

В соответствии с рекомендациями ГУ ЦБ по Челябинской области от 05.11.2020 № Т575-18-5-7/7369 «О мерах по предупреждению мошенничества» предоставляем для внимания следующие рекомендации Прокуратуры Челябинской области

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

Не переходить по ссылкам, указанным в поступивших сообщениях, безопаснее вводить ссылку вручную на уже проверенном сайте в строке браузера.

Проверять адресную строку, если поступил запрос на повторную авторизацию, чтобы убедиться, на том ли сайте находитесь.

Перед вводом логина и пароля, проверять, защищено ли соединение (наличие перед адресом сайта букв "https" говорит о защищенном соединении).

Проверять источник входящих писем и сообщений, он может быть небезопасным даже если письмо, от друга, так как его могли также обмануть или взломать телефон, почту, аккаунт.

Не заходить в интернет-банк с чужих компьютеров или телефонов (если пришлось это сделать, то по завершению сессии необходимо нажать "Выход" и очистить кэш-память).

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

Лучше использовать сложный пароль для входа в личный кабинет, а также одноразовые 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 посторонних лицах.

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.

В настоящее время довольно распространенным преступлением является мошенничество с использованием электронных средств платежа.

Ответственность за использование чужого доверия с целью завладения средствами, привязанными к платежной карте, предусматривается статьей 159.3 Уголовного кодекса РФ.

▲Способы распоряжения средствами с чужой банковской карты:

Мошенник может завладеть чужой банковской картой и ПИН-кодом к ней обманным путем.

Карта может быть похищена тайно или открыто, а ПИН-код может быть подсмотрен; снят на микрокамеру, установленную рядом с банкоматом и направленную на устройство ввода; считан при помощи специальной накладной клавиатуры.

Узнать информацию об имени держателя, срок окончания действия и CVC-код платежной карты, используемой для покупок и платежей в Интернете, мошенник может на порталах, не снабженных дополнительной защитой (3D-secure) в виде подтверждения транзакции посредством СМС-сообщения.

Зачастую мошенники представляют сотрудников банков и других известных 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.

Никогда 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.

Необходимо выбирать банкоматы, расположенные внутри офисов банков или в охраняемых точках, оборудованных системами видеонаблюдения.

Необходимо при вводе ПИН-кода закрывать клавиатуру банкомата рукой;

При 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.

Банки не рассылают сообщений о блокировке карт, а в телефонном разговоре не запрашивают конфиденциальные сведения и коды, связанные с картами клиентов.

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

Не 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.

Нельзя 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.

Практически каждый день в сводках о происшествиях и преступлениях размещается информация о зарегистрированных на территории области фактах мошеннических действий.

Наиболее распространенными способами мошенничества являются следующие случаи:

Преступник связывается с потерпевшим по телефону и представляется родственником, который попал в беду (сбил человека, находится в полиции и т.д.) и ему срочно нужно либо перечислить деньги либо передать доверенному лицу.

Также преступник может представляться сотрудником банка, сообщив, что банковская карта заблокирована и для ее восстановления необходимо провести ряд операций с указанной картой, после чего потерпевший, следуя указаниям злоумышленника, предоставляет доступ к своим данным, с помощью которых совершается хищение, либо сам переводит денежные средства неизвестному лицу.

▲ Как действовать? ▼

1. В первую очередь, положите трубку и свяжитесь с тем человеком, от чьего имени звонили. Ни в коем случае не 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 придет 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», ➡

➡ «интернет-банк», «онлайн - банк», необходимо срочно связаться с банком, заблокировать карту и приостановить обслуживание по счетам.

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

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

▲ Что делать, если вас обманули? ▼

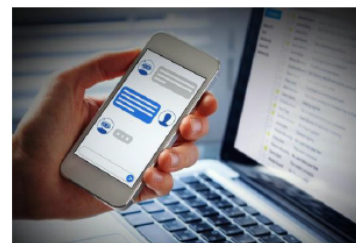
Если преступник узнал информацию о вашей банковской карте, правоохранители рекомендуют обратиться в день хищения в банк с требованием вернуть деньги на карту, заблокировать счет, запретить перевод средств с него на другие счета, приостановить обслуживание счетов, на которые были перечислены ваши деньги. 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.**