СОГЛАСЕН

Александровский городской прокурор

старший советник юстиции

А.А. Антонов

«____» марта 2025 года

ИНФОРМАЦИЯ
для размещения в СМИ

Осторожно мошенники!

Статьей 159 Уголовного кодекса Российской Федерации (далее - УК РФ) предусмотрена уголовная ответственность за мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

В настоящее время наблюдается значительный рост числа подобных преступлений, совершаемых дистанционно, с применением мобильных устройств или интернет-технологий.

Анализируя увеличение случаев кражи денежных средств посредством обмана или злоупотребления доверием с использованием мобильной связи или интернета, важно выделить наиболее часто встречающиеся методы и инструменты, применяемые преступниками.

Одним из самых распространенных приемов является сбор злоумышленниками личной информации о жертве, чтобы создать видимость доверия и использовать ее в своих корыстных целях.

Злоумышленники, совершая телефонные звонки, выдают себя за работников службы безопасности, как правило, банковских учреждений. В ходе беседы они обманным путем убеждают жертву, что действуют в ее же интересах. Разговор начинается с обращения, например: «Здравствуйте, Петр Иванович! Я из службы безопасности банка. Обнаружена попытка несанкционированного доступа к вашей карте. Чтобы предотвратить кражу, предлагаем перевести средства на защищенный счет. Для этого сообщите код, который поступит вам в СМС».

Важно понимать, что настоящий сотрудник банка имеет доступ ко всей клиентской информации и никогда не запросит номер карты, договора или счета. Подобные вопросы указывают на то, что с вами общается мошенник, стремящийся получить доступ к вашим банковским данным.

Преступники нередко выдают себя за сотрудников полиции, прокуратуры, ФСБ и других силовых структур. Важно помнить, что представители правоохранительных органов никогда не запрашивают данные банковских карт, коды из СМС, не требуют перевода денег, установки программ или оформления кредитов.

Кроме того, злоумышленники могут совершать преступления дистанционно, получая доступ к мобильным устройствам на базе операционной системы Android, зараженным вредоносным программным обеспечением. Заражение обычно происходит при установке приложений из ненадежных источников, переходе по подозрительным ссылкам, а также при отсутствии антивируса или его обновлений. Вирус перехватывает управление СМС, скрывая сообщения, связанные с «Мобильным банком» (или с номером «900»).

Схожая схема используется и при заражении компьютеров. Киберпреступники распространяют вредоносное программное обеспечение через веб-сайты, электронную почту, маскируя его под полезные программы или объявления для компьютерной техники и мобильных устройств. Пользователи, сами того не подозревая, заражают свои устройства, используя небезопасный интернет-контент.

Злоумышленники, используя вредоносное программное обеспечение, получают несанкционированный доступ к компьютерам или мобильным устройствам жертвы, что приводит к краже денежных средств:

- С банковских карт и счетов, особенно если на устройствах использовались системы онлайн-банкинга.
- Со счетов в электронных платежных системах, которыми пользуется жертва.
- С баланса мобильного телефона при заражении современных смартфонов.

Похищенные средства переводятся на счета, карты, электронные кошельки или телефонные номера, контролируемые преступником. Затем деньги собираются на промежуточном счете и обналичиваются лично или через сообщников.

Александровская городская прокуратура предупреждает: ни при каких обстоятельствах нельзя сообщать по телефону третьим лицам (независимо от их представительства) данные кредитных карт, счетов и прочую информацию о финансовых вкладах, устанавливать подозрительные приложения или передавать коды из СМС.

Прокуратура напоминает: при общении с незнакомцами, запрашивающими информацию о счетах, вкладах, номерах карт или сообщающих о выигрышах, следует соблюдать следующие правила:

1. Не разглашайте по телефону личные данные, данные карт или коды из СМС.
2. При посещении сайтов и загрузке приложений, обращайте внимание на названия сайтов и источники загрузки, используйте антивирусное программное обеспечение.

Помощник городского прокурора Д.Д. Девочкин