**ПРАВИТЕЛЬСТВО**
**КУРГАНСКОЙ ОБЛАСТИ**
**ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ**
**КУРГАНСКОЙ ОБЛАСТИ**

ул. Ленина, 35, г. Курган, 640000
телефон (8-3522) 46-14-41, факс 46-05-73
сайт: http://don.kurganobl.ru
эл. почта: mail@don.kurganobl.ru

от 29.07.2020 № ИСХ 08-02950120

на № _____

Руководителям организаций и учреждений, подведомственных Департаменту образования и науки Курганской области

Руководителям органов образования муниципальных районов Курганской области

Департамент образования и науки Курганской области направляет для сведения памятку прокуратуры Курганской области о мерах предосторожности при попытках совершения хищения денежных средств с банковских карт граждан.

Содержание памятки необходимо довести до сотрудников организаций путем проведения соответствующих обучающих занятий, разместить памятку в местах, максимально доступных для граждан, на официальных сайтах в сети «Интернет».

Приложение: на 3 л. в 1 экз.

Заместитель директора Департамента образования и науки Курганской области И.Н. Хлебников

Григорьева Татьяна Александровна
(3522) 46-10-35

## ПРОКУРАТУРА И МВД

## ПРЕДУПРЕЖДАЮТ

Ежедневно 5-6 жителей области сообщают дозвонившимся им мошенникам данные своей банковской карты, в том числе трехзначный числовой код на обратной ее стороне, а затем мошенники крадут с их карт сотни тысяч рублей.

У преступников есть базы данных номеров абонентов сотовых операторов и базы данных банковских карт. Они знают Ваши фамилию, имя, отчество, номер телефона и что у ВАС есть банковская карта в определенном банке. Мошенники умеют хорошо убеждать и обладают навыками психологического воздействия.

Чаще всего злоумышленники звонят с номеров московского региона (495), (499) или (8-800).

На сегодняшний день мошенниками придумано не менее 8 способов обмана. Они представляются сотрудницами банка, сотрудниками отдела безопасности банка, представителями торговых фирм, сотрудниками прокуратуры и т.д. т.д.

### ЗАПОМНИТЕ

**Никто** не имеет права выяснять номер Вашей карты. **Никакая** организация и никакое лицо этого делать не могут.

Если у Вас спрашивают данные вашей карты, прекратите разговор, это мошенники.

Позвоните сами в ту организацию, от имени которой Вам звонили, и Вы убедитесь, что Вам звонили не они, а мошенники.

### ЗАПОМНИТЕ

Выяснять по телефону данные банковской карты могут только мошенники. Кредитные организации и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов или 3-х значного кода.

### ЗАПОМНИТЕ

**Никакие** сотрудники государственных правоохранительных органов не могут предлагать Вам перечислить деньги за что-либо, у них нет таких полномочий.

## ОСНОВНЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

### «НЕ ДОПУСТИТЬ НЕЗАКОННОГО СПИСАНИЯ ВАШИХ ДЕНЕГ»

Мошенники, представляются сотрудниками безопасности банка, либо единой службы безопасности банков, сообщают, что была попытка незаконного списания средств со счета банковской карты и чтобы остановить эту транзакцию нужно назвать реквизиты карты (номер, ФИО держателя карты, CVV-код) и данные о сумме на счету карты.

### «ВАША КАРТА ЗАБЛОКИРОВАНА»

С номеров, которые похожи на сервисный номер Сбербанка (900), например «9ОО» (используются буквы «О»), 9 0 0 (используются пробелы между цифрами), на Ваш телефон поступает SMS-сообщение с текстом, что банковская карта заблокирована. После чего мошенники пытаются узнать реквизиты карты и пароли доступа в личный кабинет.

### «ДОЛГ ПО КРЕДИТУ»

Неизвестный представляется сотрудником банка и просит погасить задолженность по кредиту, который Вы не брали и входе разговора уточняются данные карты (ПИН-код, CVV-код и срок действия карты).

### «КУПЛЯ-ПРОДАЖА ЧЕРЕЗ ИНТЕРНЕТ»

Мошенник под видом покупателя сообщает, что желает приобрести товар, но проживает в другом городе и предлагает оплатить товар путем перечисления денежных средств на Вашу карту. Для этого он просит Вас назвать номер карты, владельца карты, срок действия карты, код на обратной стороне, а так же сотовый номер, привязанный к карте, либо по умолчанию использует номер, указанный в объявлении. После получения этих сведений мошенник использует данные о карте для оплаты покупок в сети Интернет.

Другой вариант, когда мошенник, выступающий в роли «покупателя» предлагает Вам пройти к банкомату и, якобы произведя некоторые операции, получить деньги.

Также злоумышленник под видом продавца просит у Вас предоплату за товар, а при получении денег перестает выходить на связь. Либо предлагает пройти по направленной Вам ссылке для авторизации, где необходимо выведение Ваших персональных данных.

### «КОМПЕНСАЦИЯ»

Неизвестные звонят по телефону, представляясь следователями правоохранительных органов, сотрудниками прокуратуры, и сообщают о возможности возместить стоимость услуг адвоката, а также получить моральную компенсацию за приобретенные фальсифицированные биодобавки или лекарства, а для ее получения необходимо оплатить пошлину.

**«ОШИБОЧНЫЙ ПЕРЕВОД»**

Вам приходит SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат услуг. Сразу после этого поступает звонок, и Вам сообщают, что на Ваш счет ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счёта.

**«ПОМОЩЬ ДРУГУ»**

Неизвестные путем взлома аккаунта друга в социальной сети, направляют Вам сообщение с просьбой пополнить счет или в долг перевести на банковскую карту деньги.

**«РОДСТВЕННИК В БЕДЕ»**

Под видом близких родственников мошенники звонят Вам по телефону и сообщают, что задержаны за совершение какого-либо преступления или дорожно-транспортного происшествия с жертвами. Для освобождения от уголовной ответственности просят перечислить денежные средства через банкомат или передать курьеру.