Директору Татышлинского информационного центра – филиала

ГУП РБ «Издательский дом «Республика Башкортостан»

Файзрахманову Р.Х.

Редактору редакции газеты «Ошмес»

 .03.2022 3-1-2022 Нигаматуллиной О.Б.

Уважаемые руководители

средств массовой информации!

 Прошу опубликовать в периодических изданиях и разместить на сайтах возглавляемых Вами средств массовой информации статью на тему: «Прокуратурой района постановлено на контроль расследование уголовного дела в отношении аферистки, похитившей более 90 тысяч рублей за снятие порчи. Учитывая стабильно высокий уровень преступлений анализируемой категории, прокурор разъясняет основные правила поведения, позволяющие сельчанам уберечься от дистанционных мошенников».

 Прокуратурой Татышлинского района признано законным решение о возбуждении уголовного дела по заявлению молодой женщины о хищении принадлежащих ей денежных средств путем обмана.

 Установлено, что в ноябре 2021 года в социальной сети «Инстаграм» женщина наткнулась на страницу некой «ясновидящей, гадалки», которая проводила свои обряды в прямом эфире, отвечала на вопросы бесплатно. Желая узнать причины ухудшения отношений в семье, женщина задала «гадалке» вопрос, на что последняя искусно введя женщину в заблуждение сообщила, что на неё наложена черная магия «смертельная порча». В результате под психологическим воздействием девушка перевела на счет указанной «гадалкой» банковской карты 93 900 рублей.

 В настоящее время производятся следственные и оперативно-розыскные мероприятия, направленные на установление лица и обстоятельств совершенного преступления.

Ход и результаты расследования уголовного дела поставлены на контроль прокуратуры.

Проведенный в текущем году прокуратурой района 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.

Уважаемые жители Татышлинского района в целях пресечения и противодействия преступных намерений и действий мошенников прокуратура района информирует о том, что 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 правила, которые позволят уберечься от мошенников:

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;

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

5. Только мошенники могут запрашивать пароли для отмены операций или шаблонов в «Сбербанк Онлайн». Если предлагается ввести пароль для отмены или подтверждения операций, которые не совершали, то прекратите сеанс использования услуги и срочно обратитесь в банк;

6. Никому не сообщать пин, СVC или CVV коды банковской карты и одноразовые пароли;

7. 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;

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

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

10. 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;

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

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

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

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

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

16. 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.

Прокурор района

советник юстиции Ф.Ф. Янгуразов

Ф.Ф. Янгуразов, 8(34778)2-12-65

Главе администрации муниципального района Татышлинский район Республики Башкортостан

Шайхисламову Ф.Р.

Главам сельских поселений муниципального района Татышлинский район Республики Башкортостан

 .03.2022 3-1-2022

Уважаемые руководители

органов местного самоуправления!

Прошу опубликовать в периодических изданиях и разместить на сайтах возглавляемых Вами органов местного самоуправления статью на тему: «Прокуратурой района постановлено на контроль расследование уголовного дела в отношении аферистки, похитившей более 90 тысяч рублей за снятие порчи. Учитывая стабильно высокий уровень преступлений анализируемой категории, прокурор разъясняет основные правила поведения, позволяющие сельчанам уберечься от дистанционных мошенников».

 Прокуратурой Татышлинского района признано законным решение о возбуждении уголовного дела по заявлению молодой женщины о хищении принадлежащих ей денежных средств путем обмана.

 Установлено, что в ноябре 2021 года в социальной сети «Инстаграм» женщина наткнулась на страницу некой «ясновидящей, гадалки», которая проводила свои обряды в прямом эфире, отвечала на вопросы бесплатно. Желая узнать причины ухудшения отношений в семье, женщина задала «гадалке» вопрос, на что последняя искусно введя женщину в заблуждение сообщила, что на неё наложена черная магия «смертельная порча». В результате под психологическим воздействием девушка перевела на счет указанной «гадалкой» банковской карты 93 900 рублей.

 В настоящее время производятся следственные и оперативно-розыскные мероприятия, направленные на установление лица и обстоятельств совершенного преступления.

Ход и результаты расследования уголовного дела поставлены на контроль прокуратуры.

Проведенный в текущем году прокуратурой района 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.

Уважаемые жители Татышлинского района в целях пресечения и противодействия преступных намерений и действий мошенников прокуратура района информирует о том, что 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 правила, которые позволят уберечься от мошенников:

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;

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

5. Только мошенники могут запрашивать пароли для отмены операций или шаблонов в «Сбербанк Онлайн». Если предлагается ввести пароль для отмены или подтверждения операций, которые не совершали, то прекратите сеанс использования услуги и срочно обратитесь в банк;

6. Никому не сообщать пин, СVC или CVV коды банковской карты и одноразовые пароли;

7. 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;

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

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

10. 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;

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

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

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

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

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

16. 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.

Прокурор района

советник юстиции Ф.Ф. Янгуразов

Ф.Ф. Янгуразов, 8(34778)2-12-65