



С развитием современных информационно-телекоммуникационных технологий представить жизнь современного человека без уже ставших

привычными нам технических устройств, электронных средств платежа, невозможно. Их простота и доступность в использовании привлекают все большее и большее число пользователей.



Вместе с тем, не отстают от них и преступники, использующие современные технологии в своих криминальных целях.

### РАСПРОСТРАНЕННЫЕ СХЕМЫ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

- Ошибочный перевод средств на банковский счет с просьбой вернуть деньги;
- SMS-рассылка или электронное письмо с сообщением о выигрыше автомобиля, недвижимости или иных ценных призов, с целью получения которого необходимо заплатить налог или заплатить определенную сумму;
- Сообщение с просьбой о помощи: требование/просьба перевести определенную сумму, в связи с тем, что близкий родственник либо знакомый находится в опасности, либо задержан сотрудниками правоохранительных органов;



- SMS: «Ваша карта временно заблокирована, перезвоните по номеру» с целью узнать персональные данные банковской карты;

- Размещение объявлений о продаже товаров на электронных площадках и Интернет-аукционах. Как правило, злоумышленники привлекают своих жертв заниженными ценами и выгодными предложениями и требует перечисления предоплаты путем перевода денежных средств на электронный кошелек.



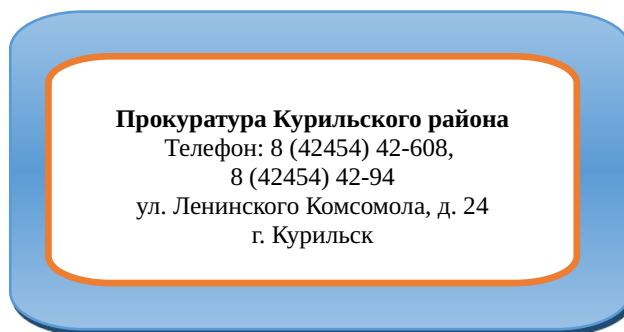
- «Мошенничество в сфере знакомств». На сайтах знакомств, мошенники, выбирая жертву налаживают переписку, обещая приехать с целью создания семьи и просят перевести денежные средства для проезда или погашения долгов.

- **Сообщения о переходе на неизвестные ссылки в сети Интернет**

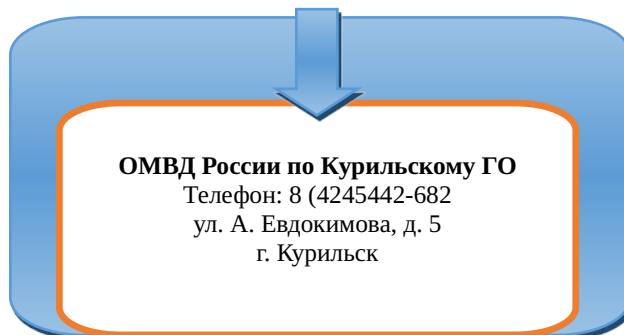
7. Не перезванивать по номерам и не переходить по ссылкам, которые приходят на e-mail или по SMS.

## КАК НЕ СТАТЬ ЖЕРТВОЙ ЭЛЕКТРОННОГО МОШЕННИЧЕСТВА

1. Установить на телефон или компьютер современное лицензированное антивирусное программное обеспечение;
2. Не устанавливать и не сохранять без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников;
3. Не использовать пароли, связанные с персональными данными;
4. Не сообщать данные карты, пароли и другую персональную информацию;
5. Поставить лимит на сумму списаний или перевода в личном кабинете банка;
6. В случае возникновения вопросов обращаться в банк, выдавший карту;



**СООБЩАЙТЕ  
О ФАКТАХ МОШЕННИЧЕСТВА**



**Прокуратура Курильского района  
Сахалинской области**

**ПАМЯТКА**

**«Профилактика и  
предупреждение  
дистанционных**



**преступлений  
в сфере  
информационно-  
телекоммуникацион  
ных технологий»**

г. Курильск, 2022 год

