Как не стать жертвой мошенников?

**Главное управление МВД России по Новосибирской области настоятельно рекомендует:**

* 1. Помнить, что сотрудники банка и любых правоохранительных органов никогда не спрашивают никаких данных о Вашей банковской карте, тем более не запрашивают кодов подтверждения, не просят оформить кредит и не просят перевести деньги куда-либо;
	2. Никто, в том числе сотрудник банка, не вправе требовать от держателя карты сообщить код подтверждения операции, поступающий в смс-сообщении. Сообщив данный код, гражданин предоставляет возможность третьим лицам совершить перевод денег с вашего счета;
	3. При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (указан на обороте карты).
	4. Никому не предавать реквизиты своих банковских карт, в том числе покупателю, который хочет приобрести продаваемый Вами товар;
	5. Никогда и не под каким предлогом не переходить по ссылкам, направляемым Вам незнакомыми лицами;
	6. Никогда не перечислять деньги незнакомым людям, даже если они внушают Вам доверие, предоставляют свои документы, положительные отзывы, любые фото и видео доказательства.
	7. Оформлять на свое имя только банковские карты, в которых имеется необходимость, по возможности избегая кредитных карт, и ответственно относиться к их сбережению;
	8. При поступлении звонка на телефон гражданину от лиц, представляющихся родственниками, которые попали в беду, незамедлительно прервать телефонный разговор и позвонить близким людям для убеждения, что с ним все в порядке.

В случае совершения покупок через интернет-магазины:

* 1. Когда вы публикуете объявления, лучше всего выбирать способ связи «В сообщениях». Тогда покупатели не увидят ваш номер телефона и смогут писать только в чат сайта объявлений. Там сервис заблокирует все подозрительные ссылки,
	2. Не переходите в другие мессенджеры для общения. В чате «авито» можно переписываться, отправлять фото и показывать видео. Общайтесь только на сайте объявлений.
	3. Не открывайте ссылки и QR-коды, сайт объявлений никогда и никому их не присылает. Пользователи оплачивают товары, получают деньги и управляют заказами через кнопки в чате.
	4. Не делитесь почтой или телефоном. Мошенники стремятся узнать их, чтобы выслать поддельный чек или ссылку.
	5. Не говорите коды из смс. Ради них злоумышленники могут даже притвориться службой поддержки.
	6. Оплачивайте товар при поступлении.

Настоятельно рекомендуем быть бдительными, не предоставлять и не сообщать свои персональные данные, в том числе по банковским картам (счетам), не убедившись в безопасности их передачи.

Помните, что самый безопасный способ оплаты товара – после его получения.

**На сегодняшний день полиция Новосибирской области располагает современными методами противодействии IT-преступности и предупреждает об уголовной ответственности как за совершение IT-преступлений, так и за пособничество в их совершении, в связи чем настоятельно рекомендует:**

**– в целом воздержаться от совершения преступлений;**

**– не осуществлять никаких операций с найденными банковскими картами;**

**– не оформлять на своё имя сим-карты, организации, банковские карты и расчетные счета с целью их дальнейшей передачи третьим лицам.**

**Помните, что действующие законодательство предусматривает наказание за IT-преступления вплоть до 10 лет лишения свободы.**

**Подробно о всех современных способах совершения IT-преступлений можно прочитать на официальном сайте ГУ МВД России по Новосибирской области, а также в официальном телеграм-аккаунте mvd\_54.**

Информация предоставлена

ГУ МВД России по Новосибирской области