|  |
| --- |
| **« УТВЕРЖДАЮ »** |
| И.о. прокурора Волосовского района |
| наименование органа прокуратуры |
| младший советник юстиции |
| классный чин, фамилия, инициалы прокурора |
| Жигунов М.С. |
|  |
|  |
| (подпись) |
|  |

Прокуратура Волосовского района разъясняет о преступлениях в сфере информационно-коммуникационных технологий.

Надзорная и координационная деятельность свидетельствует, что наиболее массовыми в последнее время стали факты дистанционного хищения с банковских карт и счетов граждан, которые совершаются с использованием информационно – коммуникационных технологий (далее – ИТТ).

Преступники используют предоставленные самими же гражданами возможности «управлять» своими денежными средствами через мобильный телефон или компьютер: переводить деньги, оформлять кредиты, совершать покупки в «Интернет-магазинах» и др. Преступники обладают умением и мошенническими навыками по работе с различными банковскими сервисами.

В частности используются различные способы:

- преступники звонят гражданам, которые разместили объявления о продаже каких-либо товаров или предоставлении услуг на сайтах бесплатных объявлений, чаще всего на сайте «Авито». Предлагают внести предоплату и просят назвать реквизиты банковской карты: ее номер, срок действия, цифровые пароли и т.д.;

- мошенники рассылают СМС-сообщения, либо совершают «обзвон» и абонентам сообщают ложную информацию о, якобы, возникших проблемах с банковской картой.

Очень часто в таких случаях мошенники называются сотрудниками службы безопасности различных банков. Потенциальную жертву подкупает то, что номер телефона звонящего зачастую похож на настоящий номер банка;

- практически всегда собеседник, обладая отдельными психологическими способностями, «влияет» на жертву преступления, доверительно обращается к потерпевшему по имени и отчеству. В результате гражданин выполняет «инструкции» злоумышленника по переводу средств на, так называемые, «безопасные счеты», телефонные номера в результате чего лишается своих денег.

Для сведения: все владельцы банковских карт должны знать, что сотрудники банков никогда не звонят своим клиентам для того, чтобы узнавать информацию по счету, попросить сделать какие-то переводы. Работники кредитных организаций в силу специфики их деятельности обладают и так всей необходимой информацией о клиентах.

Для выяснения любой сомнительной ситуации необходимо гражданам самим звонить в банк по телефону, указанному на карточке.

Современные компьютерные программы (it-технологии) позволяют преступникам использовать, так называемые «подменные номера».

В частности, гражданину поступает звонок на телефон, который определяется как номер дежурной части полиции, диспетчерской службы, номер «горячей линии» банка или другой знакомый ему номер.

Потерпевший умышленно вводится тем самым в заблуждение и выполняет требования мнимых сотрудников правоохранительных органов, служб безопасности.

В таких случаях не надо вести переговоры, следует положить трубку и перезвонить самим по данному номеру. Так будут исключены общения с мошенниками и клиенты смогут сохранить свои сбережения на счетах.

В этой связи, в целях безопасности рекомендуется учесть некоторые советы и пожелания:

- не в коем случае не передавать незнакомым лицам реквизиты банковских карт. Не сообщать коды и пароли подтверждения банковских операций из СМС сообщений;

- не переводить денежные средства незнакомым лицам на неизвестные банковские счеты. При возникновении любой проблемы с счетом обращаться в отделение банка;

- не размещать на общее обозрение, в том числе в социальных сетях, свои персональные данные (паспортные данные, реквизиты банковских карт);

- не спешить переводить деньги знакомым и родственникам на их просьбы в социальных сетях;

Помощник прокурора района

юрист 3 класса Н.К. Комаева