Несмотря на противодействие правоохранительных органов, информационные технологии развиваются, а с ними появляются новые способы хищений. Недобросовестные граждане как в одиночку, так и группой реализуют мошеннические схемы увода средств с банковских карт и телефонов у населения в регионе.

Не исключением является и Угловский район.

Раньше от телефонных мошенников страдали в основном одинокие люди пожилого возраста в силу их доверчивости.

Им приходили СМС о том, что их близкий или родственник попал в беду, в ДТП. Чтобы уладить дело, мошенники просили выслать определенную сумму. И бабушки отправляли последние сбережения, порой весьма значительные. С аналогичной просьбой могли поступать звонки на домашние телефоны.

Кроме указанных в настоящее время есть и другие методы электронного воровства, на которые попадаются люди среднего возраста, считающие себя вполне грамотными и адекватными.

В 2015г. на территории района зарегистрирован ряд преступлений, связанных с хищением денежных средств путем мошенничества со счетов граждан.

Основными способами мошенничества являются: звонят и говорят, что ваш сын попал в ДТП, отправляют СМС-сообщения «Ваша карта заблокирована», просят перевести компенсацию за медицинские аппараты и препараты, оплатить покупки через интернет-сайт. Звонки и СМС поступают из самых разнообразных городов страны.

В некоторых случаях мошенники, промышляющие на сайте avito.ru, переводят часть суммы и просят под разными предлогами дать дополнительные данные о банковском счете или ПИН-код карты. После этого преступник дистанционно получает право доступа к счету и самостоятельно переводит с него деньги.

Так, житель одного из сел района продавал мед, ему позвонил преступник, предложил купить всю партию меда сразу и поинтересовался есть ли у него банковская карта и подключен ли к ней «мобильный банк» с целью перечисления на нее обусловленной суммы. Продавец меда сообщил, что банковская карта с подключенным «мобильным банком» есть у жены и передал трубку для дальнейшего разговора супруге. Та в свою очередь сообщила преступнику номер банковской карты. После этого преступник положил трубку и сказал, что перезвонит. Через короткий промежуток времени он перезвонил и попросил сообщить ему пароль, который пришел для подтверждения торговой операции на сотовый телефон потерпевшей, который она ему сообщила. Таким образом преступник несколько раз просил сообщить ему пароли, которые приходили на телефон потерпевшей. Тем самым преступник похитил с банковской карты потерпевшей значительную сумму денег.

Еще одним примером является факт взлома странички одного из друзей в социальных сетях, от имени которого под различными предлогами потом у

потерпевшего выясняются данные банковской карты, с которой в последующем похищаются денежные средства.

Иногда по телефону просят подключить услугу «Мобильный банк» для якобы ускорения перевода. Продавец идет к банкомату, подключает услугу, в тот момент мошенник «привязывает» банковский счет потерпевшего к своему «Мобильному банку», получая таким образом доступ к электронным деньгам жертвы.

Гораздо труднее выявить злоумышленника, если он проник в «Мобильный банк», а затем и на банковский счет через Интернет с помощью программы-вируса. Такие факты также имели место на территории района.

Так, в смартфон потерпевшего попадает вирус чаще всего во время закачки сервисных программ из непроверенных источников. Злоумышленник может поменять в названии программы размер буквы или ее шрифт с кириллицы на латиницу. Это трудно заметить. Потерпевший проходит по фальшивой ссылке, и телефон заражается.

Вирус можно занести при оплате услуг или покупке на ненадежных сайтах, при получении писем на электронную почту, при получении СМС, в которых говорится, что вам прислали фотографию, для ее получения пройдите по ссылке. Потерпевший проходит по ссылке и вирус заражает смартфон. Работая в автономном режиме, вирус отправляет СМС -запросы на номер сервиса «Мобильный банк», получает информацию о подключенном счете и предоставляет ее на сервер преступников.

Так как в банках существует лимит по снятию наличных со счета, то злоумышленники выводят их ежедневно небольшими суммами. При этом программа-вирус все СМС и звонки от банка о снятии денег блокирует.

По мнению специалистов, даже если удалить приложение, с которого был закачен вирус, он все равно останется в телефоне. И в связи с тем, что большинство пользуется бесплатными тестовыми версиями антивирусных программам, они не могут распознать вирус.

Действия потерпевших при хищении денег с банковской карты должны быть следующими.

1. Необходимо обратиться в банк, со счета которого похищены средства. Если деньги ушли на номера телефонов, звонить на «горячие линии» соответствующих сотовых компаний, объяснить ситуацию и попытаться заморозить их дальнейшее движение. С информацией о движении денежных средств потерпевший может обратиться в полицию. Потерпевшим необходимо приготовиться к тому, что телефон, через который совершено хищение, будет изъят полицией примерно на месяц. За это время правоохранители сумеют выделить из него образец вируса, который является вещественным доказательством преступления.

2. Не передавать незнакомым людям номера, ПИН-коды пластиковых карт, номера банковского счета, а также личные персональные данные (фамилия, имя, отчество).

3. В случае поступления СМС о блокировке счета не перезванивать по этому телефону, а обратиться в представительство банка, где находится счет.

4. Не соглашаться на предложение мошенников о переводе задатка на банковский счет и сим-карту сотовых операторов.

5. При поступлении звонка от неизвестных лиц о том, что с вашим родственником произошел несчастный случай, перезвонить родственнику и в полицию, чтобы убедиться в правдивости информации.

6. При смене сим-карты сотовых операторов необходимо сразу отключить услугу «Мобильный банк», написав в банк, где была подключена услуга, соответствующее заявление.

7. Если телефон использует операционную систему android, то отключить услугу «Мобильный банк», заменив ее услугой «СМС-оповещение о движении денежных средств». Либо пользоваться «Мобильным банком» со стационарного компьютера, который более защищен от вирусов, чем телефон.

8. Перед закачкой программы из ненадежных источников ограничить в настройках телефона права программы. Если программа требует права администратора, возможность совершать входящие и исходящие вызовы, то это должно вызвать подозрение.

Прокурор района
Клименко Р.Ю.