Вопрос: Каковы отличительные особенности хищений, совершаемых с использованием ИТК? И как не стать жертвой мошенников?

Ответ: Все рассматриваемые хищения денежных средств с банковских счетов граждан, совершенных с использованием систем дистанционного банковского обслуживания, целесообразно разделить на две основные группы: бесконтактные, т.е. совершаемые без контакта злоумышленника с потенциальным потерпевшим, и контактные, т.е. совершаемые посредством установления контакт злоумышленника с потенциальным потерпевшим (например, путем телефонного звонка или SMS-сообщения).

Указанные виды хищений характеризуются рядом особенностей:

1. При совершении рассматриваемых преступлений всегда используется банковская карта либо сотовый телефон:

- с установленными (посредством специальных приложений) банковскими картами;
- с подключенной услугой «Мобильный банк» к счету банковской карты ПАО «Сбербанк».

2. Как правило, в преступлениях с использованием систем дистанционного банковского обслуживания участвуют несколько лиц (в том числе и непосвященных в преступный замысел мошенников).
3. Хищения такого рода могут быть совершены лицами (осужденными) непосредственно в пенитенциарных учреждениях, либо в период нахождения последних вне мест лишения свободы.
4. Для общения с потенциальными жертвами злоумышленники используют телефонный звонок, либо SMS - сообщение.
5. Основной целью злоумышленников в данном случае является необходимость убедить жертву в реальности предоставляемой ей информации, наличности факта потенциальной «угрозы» его близким родственникам, потери денежных средств и пр. и необходимости передачи (перевода) денежных средств мошенникам добровольно.
6. Установление места совершения преступления, их раскрытие и расследование затрудняет то, что они начинаются на территории одного субъекта РФ, а продолжаются и заканчиваются на территории другого, либо вообще за пределами территории России. Исходя из этого, потерпевшие по уголовному делу могут находиться в одном регионе страны, а лица, совершившие преступление - в другом.

Для того, чтобы не стать жертвой мошенников, необходимо придерживаться основных правил:

1. Не оставляйте данные своих банковских карт на подозрительных сайтах;
2. Перед покупкой в интернет магазинах убедитесь в его безопасности;
3. Не сообщайте данные своих карт по телефону;
4. Если звонит покупатель и продавец товара соглашайтесь на оплату только после передачи товара;
5. Не отвечайте на подозрительные звонки и смс;
6. В случае поступления звонка из банка, перезвоните на официальные номер своего банка, чтобы уточнить сложившуюся ситуацию;
7. Не открывайте неизвестные ссылки, поступившие с незнакомых вам номеров;
8. Установите ограничения на операции – платежи, переводы и снятие;
9. Не храните большие суммы денег на основной карте, которой постоянно пользуетесь;
10. Обязательно подключите оповещения по смс;
11. Старайтесь пользоваться банкоматами, которые стоят в отделениях банков, перед операцией убедитесь, что отсутствуют какие-либо устройства в картоприемнике и накладные клавиатуры;
12. Установите на компьютер и телефон антивирус и регулярно обновляйте его;
13. Ничего не загружайте с подозрительных сайтов;
14. В случае утери карты сразу обратитесь в свой банк для ее блокировки.

Прокурор Конышевского района Н.В.Силаков