

Несмотря на принимаемые правоохранительными органами меры, дистанционные хищения с использованием информационно-телекоммуникационных технологий стремительно набирают силу. Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву раскрывать всю информацию о себе либо совершать те или иные действия, используют человеческие слабости (стяжательство, алчность), чувства (сострадание, обеспокоенность за близких, жалость) в своих корыстных интересах.



1. Случай с родственником.

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками полиции за совершение какого-либо правонарушения. Просит передать ему какую-то сумму через человека с которым необходимо встретиться.

2. Розыгрыш призов (это могут быть телефон, ноутбук, автомобиль и др.).

На телефон абонента сотовой связи приходит смс-сообщение, из которого следует, что в результате проведенной лотереи он выиграл автомобиль. Для уточнения всех деталей предлагается позвонить по одному из указанных телефонных номеров. Во время разговора мошенники сообщают о том, что для

выполнения необходимых формальностей счастливому обладателю автомобиля необходимо перечислить на счет указанную ими сумму. Как только перечисляются деньги- обнуляют счет и выключают телефон.

3. SMS-просьба.

Абонент получает на мобильный телефон сообщение: «У меня проблемы, позвони по такому-то номеру, если номер не доступен, положи на него определенную сумму и перезвони». Человек пополняет счёт и перезванивает, телефон по-прежнему не доступен, а деньги вернуть уже невозможно.

4. Платный код.

Поступает звонок, якобы от сотрудника службы технической поддержки оператора мобильной связи, с предложением подключить новую услугу для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

5. Ошибочный перевод средств.

Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а человек переводит свои собственные средства.

6. Продажа имущества на интернет-сайтах.

При звонке на телефон, размещенный на Интернет-сайтах объявлений (Авито, ФарПост, Дром и др.) правонарушитель просит пополнить счет его телефона, либо сообщить данные и номер карты потерпевшего для перевода денежных средств в качестве задатка за товар. После сообщения данных карты происходит списание денежных средств.

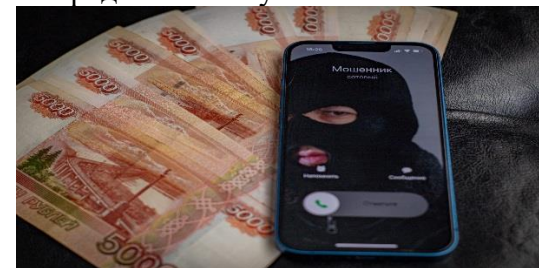
7. Новая схема телефонного мошенничества «Вишинг».

Цель мошенников под любым предлогом извлечь секретную личную информацию о кредитке. Для получения доступа к конфиденциальным данным владельца мнимые помощники используют телефонную связь как в автоматизированном режиме, так и напрямую от мнимого «операциониста» банковского сектора.

8. Хищения с карт, подключенных к опции бесконтактных платежей.

Для проведения оплаты по такой карте достаточно приложить её к терминалу. Ввод ПИН-кода не требуется если сумма не превышает 1 000 рублей. При этом количество расходных транзакций не ограничено.

Чтобы получить деньги, мошеннику даже не понадобится воровать карту у клиента. Если в общественном транспорте поднести устройство к сумке или карману владельца, то средства спишутся.



**ПАМЯТКА для граждан о
профилактике и предупреждении
дистанционных преступлений в
сфере информационно-
телекоммуникационных
технологий:**

Чтобы не оказаться жертвой мошенников необходимо знать следующее:

- сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;
- не при каких обстоятельствах не сообщать данные вашей банковской карты, а так же секретный код на оборотной стороне карты;
- хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;
- не сообщать пин-код третьим лицам;
- остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;
- лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;
- внимательно читайте СМС сообщения приходящие от банка;
- никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС сообщении от банка;
- помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в СМС сообщении от банка;
- сотрудники банка никогда не попросят вас пройти к банкомату;

- если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;
- не покупайте в интернет – магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;
- никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;
- в сети «Интернет» не переходите по ссылкам на неизвестные сайты;
- действуйте обдуманно, не торопливо, помните, что «Бесплатный сыр только в мышеловке».

**Каждый человек может стать
жертвой мошенничества, если не
будет следовать простым правилам
безопасности!**

Наш адрес:

–354200, г. Сочи, мкр. Лазаревское,
ул. Партизанская, д.6,
тел. **270-07-24**
с. Детляжка ул. Рязанская, д.12,
тел. 252-93-64;
пос. Дагомыс, ул. Делегатская, д.12,тел. **252-16-91;**
мкр. Лоо, ул. Разина, д.22-а,
тел. 252-72-61.

МИНИСТЕРСТВО ТРУДА И
СОЦИАЛЬНОГО РАЗВИТИЯ
КРАСНОДАРСКОГО КРАЯ
ГБУ СО КК «СОЧИНСКИЙ КЦСОН
ЛАЗАРЕВСКОГО РАЙОНА»
Организационно-методическое
отделение

**Профилактика и предупреждение
дистанционных преступлений в
сфере информационно-
телекоммуникационных технологий
в отношении пожилых граждан.**



г.Сочи
2023