый день в  
ах о происшествиях и  
уплениях размещается  
омация о зарегистрированных на  
тории области фактах  
нических действий.

аиболее распространенными  
бами мошенничества являются  
ющие случаи:

реступник связывается с  
певшим по телефону и  
тавляется родственником,  
ый попал в беду (сбил человека,  
дится в полиции и т.д.) и ему  
о нужно либо перечислить деньги  
передать доверенному лицу.

акже преступник может  
тавляться сотрудником банка,  
див, что банковская карта  
кирована и для ее восстановления  
одимо провести ряд операций с  
ной картой, после чего  
певший, следуя указаниям  
ышленника, предоставляет  
п к своим данным, с помощью  
ых совершается хищение, либо  
переводит денежные средства  
естному лицу.

### ▲ Как действовать? ▲

В первую очередь, положите  
у и свяжитесь с тем человеком, от  
имени звонили. Ни в коем случае  
сообщайте по телефону

неизвестным лицам свои данные, а также  
данные Ваших банковских карт.  
Незамедлительно обращайтесь в  
правоохранительные органы.

2. В настоящее время значительное  
количество преступлений совершается  
при продаже или покупке товаров с  
помощью интернет-сайтов.

Злоумышленниками в отношении граждан  
осуществляются следующие действия.

а) Наиболее распространенная  
схема, когда мошенник размещает  
объявление о продаже товара по  
привлекательной цене, потерпевший  
перечисляет денежные средства по  
предоплате, товар не доставляется. В  
большинстве случаев преступления  
совершаются лицами, которые  
представляются не своими данными,  
используют чужие сим-карты, а для  
расчета – QIWI кошелек. При этом  
продавец живет в другом городе,  
некоторые из них находятся в местах  
лишения свободы. Все это вызывает  
определенные трудности при раскрытии  
преступления.

б) Мошенник «покупает» товар у  
продавца. Автору объявления о продаже  
звонит потенциальный покупатель,  
который готов приобрести товар и даже  
согласен внести предоплату на  
банковскую карту. Существует много  
вариантов обмана. Например, покупатель  
якобы живет в другом городе или по иной  
причине не может сам забрать товар,

поэтому пришлет за ним курьера или  
знакомых. В ходе разговора мошенник  
пытается получить данные карты и ее  
привязки к мобильному телефону, может  
просить назвать коды, поступающие по  
СМС. Также он может попросить  
потерпевшего пройти к банкомату и  
произвести ряд операций, в результате  
которых денежные средства похищаются.

в) Мошенник прислал СМС об  
обмене. После публикации в Интернете  
объявления о продаже товара с указанием  
контактных данных потерпевшему  
приходит СМС. Отправитель предлагает  
обмен и прилагает гиперссылку на товар.  
Владельцы смартфонов, перейдя по  
ссылке, незаметно для себя скачивают на  
устройство вирус, который при  
подключенной услуге «Мобильный банк»  
с помощью скрытых сообщений  
направляют от имени потерпевшего  
указания банку о переводе средств на  
другой счет.

### ▲ Как себя обезопасить? ▲

При получении подобных СМС  
рекомендуется не переходить по ссылкам  
и удалить сообщение. Если телефон  
заражен, необходимо его выключить,  
сим-карту перевыпустить у оператора.  
Если к номеру телефона, на который  
пришло СМС, привязана банковская  
карта, услуги «мобильный банк», →