Профилактика дистанционного мошенничества.

Дистанционное мошенничество, преимущественно, совершается следующими способами:

- Потерпевшие под различными предлогами перечисляют денежные средства мошенникам.

- Потерпевшие сообщают мошенникам реквизиты и пароли доступа к операциям по счету посредством поступившего им СМС-сообщения, что приводит к хищению денежных средств.

- Значительную распространённость имеют преступления, совершенные с использованием высоких технологий, то есть в сети Интернет, в том числе объявления о продаже и рассылки вирусных ссылок в социальных сетях.

Анализ преступлений, совершенных дистанционным способом, показывает, что одним из признаков подготавливаемого или совершаемого преступления телефонного мошенничества является, когда мошенники выступают в роли «сотрудников службы безопасности банков» и в ходе телефонного разговора получают информацию по банковской карте (номер банковской карты, а также CV-код).

Дальнейшим основным фактором является получение злоумышленниками разового пароля (в виде СМС-сообщения), который поступает на абонентский номер, привязанный к банковской карте. Держатель банковской карты сообщает разовый пароль мошенникам, тем самым предоставляет доступ к денежным средствам

В настоящее время активно распространен вид телефонного мошенничества, злоумышленники звонят и представляются сотрудниками служб безопасности банков, после чего дезинформируют о том, что с карты осуществляются попытки несанкционированного списания денежных средств.

Основные моменты:

1. Не диктовать пароли из смс-сообщений.

2. При поступлении подобного рода звонка, незамедлительно завершить разговор, и перезвонить по официальному телефону банка.

3. В случае утери телефона незамедлительно сообщите в банк о приостановлении (блокировке) имеющихся на счетах сбережений.

Наибольшее количество мошенничеств данного вида зарегистрировано в крупных городах, что составляет более 70% от всего количества зарегистрированных мошенничеств.

В массиве зарегистрированных «дистанционных» мошенничеств наиболее распространенными по способу совершения являются:

- Получение сведений о банковской карте при купле-продаже товаров на сайтах бесплатных объявлений;

- Покупка или продажа товара на Интернет-площадках, когда используются сайты-двойники, в домене которых имеется небольшое различие с оригиналом, зачастую лишь в одном символе;

- Просьба в предоставлении денежных средств родственнику или знакомому, чаще всего через социальные сети, доступ к которым взламывается злоумышленниками;

- В сфере грузоперевозок, когда злоумышленники путем взлома аккаунтов добросовестных перевозчиков, завладевают грузом, причиняя материальные ущербы, исчисляемые миллионами рублей.

Убеждайтесь в достоверности информации, полученной в ходе телефонного разговора и интернет переписки с неизвестными. Мошенники могут представляться сотрудниками правоохранительных органов, представителями операторов сотовой связи и банковских учреждений, знакомыми и даже Вашими родственниками. Обязательно свяжитесь с теми, от чьего имени действуют незнакомцы, и убедитесь в правдивости информации.

Ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и карт, тем более пароли от них.

Фишинг — мошенничество по получению конфиденциальных данных. Это самый распространённый способ интернет-мошенничества на сегодняшний день и не связан с банковскими картами напрямую. Вы получаете письмо (будто бы от банка или от другой

реальной организации), переходите, ничего не подозревая, по ссылке, которая есть в письме. Для входа в аккаунт вводите свой логин и пароль, что и получают злоумышленники. Потому что сайт был сделан мошенниками для сбора конфиденциальной информации. Для создания сообщений используется логотип, стиль организации, от которой якобы отправлено письмо, оно может быть именным. Или приходит SMS-сообщение, что с картой проблемы, с ней совершены мошеннические действия, а чтобы устранить угрозу, необходимо позвонить по указанному телефону. Жертва звонит, и ее просят назвать PIN-код или пароль.

Рекомендации гражданам:

1. Только мошенники могут запрашивать Ваш номер мобильного телефона и другую дополнительную информацию, помимо идентификатора, постоянного и одноразового паролей.

2. Только мошенники могут запрашивать пароли для отмены операций или шаблонов в «Сбербанк Он-лайн». Если Вам предлагается ввести пароль для отмены или подтверждения операций, которые Вы НЕ совершали, то прекратите сеанс использования услуги и срочно обратитесь в банк.

3. Никому не сообщать пин-, CVC- или CVV- коды банковской карты и одноразовые пароли;

4. В торговых точках, ресторанах и кафе все действия с банковской картой должны происходить в присутствии держателя карты. В противном случае мошенники могут получить реквизиты карты, либо сделать копию при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки;

5. В случае потери банковской карты немедленно позвонить в банк для блокировки - это поможет сохранить денежные средства;

6. Подключить услугу СМС-информирование - это обеспечит контроль за проведением любых операций по карте. При получении СМС о несанкционированном списании средств со счета, заблокировать карту;

7. Установить лимит выдачи денежных средств в сутки и за одну операцию (это можно сделать в отделении банка или удалённо в Интернет-банке). Мошенники не смогут воспользоваться сразу всей суммой, которая находится на карте;

8. При вводе пин-кода прикрывать клавиатуру. Вводить пин-код быстрыми отработанными движениями - это поможет в случае установки скрытых видеокамер мошенников;

9. Выбирать для пользования терминалы и банкоматы, которые расположены непосредственно в отделениях банка или других охраняемых учреждениях;

10. Использовать банковскую карту в торговых точках, не вызывающих подозрений;

11. Перед тем как вставить карту в картоприемник, внимательно осмотреть банкомат на предмет наличия подозрительных устройств, проверить, надежно ли они закреплены.

12. В случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или самопроизвольно перезагружается, рекомендуется отказаться от его использования.

13. Не сообщать реквизиты карты никому. Представители банка их знают! Ни одна организация, включая банк, не вправе требовать ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка.

Заместитель прокурора района
Силич С.Ю.