Добрый день уважаемые жители, прокуратурой района продолжается работа по правовому просвещению населения. Сегодня хочу разъяснить некоторые способы совершения преступлений с использованием информационно-коммуникационных технологий и алгоритме действий при контакте со злоумышленниками.

1. Покупки в интернете. Клиент находит объявление о продаже товара или услуг. Переводит деньги, мошенники перестают выходить на связь.

2. «Близкий человек попал в беду». В соцсетях пишет родственник или друг. Он попал в непростую ситуацию и ему срочно нужны деньги. Так действуют мошенники, взломав аккаунты.

3. Служба безопасности банка. Клиенту поступает звонок или SMS с просьбой перезвонить. Мошенники представляются службой безопасности банка, говорят, что зафиксирована попытка списания денег со счета клиента, выясняют данные карты и коды подтверждения и списывают деньги со счета.

4. Лотерея или опрос. Клиент видит рекламу в интернете или таргетированную рассылку: можно получить вознаграждение, поучаствовав в лотерее или пройти опрос. Для этого нужно заполнить небольшую форму. Клиент вводит данные карты — мошенники списывают средства, либо получают данные для последующих попыток обмана.

5. Продажа в интернете. Клиент размещает объявление о продаже товара. Мошенники звонят и узнают данные карты продавца под предлогом необходимости совершить перевод за товар. Далее они списывают деньги с карты, узнав у продавца код подтверждения (якобы он нужен для зачисления).

6. Черные брокеры. Клиенту поступает предложение заработать на инвестициях. Он связывается с лжеброкерами и переводит им деньги для игры на бирже. Сумма на «брокерском» счете начинает быстро расти. Клиент хочет вывести средства, но для этого нужно заплатить дополнительную комиссию. Он переводит деньги — мошенники пропадают.

7. Программы удаленного доступа. Звонит «служба безопасности банка»: на устройстве клиента обнаружен вирус, необходимо скачать антивирус и сканировать гаджет. Во время сканирования устройство, якобы, нельзя использовать, так как вирус может распространиться дальше. На самом деле клиент скачивает программу удаленного доступа, а во время «проверки» мошенники получают доступ к мобильному банкингу и выводят средства клиента.

8. Безопасный счет. Звонок от «службы безопасности»: произошла утечка данных, в ней замешаны сотрудники. Необходимо снять деньги через безопасный банкомат банка-партнера и перевести их на специальный страховочный счет.

9. Знакомства в сети. На сайте знакомств девушка предлагает сходить в кино. Отправляет ссылку на сайт-однодневку VIP-кинотеатра. Клиент покупает билеты, на этом знакомство завершается.

За все перечисленные действия предусмотрена уголовная ответственность, предусмотренная статьей 159 УК РФ (мошенничество, то есть хищение чужого

имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием).

Алгоритм действий в таких ситуациях:

Не отправлять денежные средства на неизвестные адреса, в том числе с целью приобретения вещей в сети Интернет.

Не верить телефонным звонкам с неизвестных номеров о том, что ваш родственник, близкий или знакомый совершили, или пострадали в ДТП, стали соучастниками преступления. Задайте звонящему вопросы личного характера, помогающие отличить близкого человека от мошенника. Под любым предлогом прервать контакт с собеседником и перезвонить родным и узнать, все ли у них в порядке.

Не разглашать свои персональные данные, такие как фамилия, имя, отчество, паспортные данные, данные банковских карт, счетов, а также защитные коды и пароли, ни под каким предлогом;

Не передавать деньги не знакомым лицам, не под каким предлогом.

Не соглашаться на предложение обменять деньги на новые или иностранные купюры. Рассказы о грядущей денежной реформы не правда.

Не доверять СМС-сообщениям, приходящим на телефон, будь то крупный выигрыш, победа в конкурсе или лотереи, особенно в тех случаях, когда для получения выигрыша просят оплатить налог. Необходимо знать, что настоящий розыгрыш призов не должен подразумевать денежные выплаты с Вашей стороны!

Не перезванивать на номер, с которого пришло СМС-сообщение о том, что банковская карта заблокирована и не отправлять ответных смс-сообщений. Позвоните в банк, выпустивший и обслуживающий карту (телефон банка указан на обороте банковской карты).

Избегать лиц, которые навязчиво пытаются вовлечь в разговор, предлагают какие-либо товары и услуги или же хотят поделиться найденными деньгами.

Избегать внимания людей при снятии денег с банковской карты или сберегательной книжки.

Берегите свои денежные средства!

Помощник прокурора Братского района  В.В. Кошева