Рекомендации для пресечения и противодействия преступным намерениям

Распространённость преступлений в сфере информационно-телекоммуникационных технологий (ИТТ) настоящее время крайне высока. Злоумышленники звонят и представляются сотрудниками служб безопасности банков, после чего дезинформируют о том, что с карты осуществляются попытки несанкционированного списания денежных средств.

Также распространены такие виды мошенничества с использованием сети Интернет, как:

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

- покупка или продажа товара на Интернет-площадках с использованием «сайтов-двойников», 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 целях пресечения и противодействия преступных намерений и действий мошенников, доводим от СУ УМВД России по г. Кирову следующие рекомендации:

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 Онлайн». 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.

14. При наступлении вышеописанных событий незамедлительно обратиться в банк по телефону горячей линии и заблокировать счет. Разблокировать его со сменой пароля можно при личном обращении в отделение банка с паспортом и картой.

15. В случае совершения противоправных действий незамедлительно обратиться в полицию по телефонам «02», с мобильного телефона - 102.