

## Банковские пластиковые карты – способ совершения преступления

Последние годы злоумышленники чаще всего звонят гражданам, представляясь сотрудниками банков, называя по имени – отчеству, и просят сообщить данные карт. При этом могут быть использованы программы подмены телефонных номеров, входящий звонок может определяться у клиента как номер банка.

Для совершения мошенничества с кредитными картами могут использоваться фальшивые банкоматы либо переделанные старые банкоматы. Размещаются они в наиболее оживленных местах. После введения карты и PIN-кода на дисплее такого банкомата появляется надпись, что денег в банкомате нет или что банкомат неисправен.

Также преступники могут использовать особые устройства, считывающие информацию с магнитных полос карты (скимминг). Как правило, это специально изготовленные клавиатуры, которыми накрывают существующие.

Самое трудное для мошенников – узнать PIN-код. Для этого могут использоваться различные способы.

Нередко мошенники для кражи денег пользуются психологическими приемами для управления действиями человека. Они изображают покупателей автомобилей, земельных участков, животных, мебели, одежды и др. на сайтах бесплатных объявлений или в социальных сетях. При этом они все находятся где-то далеко, но для того чтобы вожделенный товар не приобрел кто-то другой, они готовы перевести часть стоимости или даже полную стоимость немедленно на банковскую карту продавца.



## Основные правила безопасности для владельцев пластиковых карт

**. Никогда и никому не сообщаете PIN-код карты, не пишете его на карте или другом носителе, не храните его рядом с картой. Выучите PIN-код.**

**Для оперативного получения информации об операциях по расчетному счету подключите на телефоне услугу «СМС-оповещение».**

**Обратившись в обслуживающий Вас банк, установите лимит (дневной) снятия наличных денежных средств с карты**

**Не стесняйтесь закрывать от посторонних клавиатуру банкомата во время ввода PIN-кода.**

**Снимайте денежные средства и производите операции по карте в банкоматах, которые расположены в офисах банка, рядом с ними, или находящимися в государственных учреждениях, крупных торговых центрах и т.д.**

**Не пользуйтесь советами третьих лиц**

**Не передавать карту другим лицам**

**. Пользуясь картой в сети «Интернет», внимательно относитесь к своевременному обновлению антивирусной программы.**

**Если карта утрачена или есть подозрения, что данные карты стали известны третьему лицу, незамедлительно позвоните в банк и заблокируйте карту.**

**Не сообщайте данные карты, персональные данные, коды, сведения, содержащиеся в SMS-уведомлениях, посторонним лицам.**

**Регулярно меняйте PIN-код Вашей карты.**



**Только Ваша бдительность и внимательность поможет Вам не стать жертвой преступления!**

Прокуратура Ставропольского края  
355035, г. Ставрополь,  
пр. Октябрьской революции, 9/1  
телефон: +7 (8652) 26-14-00



ГБУ ДПО «Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования»



- ❖ ОСНОВНЫЕ СХЕМЫ,
- ❖ ТАКТИКА МОШЕННИКОВ,
- ❖ КАК РЕАГИРОВАТЬ?

г. Ставрополь 2022 г.

## Способы телефонного мошенничества

### Первый способ

На сотовый телефон абонента поступает SMS-сообщение с просьбой пополнить телефонный счет отправителя.

При этом в сообщении указывается, что отправитель находится на дороге, где произошло ДТП, либо сломался его автомобиль и ему срочно нужно позвонить, а деньги на телефоне закончились.

Абонента просят положить на счет отправителя небольшую фиксированную сумму денег (как правило, от 100 до 500 рублей) либо «сколько не жалко». Подобные сообщения могут носить анонимный характер, однако во многих случаях они подписаны распространенными именами, например, Саша или Иван.

### Второй способ

На телефон абонента поступает звонок, при этом звонящий говорит взволнованным голосом и представляется родственником абонента, как правило, сыном или внуком.

Звонящий может называть женщину мамой или бабушкой, а мужчину – папой, и сообщает о том, что сбил человека, разбил чужую машину или совершил какое-либо другое преступление.

После этого звонящий говорит о том, что в отношении него могут возбудить уголовное дело и, чтобы этого не произошло, необходимы денежные средства, и передает трубку якобы представителю правоохранительных структур.

Второй человек представляется сотрудником правоохранительных органов и уже спокойным голосом сообщает информацию, аналогичную той, которую сообщил первый собеседник. Во избежание уголовного преследования родственнику абонента предлагается собрать сумму денег и либо передать ее некоему человеку при встрече, либо отправить через банк «Блиц»-переводом. В указанных случаях мошенники называют денежные суммы от нескольких десятков до нескольких сотен тысяч рублей.

### Третий способ

Преступники обзванивают абонентов с предложением о какой-либо услуге (в том числе представляясь сотрудниками операторов сотовой связи) или запугивают, предлагая перевести средства.

### Четвертый способ

На Ваш телефон приходит короткое SMS-сообщение с просьбой внесения, зачисления денежных средств на указанный телефонный номер.

### Пятый способ

Вас текстовым сообщением уведомляют о выигрыше подарка или уникального приза, а чтобы получить дополнительную информацию, предлагают отправить смс-сообщение или позвонить по определенному номеру. После Вам могут предложить перевести денежные средства для получения приза.

### Шестой способ

Вам на счет вдруг неожиданно начисляется некая сумма денег, о чем иногда может прийти уведомление. После Вам звонят и вежливо извиняются, сообщая о том, что ошиблись. Иногда мошенники не звонят, а присылают сообщение о том, что произведет ошибочный платеж.

### Седьмой способ

Вам приходят сообщения и поступают звонки от «оператора сотовой связи». Такие сообщения от псевдооператоров могут приходиться в различных вариантах. Например: «Условия Вашего тарифного плана были изменены. Подробности доступны при отправке SMS на номер \*\*\*». Номер для отправки, как обещают в сообщении – бесплатный.

Помимо рассылки SMS, бывают и звонки из «технической поддержки оператора». По словам звонящих, у вас проблема с номером телефона.

### Восьмой способ

При покупке в интернет – магазине товаров по суперпривлекательной цене Вам предлагают перечислить предоплату.

### Девятый способ

Вы получили SMS-сообщение со ссылкой на скачивание открытки, музыки, картинки и программы.

## Как поступить правильно, чтобы не стать жертвой телефонных мошенников?

- Ни в коем случае **не пополняйте** счета абонентов, чьи номера телефонов Вам не знакомы. Если все-таки это необходимо, то удостоверьтесь, что номер принадлежит Вашему родственнику или знакомому.
- **Свяжитесь** со своим родственником, о котором шла речь в ходе телефонного разговора, и выясните у него, имели ли место события, о которых Вам сообщалось по телефону. Если не представляется возможным быстро связаться с родственником, необходимо обратиться в органы внутренних дел.
- **Проверяйте** состояние своего лицевого счета телефона, а также подобные данные через оператора.
- Если у Вас возникают сомнения по поводу услуг, предоставляемых оператором сотовой связи, **позвоните** в службу техподдержки.
- Обращайте внимание на номер телефона звонившего и ни в коем случае **не переводите** денежные средства, даже если просят очень настойчиво. Никогда **не отправляйте** деньги незнакомым лицам на их электронные счета.
- **Не перечисляйте** деньги на электронные кошельки и счета мобильных телефонов людям, которых Вы не знаете.
- **Не переходите** по ссылке, указанной в сообщении.
- При общении в социальных сетях **не размещайте и не передавайте** информацию личного характера, которая может быть использована во вред.
- При появлении подозрений, что звонок поступает от мошенника необходимо незамедлительно **обратиться** с заявлением в ближайшее подразделение органов внутренних дел, прокуратуру либо сообщить об этом по ведомственным «телефонам доверия».



