Как защитить себя от кибермошенничества

(районный материал)

Схема большинства преступлений проста: мошенники звонят жертве в любом из мессенджеров, как правило это «Viber», на домашний телефон, либо с абонентских номеров иностранных государств, маскируются под сотрудников банков, правоохранительных органов и сообщают о проблемах с банковским счетом, в случае звонка на домашний телефон могут представиться работником абонентского отдела провайдера услуг интернет связи. В случае со звонком на мобильный телефон вас не должно сбивать с толку, если номер абонента подписан как «BELARUSBANK», «МВД» и т.д. Для решения проблем предлагают сообщить личные данные (номер карты, идентификационный номер паспорта и прочее), после чего с помощью этих данных и выводят средства со счета жертвы. Как правило, человека торопят, призывают принять решение здесь и сейчас, просят никому об этом не сообщать из-за чего он теряется и предоставляет информацию. Но стоит помнить, что сотрудники банков никогда не звонят клиентам в мессенджерах. Нередки случаи, когда злоумышленники сообщают о проведении служебного расследования по факту хищения денежных средств клиентов неустановленным сотрудником банка и просят не звонить в банк, мотивируя это тем, что звонок может помешать расследованию, и предупреждают о наличии уголовной ответственности за препятствование расследованию (при этом могут ссылаться на произвольный номер статьи Уголовного кодекса Республики Беларусь).

Мошенник может представиться:

- Сотрудником банка;
- Сотрудником правоохранительных органов;
- Родственником или другом из социальных сетей;
- Сотрудником поставщика услуг.

Назвать причину:

- Вам одобрен кредит;
- По вашему счету обнаружены мошеннические операции;
- Подтверждение на оформление доверенности на операции по вкладу;
- Продление договора на поставку интернет-услуг.

Мошенник может попросить:

- Назвать номер, срок действия и трехзначный код на обороте карты, коды из смс-сообщений;
- Установить программу или мобильное приложение для отмены операции по счету или защиты своего счета от мошенников;

- Войти в ваш интернет-банкинг и проверить не изменился ли баланс счета;
- Назвать или напечатать цифры из смс-сообщения;
- Помочь разоблачить недобросовестного сотрудника банка;
- Оформить кредит в банке;
- Перевести деньги на «защищенный» счет;
- Сообщить паспортные данные.

Что делать в вышеуказанных ситуациях:

- НЕ СООБЩАЙТЕ ДАННЫЕ КАРТЫ И КОДЫ ИЗ СМС;
- НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММЫ ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ;
- НЕ ОФОРМЛЯЙТЕ КРЕДИТЫ;
- НЕ ПЕРЕВОДИТЕ ДЕНЬГИ НА «ЗАЩИЩЕННЫЙ» СЧЕТ;
- НЕ СООБЩАЙТЕ ПАСПОРТНЫЕ ДАННЫЕ.

Доведите указанную информацию до своих родных, близких, друзей и знакомых, в особенности пожилых граждан, чтобы они могли избежать аналогичных случаев хищения денежных средств с их банковских карт и не стали жертвами мошенников.

Информация подготовлена
отделом идеологической работы
и по делам молодежи
Речицкого райисполкома