ПРОКУРАТУРА ТРОСНЯНСКОГО РАЙОН РАЗЪЯСНЯЕТ!

**Профилактика дистанционного мошенничества**

Распространение в последние несколько лет использования преступниками средств сотовой связи, компьютерных программ и сети Интернет, социальных сетей для совершения хищений получило в практике и научном сообществе наименование «дистанционное мошенничество».

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;

-рассылка вирусных ссылок в социальных сетях, предоставляющих доступ к личным данным потерпевших.

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

**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 Онлайн». Если Вам предлагается ввести пароль для отмены или подтверждения операций, который Вы не совершали, то прекратите сеанс использования услуги и срочно обратитесь в банк.

3.Никому не сообщайте коды банковской карты и одноразовые пароли.

4. Все действия с банковской картой должны происходить в присутствии держателя карты (в кафе, ресторанах, торговых точках). 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, что поможет сохранить денежные средства.

6. Подключите услугу СМС-информирование – это обеспечит контроль за проведением любых операций по карте.

7. Установите лимит выдачи денежных средств за сутки и за одну операцию.

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

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

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.

**ВНИМАНИЕ:**

Основной признак «зеркального» сайта банка – после ввода логина и пароля на странице появляется надпись о техническом обслуживании сайта или любая информация, в которой будет указано о том, чтобы обратиться на сайт позднее. При этом на телефон поступает СМС-сообщение от банка о входе в личный кабинет, если такая форма оповещения предусмотрена.

При наступлении вышеуказанных событий незамедлительно обратитесь в банк по телефону горячей линии и заблокируйте счет. Разблокировать счет со сменой пароля можно при личном обращении в отделение банка с паспортом и картой.