



## Как вычислить мошенника?

Насторожьтесь, если Вам пришло письмо, сообщение, электронное письмо или ссылка, в котором от Вас требуется предоставление конфиденциальных данных;

Речь в разговорах, письмах или сообщениях всегда идет о деньгах.

Ведь какова цель мошенника?

Правильно! Выманить Ваши деньги!

Вас всегда просят сообщить данные – ПИН-код, пароль и иные реквизиты карты.

Мошенники пытаются повлиять на Вас через эмоции – сильно напугать или же, наоборот, обрадовать.

Вас торопят с переводом или выводом денег? На Вас давят?

Можете не сомневаться –

Вы разговариваете с мошенником!

**Будьте внимательны: если Вы сами сообщили злоумышленникам ПИН-код или код из СМС, необходимый для подтверждения платежей и переводов, к сожалению, банк не вернет деньги.**

## В случае нарушения прав обращайтесь в прокуратуру Краснотурьинска

По адресу: г. Краснотурьинск, ул. Ленина, д. 9

Телефон: 8(34384)6-22-64

Время работы: Пон-Четв: с 9-00 до 18-00; Пятн: с 9-00 до 17-00; обеденный перерыв: с 13-00 до 13-48



ПРОКУРАТУРА СВЕРДЛОВСКОЙ ОБЛАСТИ

ПРОКУРАТУРА  
ГОРОДА КРАСНОТУРЬИНСКА

## Назовите Ваш ПИН-код

Памятка  
«Как распознать  
мошенника?»

2022 г.



## Что делать, если Вы все-таки столкнулись с мошенничеством?

Если с Вашей банковской карты вдруг списали деньги, то не позднее следующего дня, как Вы были уведомлены о незаконной операции сообщите о мошеннической операции в банк и заблокируйте карту.



Обратитесь в отделение банка и напишите заявление о несогласии с операцией. Сохраните экземпляр заявления с отметкой банка о приеме.

Обратитесь в правоохранительные органы с заявлением о хищении Ваших денежных средств.

## Типичные варианты мошенничества с банковскими картами онлайн:

при продаже товара или покупке с рук мошенники – потенциальные покупатели или продавцы – просят не только номер карты, но и секретные данные;

Ваш друг в социальных сетях просит одолжить деньги или же отправляет Вам странную ссылку;

на Вашу электронную почту приходит письмо с информацией о том, что Вы выиграли большую сумму денег, или же с предложением работы, которую Вы не искали, с большой зарплатой;

Вы перешли на известный Вам сайт, например, ГИБДД или ФНС, однако, заметили некие изменения, которые не замечали ранее – лишняя буква в строке браузера, измененный номер телефона для связи с той или иной службой.



Все указанные варианты предполагают предоставления Вами лично конфиденциальной информации о данных своей банковской карты - номер карты, имя и фамилия владельца, срок действия, код проверки подлинности карты (три цифры на обратной стороне, например, CVV или CVC), ПИН-код.

## БУДЬТЕ ВНИМАТЕЛЬНЫ и ОСТОРОЖНЫ!

При подготовке памятки использованы материалы, размещенные на интернет-сайте «Финансовая культура» <https://fincult.info>

