Противодействие преступлениям, совершаемым с использованием информационных технологий и методов социальной инженерии.

Потерпевшими от таких преступлений являются граждане абсолютно всех категорий.

При совершении преступлений:

- потерпевшие сами предоставили конфиденциальные данные преступникам, позволившие похитить со счета денежные средства;
- потерпевшие под воздействием обмана самостоятельно осуществляли операции по переводу злоумышленникам денежных средств, в том числе,

предварительно оформив на себя кредиты на существенные суммы.

Самые распространенные способы хищений денежных средств граждан:

1.Вам звонят из службы безопасности банка и сообщают, что по вашей карте производится незаконное снятие денежных средств, просят назвать полный номер карты, трехзначный код на обороте карты и код из поступившего смс».

2.Сотрудники Центробанка сообщают, что произошла попытка оформления кредита, сообщите код из смс-сообщений или переведите деньги на безопасный счет».

3.Вам звонят из правоохранительных органов и сообщают, что родственник попал в беду (ДТП, возбуждено уголовное дело и т.д.), перечислите деньги».

4.Специалист Росфинмониторинга сообщает, что с ваших счетов финансируется терроризм или идет перевод средств в иностранные банки для того, чтобы остановить перехват преступников.

5.Представитель сотовой компании сообщает, что необходимо

продлить срок действия договора на оказание услуг сотовой связи. Для этого необходимо сообщить персональные данные и коды, пришедшие в смс-сообщениях.

6.Мошенники могут представиться сотрудниками почты, «Госуслуг», Пенсионного фонда, покупателем на «Авито» и даже прокуратуры - список не ограничен!!!

Под любыми предлогами они будут выманивать код из смс, просить его назвать «автоматизированной системе» в условиях строгой конфиденциальности!

Помните - это МОШЕННИКИ!

Как не стать жертвой мошенников:

- Никогда не отправляйте деньги незнакомым лицам на их электронные счета!
- Никогда не пользуйтесь услугами непроверенных и неизвестных сайтов!
- Никогда не переходите по ссылке, указанной в сообщении на скачивание открытки, музыки, программы и т.д.!
- Никогда не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред!
- Не передавайте никому код из СМС, даже если представляются сотрудником банка!
- Никому не сообщайте данные своей банковской карты!
- Не реагируйте на звонки, где сообщают, что родственник попал в ДТП. При поступлении таких звонков, в обязательном порядке свяжитесь с родственником, уточните действительно ли он находятся в трудной ситуации и сообщите в органы полиции о произошедшем.

Будьте бдительны и доведите указанную информацию до своих родных и близких!

В целях детального разъяснения, просим всех жителей муниципалитета ознакомиться с социальными видеороликами, подготовленными

Дальневосточным юридическим институтом (филиалом) Университета прокуратуры Российской Федерации, переходя по ссылкам:

https://disk.yandex.ru/i/WaxOnz8zzDpXQQ;

https://disk.yandex.ru/i/VgQM6cWLVCat8g;

https://disk.yandex.ru/i/I06gdo2qjz7PAQ;

https://disk.yandex.ru/i/VieGq2HBFI9b