

Сотрудники ГУ МВД России по РО предупреждают граждан от различных махинаций, к которым прибегают мошенники:

Вам приходит электронное письмо якобы от имени банка, платежной системы или онлайн магазина. *При переходе по ссылке* вы попадаете на *поддельный сайт компании,* интерфейс которого внешне не отличим от настоящего сайта, где вас просят ввести свои персональные данные: серию и номер паспорта, данные карт и счетов, пароли для входа в платежные системы, аккаунты в социальных сетях, электронную почту.

«Не дайте себя обмануть!»

- Будьте внимательны при переходе по ссылкам из писем, обращайте внимание на *адресное имя сайта, оно может отличаться от официального всего лишь одним символом.*
- Не спешите вводить свои данные, помните банки и платежные системы никогда не присылают писем с просьбой предоставить свои данные.

« Вирусная рассылка»

Мошенники рассылают смс-сообщения с определённой ссылкой, переходя по которой устройство заражается вредоносной программой.

Данная программа собирает и передаёт мошенникам сведения для хищения денег с банковского счёта либо со счета мобильного оператора

Мошенники используют разнообразные предлоги для того, чтобы вы перешли по ссылке:

- «Ваша карта заблокирована, перейдите по ссылке для ее разблокировки»
- «Мне прислали твою фотографию, я и не мог подумать, что ты так поступишь (ссылка)

Единственное правило, которому стоит передерживаться гражданам, не переходить по сомнительным ссылкам в сообщениях

Если в отношении вас были совершены противоправные действия незамедлительно обратитесь в ближайший отдел полиции

: Полиция предупреждает граждан: никогда и никому не сообщайте данные вашей банковской карты: пин код, верификационный код и коды из смс.

Лжепокупатель может оказаться мошенником.

Вы решили продать в интернете какую-то свою вещь, оставили объявление о продаже на специальном сайте и вам позвонил или написал покупатель. Он не хочет смотреть товар, а сразу желает внести предоплату и требует данные вашей карты, (защитный) трехзначный код безопасности, а также коды из смс, объясняя, что только так он сможет перевести деньги.

Будьте осторожны, это может быть мошенник!

Никому не сообщайте данные вашей банковской карты: пин код, верификационный код и коды из смс.

Как не стать жертвой мошенников.

Вам поступает сообщение о якобы полученном выигрыше, для получения которого нужно перевести организаторам деньги.

Не дай себя обмануть!!

Простые правила:

- выиграть можно только в той лотерее, в которой Вы приняли участие!;
- не сообщайте лжеорганизаторам своих данных;
- не переходите по ссылкам из сообщений;
- Если вы стали жертвой мошенников, незамедлительно обратитесь в полицию

«Телефонное мошенничество»

По телефону мошенники говорят, что родственник или другой близкий человек попал в беду:

- 1) Он попал в серьёзное ДТП;
- 2) Совершил преступление и находится в полиции;
- 3) Попал в больницу и ему нужны деньги на операцию.

После этого, мошенники давят на жертву и предлагают прямо сейчас «решить вопрос» спасти близкого. Нередко для подтверждения трубка передаётся «родственнику». Голос может быть похож, на самом деле пострадавшие просто находятся в состоянии шока. Затем преступники называют сумму которую необходимо передать или перевести.

Пример:

Мошенник позвонил пенсионерке, и сообщил что ее сын убил человека. Для решения вопроса ей нужно передать 450к рублей. В назначенное время подъехал водитель и забрал деньги. Пенсионерка через некоторое время связалась с сыном и поняла, что была обманута!

Не дай себя обмануть!!

Три условия:

- Никогда и никому не отправляйте и не передавайте деньги;
- Свяжитесь со своим близким;
- Позвоните в полицию или в больницу и проверьте полученную информацию;
- Если вы стали жертвой мошенников, незамедлительно обратитесь в ближайший отдел полиции.