М В Д Р о с с и и

УПРАВЛЕНИЕ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО КУРСКОЙ ОБЛАСТИ
(УМВД России по Курской области)

ул. С. Саровского, д. 2, Курск, 305000

СЭД МВД
№46/1232 от 23.09.2020

Заместителю Губернатора Курской области

А.В. Чуркину

О направлении информации

Уважаемый Александр Владимирович!

Анализ оперативной обстановки в сфере борьбы с мошенническими посягательствами свидетельствует об активном использовании преступниками электронных платежных систем и средств мобильной связи, что значительно снижает для них риск быть привлеченными к уголовной ответственности. В настоящее время лица установлены лишь по каждому пятому противоправному деянию из числа зарегистрированных.

В целях предупреждения краж и мошенничеств, совершаемых с помощью информационно-коммуникационных технологий, прошу Вас организовать в образовательных организациях Курской области профилактические мероприятия по максимальному доведению до преподавательского состава и обслуживающего персонала информации по профилактике преступлений указанной категории.

Кроме того, прошу рекомендовать преподавательской общественности довести данную информацию до родителей учащихся учебных организаций на родительских собраниях с приглашением сотрудников полиции и распространением памяток.

В рамках работы с учащимися школ предлагаем совместно организовать и провести конкурс по указанной тематике «Детские советы взрослым» с целью привлечения широкой целевой аудитории к данной проблеме.

Приложение: Лекционный материал о формах мошенничеств с примерами и разъяснениями по недопущению совершения преступлений данной категории.

С уважением,

Врио начальника

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 016FD79A00F8AB03854B2DC41CF305C42B
Владелец **Маркин Сергей Петрович**
Действителен с 14.07.2020 по 14.10.2021

С.П. Маркин

Отп. в ед. экз. – в дело ООДУУП и ПДН
электронная копия
2 – в Администрацию Курской области
исп. Е.А. Мухин
8 (4712) 36 66 23

Лекционный материал
о формах мошенничеств с примерами и разъяснениями по недопущению совершения преступлений данной категории.

Все большую роль в жизни современного человека играют информационные технологии: Интернет, смартфоны, банковские карты. Они призваны облегчить жизнь граждан, однако мошенники взяли эти удобства на вооружение. Несмотря на систематические предупреждения жителей области о способах мошенничества с использованием сети Интернет и сотовой связи, граждане попадаются на уловки аферистов и переводят им денежные средства.

1. СМС или звонок «Ваша карта заблокирована...», а также другие мошенничества с банковскими картами (происходит списание по карте и т.д.).

59-летней женщине поступил звонок от незнакомца, который представился сотрудником банка. Он сообщил женщине, что с ее банковского счета происходит несанкционированное списание денежных средств, а чтобы приостановить данную операцию, ему необходимо сообщить все данные банковской карты и код из смс-сообщения, которое поступит на ее телефон. Пенсионерка выполнила условия мошенника и лишилась 63 тысяч рублей.

Меры противодействия: помните главное: банки никогда не звонят своим клиентам с просьбой представиться, назвать номер карты и CUV-код. Все возникшие неисправности банк устраняет самостоятельно, не привлекая клиентов. Не вступайте в беседы с незнакомцами, которые представляются работниками службы безопасности банка, не выполняйте их поручения, полученные по телефону. В случае возникновения вопросов необходимо обратиться в ближайшее отделение банка, либо позвонить по телефону «горячей линии», который указан на оборотной стороне каждой банковской карты.

Ни в коем случае не сообщайте КОДЫ и ПАРОЛИ подтверждения операции, приходящие в смс-сообщениях

2. Мошенничества на «Авито» и других сайтах бесплатных объявлений

Полиция призывает граждан к бдительности при общении через Интернет с незнакомыми людьми. Невнимательность и полное доверие к чужим людям позволяют аферистам обманывать граждан, принуждая их к передаче денежных средств либо сведений, позволяющих похитить сбережения с электронного счета.

31-летний гражданин в сети Интернет нашел объявление о продаже сидений для автомобиля и решил купить их. Для совершения сделки мужчина перечислил незнакомцу 6 тысяч рублей и ожидал доставки товара через транспортную компанию. Однако этого не произошло, а лжепродавец удалил объявление с сайта и не выходил больше на связь.

34-летняя потерпевшая нашла на сайте объявление о продаже автомобильных дисков и перевела продавцу 20 тысяч рублей. Однако в назначенное время свою посылку она не получила. При этом, телефон продавца перестал отвечать, а объявление было удалено.

Выставив объявление на Авито о продаже земельного участка, денежных средств лишилась 69-летняя женщина. По объявлению позвонил неизвестный и сообщил, что готов внести задаток за продаваемый объект. Для этого ему нужно было продиктовать номер банковской пластиковой карты и код, пришедший в смс-сообщении. Пенсионерка выполнила его условия. Через некоторое время злоумышленник сообщил женщине, что перевел ей на 49,5 тысяч рублей больше и попросил вернуть их. Потерпевшая зачислила их на несколько абонентских номеров.Как выяснилось, получив доступ к мобильному банку пенсионерки, он увидел, что на ее счету в банке лежат 49,5 тысяч рублей. А женщина, будучи обманутой, сняла свои деньги и перевела их мошеннику.

37-летняя гражданка лишилась 30 тысяч рублей в надежде сдать квартиру в аренду. Она разместила на «Авито» объявление и ждала звонков. К ней позвонил неизвестный и выразил желание арендовать квартиру на 2,5 года. При этом, мужчина готов был внести предоплату, чтобы арендодательница сняла объявление с сайта. Женщина согласилась и продиктовала незнакомцу всю запрашиваемую им информацию: номер карты, трехзначный код с оборотной стороны, кроме того, она назвала пин-коды из смс-сообщений, которые поступили на ее телефон.Когда со счета потерпевшей стали списываться денежные средства, она поняла, что ее обманули. Ущерб от действий злоумышленника составил 30 тысяч рублей.

35-летний мужчина лишился 14 тысяч рублей, продавая диван через Интернет .Лже-покупатель предложил внести предоплату на карту собственнику имущества. Мужчина согласился, и по указанию аферист прошел к банкомату, на котором под диктовку выполнил ряд некоторыхопераций. После этого со всех счетов потерпевшего были списаны сбережения.

<u>3. Под предлогом оказания помощи в получении кредита</u>

В полицию поступают заявления от граждан о потере денег после общения с аферистами, выдающими себя за сотрудников банков.

Так, 29-летняя гражданка обратилась в полицию с заявлением о том, что мошенники похитили у нее крупную сумму денег. Позже выяснилось, что

женщина на разных интернет-сайтах оставляла заявки о выдаче кредита. Через некоторое время ей позвонил неизвестный, который представился сотрудником банка и сообщил, что запрошенный ею кредит одобрен. Для его получения необходимо оплатить 5 тысяч рублей. Потерпевшая перевела требуемую сумму. Далее лжеконсультант неоднократно просил деньги на оплату страховки и различные услуги. В результате ничего не подозревавшая женщина перевела незнакомцу порядка 77 тыс. рублей.

Еще одной жертвой мошенников стала 63-летняя гражданка. Она рассказала полицейским, что к ее подруге поступил телефонный звонок от якобы специалиста банка, который сообщил, что ей одобрена сумма кредита в 500 тысяч рублей и деньги будут привезены к ней домой сразу после оплаты страховки и возмещения затрат за работу специалистов. Женщина, желая получить займ, позвонила подруге и попросила в долг необходимую сумму денежных средств. Женщина, долго не раздумывая, перевела деньги незнакомцу. Получив желаемое, лжебанкир отключил мобильный телефон. Таким образом, ущерб составил 82 тысячи рублей.

4. Признаки мошенничества со стороны продавца при покупках в Интернете:

1. Отсутствует адрес и телефон, все общение предлагается вести через электронную почту или программы обмена мгновенными сообщениями.
2. Отсутствует реальное имя продавца, человек прячется за «ником».
3. Продавец зарегистрирован на сервисе недавно, объявление о продаже - единственное его сообщение.
4. Объявление опубликовано с ошибками, составлено небрежно, с использованием транслитерации, без знаков препинания, заглавными буквами и т.д.
5. Отсутствует фото товара либо приложен снимок из Интернета (это можно определить, используя сервисы поиска дубликатов картинок).
6. Слишком низкая цена товара в сравнении с аналогами у других продавцов.
7. Продавец требует полную или частичную предоплату (например, в качестве гарантии, что вы пойдете получать товар на почте с оплатой наложенным платежом).
8. Продавец принимает оплату только на анонимные реквизиты: электронные кошельки, пополнение мобильного телефона или на имя другого человека (родственника, друга и т.д.).

5. Признаки мошенничества со стороны покупателя при продажах в Интернете:

1. Покупатель не особо интересуется товаром, быстро демонстрирует свое желание сделать покупку и переходит к разговору о способе оплаты.

2. Покупатель просит вас назвать полные реквизиты карты, включая фамилию-имя латиницей, срок действия и cvc-код. При помощи этих данных он сам легко сможет расплатиться вашей картой в Интернете.
3. Покупатель просит вас сообщить ему различные коды, которые придут к вам на мобильный телефон, якобы необходимые ему для совершения платежа.
Так, жертвой интернет-мошенников стала 54-летняя гражданка, которая разместила на **интернет-сайте «Авито»**объявление о продаже мягкой мебели. Ей позвонил мужчина и выразил готовность купить товар, переведя деньги на ее банковскую карту. Женщина направилась к банкомату и под диктовку мошенника ввела требуемую комбинацию цифр, после чего с ее банковской карты были списаны денежные средства в размере более 47 тыс. рублей.

Как не стать жертвой Интернет-мошенничества:

- следует внимательно изучить информацию Интернет-сайта, отзывы, сравнить цены за интересующий товар. Отсутствие информации, запутанная система получения товара зачастую является признаками мошенничества.
- получить максимум сведений о продавце или магазине, адреса, телефоны, историю в социальных сетях, наличие службы доставки и т.п. Действующие легально Интернет-магазины или розничные продавцы размещают полную информацию и работают по принципу «оплата товара после доставки»;
- нельзя сообщать (а уж тем более посылать по электронной почте) информацию о своих пластиковых картах. Преступники могут воспользоваться их реквизитами и произвести, например, различные покупки.

Ни в коем случае не сообщайте коды и пароли подтверждения операции приходящие в смс-сообщениях

Меры противодействия: помните, что предоплату за товар вы вносите на свой страх и риск, 100%-ой гарантии получения товара не существует. При заказе товаров внимательно проверяете название сайта в адресной строке браузера, чтобы не попасть на сайт-двойник. Пользуйтесь услугами Интернет-магазинов, работающих длительное время и заслуживших положительную репутацию покупателей, читайте отзывы покупателей о работе данных Интернет-магазинов.

Ни при каких обстоятельствах, как бы вас не уговаривал продавец (покупатель), не сообщайте номер вашей банковской карты вместе с CUV-кодом (указан на оборотной стороне банковской карты).

6. Денежные компенсации за ранее приобретенные БАДы, медицинские приборы, оказание «не качественных услуг», возврат потерянных денег на различных фондовых биржах и т.д.:

Полиция напоминает**:** компенсация за биологически активные добавки, приборы медицинского назначения – одна из самых распространенных схем обмана граждан.

Так, 55-летний лишился 301 тысячи рублей в надежде получить компенсацию за некачественные БАДы. К нему на сотовый телефон позвонила женщина, которая представилась работником прокуратуры. Она сообщила, что в отношении организации, в которой мужчина несколько лет назад приобретал БАДы, проводится проверка и ему полагается компенсация в размере 580 тысяч рублей. Для ее получения, необходимо выполнить несколько условий: внести комиссию в размере 6% от суммы компенсации и оплатить услуги инкассаторов, чтобы доставить к нему денежные средства. Мошенница уверяла: все оплаченные расходы вернутся вместе с компенсацией. Мужчина, не раздумывая, согласился. В несколько приемов он перевел аферистам 301 тысячу рублей.

По аналогичной схеме злоумышленники похитили у 34-летней гражданки 432 тысячи рублей. Эту сумму безработная домохозяйка заняла у родных, чтобы оформить документы на возмещение морального ущерба, нанесенного ей продавцами бесполезных пилюль для снижения веса. Жулики внушили наивной даме, что недобросовестные торговцы вернут ей по суду… семь миллионов рублей.

63-летняя гражданка, тоже желая получить компенсацию за некачественные лекарства, лишилась 309 тысяч рублей. Она раньше неоднократно заказывала дорогостоящие лекарственные препараты в одном из Московских медико-консультационных центров, о котором потерпевшая узнала по объявлению на радио. Пропив препараты, она ни какого эффекта не заметила и лучше себя чувствовать не стала. Через некоторое время на телефон женщины поступил звонок от незнакомца, который представился старшим следователем следственного управления г. Москвы. Лже-сотрудник пояснил, что научно-исследовательский институт, в котором она заказывала лекарства, совершал мошеннические действия в отношении граждан, в связи с чем ей полагается компенсация в размере 450 тысяч рублей. Также аферист сообщил пенсионерке, что для получения компенсационных выплат, необходимо оплатить страховку в размере 95 тысяч рублей. Женщина, желая получить столь крупную для нее сумму денег, согласилась с предложением незнакомца и перевела на указанный им счет деньги. Однако компенсацию в размере 450 тысяч рублей она так и не получила.Примечательно, что потерпевшая для приобретения лекарств и оплаты страхового взноса оформила кредит в банке.

7. Сын/родственник попал в полицию

Это самый «древний», но продолжающий успешно работать на преступников способ. Чаще всего жертвами таких преступлений становятся пожилые граждане. Злоумышленники пользуются доверчивостью пенсионеров, которые готовы отдать все сбережения за спасение сына или внука.

Полицейские рекомендуют гражданам регулярно проводить со своими пожилыми родственниками профилактические беседы и объяснить им, как действовать в подобных ситуациях.

Злоумышленники действуют по следующей схеме: раздается звонок, Вы берете трубку, неизвестный взволнованным голосом сообщает, что ваш родственник попал в ДТП, сбил человека и ему срочно нужны деньги, что бы избежать уголовной ответственности. Деньги просят перевести на счет абонентского номера или на счет банковской карты. В некоторых случаях за деньгами отправляют на адрес потерпевшего курьера или водителя такси.

Таким образом были обмануты граждане. Они перевели мошенникам по 30 тысяч рублей.

Меры противодействия: Не вступайте в беседы с незнакомцами, которые звонят (отправляют сообщения) с неизвестных вам номеров, представляются вашими знакомыми, родственниками, сотрудниками правоохранительных органов, и просят перечислить денежные средства. Ни что не мешает вам прервать разговор и перезвонить своим знакомым, родственникам, уточнив, действительно ли с ним случились неприятности. В случае продолжения беседы, попросите звонившего представиться и уточните куда возможно доставили родственника. В дальнейшем через «Интернет» найдите телефон дежурной части отдела и перезвоните. Особенно на эту уловку попадаются люди престарелого возраста

8. Заражение вирусами сотовых телефонов, работающих на операционных системах «Андроид» с подключенной услугой «мобильный банк»

Данному виду преступлений в основном подвергнуты клиенты ОАО «Сбербанк России», так как банком при открытии счета гражданам услуга «мобильный банк» подключается автоматически, а для ее отключения необходимо написать заявление, о чем не всегда предупреждают клиентов.

В настоящее время можно выделить три основных способа, при помощи которых совершаются хищения денежных средств, но сразу следует пояснить, что данный перечень не исчерпывающий, так как возможны абсолютно иные способы хищений денежных средств, а также измененные или скомбинированные из различных способов.

Способ «Двойной «Мобильный банк».

Потерпевшим при заключении договора указывается абонентский номер, который и подключается к «мобильному банку». По различным причинам, многие владельцы пластиковых карт банков перестают в дальнейшем пользоваться абонентскими номерами (потерял, переехал, сменил оператора и т.д.), в связи, с чем оператор сотовой связи через 6 месяцев перевыпускает СИМ-карту с данным абонентским номером и выставляет ее на продажу. Также возможна утеря СИМ-карты и неотключение ее «мобильного банка».

Новый абонент приобретая данную СИМ-карту начинает получать СМС о движении денежных средств по счёту потерпевшего, кроме того он получает возможность управлять денежными средствами лицевого счета, к которому она подключена.

Меры противодействия: в случае утраты сим-карты, либо ее неиспользовании более полугода отключить услугу «мобильный банк»

Способ «Вредоносные программы». Способы заражения вредоносным программным обеспечением (ВПО) телефонных аппаратов на операционной системе «Android».

1. Потерпевший получает СМС-сообщение от контент-провайдера, в котором находится ссылка на информационный ресурс, перейдя по которой, абонент закачивает на телефон вредоносное программное обеспечение (далее ВПО).

2. Потерпевший получает СМС-сообщение от своего «знакомого», телефон которого уже заражен ВПО, при этом ВПО само направляет данное сообщение на номера, которые имеются в адресной книге потерпевшего. В данном сообщении также находится ссылка на информационный ресурс, перейдя по которой абонент закачивает на телефон ВПО.

3. Потерпевший, находясь в сети «Интернет», с помощью телефона, получает по электронной почте, либо через социальные сети, ICQ сообщение, в котором находится ссылка на информационный ресурс, перейдя по которой абонент закачивает на телефон ВПО.

4. Потерпевший, находясь в сети «Интернет», с помощью телефона, скачивает, например, программныепродукты, музыку, фотографии, в которых находится ссылка на информационный ресурс, перейдя по которой абонент закачивает на телефон ВПО.

Поле заражения телефона «вирус» проверяет наличие подключенной услуги «Мобильный банк». Если услуга подключена, то вирус с помощью нее осуществляет перевод денежных средств с банковской карты протерпевшего на различные абонентские телефонные номера, электронные платежные системы (Киви-кошелек и др.), либо на лицевой счет абонентского телефонного номера потерпевшего и далее на электронные платежные системы, либо банковские карты преступника. При этом вирус блокирует (не выводит на дисплей телефона, а также

удаляет их из телефона потерпевшего) информационные СМС-сообщения о произведенных транзакциях, которые поступают от Банка.

Меры противодействия: гражданам, имеющим телефоны, работающие на операционной системе «Андроид», в случае получения СМС, ММС и др. сообщений (в т.ч. от своих «знакомых»), содержащих ссылки на незнакомые ресурсы ни в коем случае не переходить по ним, не скачивать программные продукты с сомнительных сайтов.
Пользуйтесь лицензированной антивирусной программой и периодически обновляйте ее.

9. Займ денежных средств в социальных сетях
38-летней женщине в социальной сети «Одноклассники» написала подруга, которая попросила о помощи. Женщина спросила ее, что случилось, а та в ответ попросила взаймы 14 тысяч рублей. Женщина, не раздумывая, перевела деньги на счет банковской карты, который указал злоумышленник. После этого подруга вновь попросила деньги, однако у потерпевшей не оказалось запрашиваемой суммы и она решила позвонить ей. Выяснилось, что страницу подруги в социальной сети взломали, а потерпевшая перечислила денежные средства мошенникам.
Меры противодействия: запомните главное правило – в первую очередь связаться с родственниками, знакомыми от чьего имени у Вас просят денежные средства!

10. Выигрыш приза в размере N суммы рублей или иного имущества
23-летней девушке на одном из интернет-сайтов поступило сообщение о том, что она выиграла в конкурсе сотовый телефон. В ходе переписки девушке сообщили, что для его получения необходимо оплатить доставку товара. Девушка, не подозревая обмана и желая получить приз, решила заплатить запрашиваемую сумму. Но на этом злоумышленник не остановился и под предлогом оплаты страховки, налога, выманил у потерпевшей еще деньги. В результате она лишилась 122 тысяч рублей.
Меры противодействия: запомните главное правило – «халявы» не бывает! Не задумываясь удаляйте из телефона полученные сообщения о выигрыше BMW, Mercedes, Apple, IPhone и т.д.! Не будьте жадными!

11. Под видом работников газовых и социальных служб
Злоумышленницы похитили у 75-летней гражданки золотые украшения. К ней в квартиру постучались три незнакомки, которые представились сотрудниками газовой службы. Пенсионерка впустила их к себе домой.

Две женщины прошли с хозяйкой на кухню для осмотра газовой плиты, а третья осталась в комнате. После их ухода бабушка обнаружила пропажу из шкатулки золотых колец на общую сумму 14 тысяч рублей.

Меры противодействия: не впускайте в жилище посторонних, требуйте представить документы, подтверждающие принадлежность к той или иной организации. Не поленитесь позвонить в данную организацию и уточнить, работает, ли там сотрудник и действительно ли вам положены какие-либо выплаты, для этого рекомендуется заранее записать телефоны управляющих компаний, учреждений социальной защиты, пенсионного фонда, здравоохранения, коммунальных служб и т.д., а не звонить по телефонам которые Вам диктуют прибывшие «представители» той или иной организации, учреждения.

12. Денежные реформы, компенсационные выплаты:

Жертвами преступлений в основном являются пенсионеры, которым приходят или звонят злоумышленники и под предлогом проведения денежной реформы, различных выплат, предлагают обменять денежные средства или просят сообщить реквизиты банковской карты, с которой в последующем снимают денежные средства.

68-летняя пенсионерка по собственной невнимательности обогатила аферистов на 74 тысячи рублей. Днем к пенсионерке в квартиру пришла незнакомка и сообщила, что в связи с денежной реформой производит обмен старых денег на купюры нового образца. Доверчивая женщина достала все свои сбережения и передала аферистке, а взамен получила игрушечные деньги. Только после ухода мошенницы бабушка поняла, что ее обманули.

Меры противодействия: Реформа денежных знаков давно проведена. Не впускайте в жилище посторонних, сообщите об их визите родственникам, соседям или в полицию.

Никаких замен денежных купюр на якобы новые не государственные или иные организации НЕ ПРОВОДИТ (тем более на дому)

Меры противодействия: Никому не сообщайте сведения о держателе банковской карты, ее реквизиты, CUV-код и КОДЫ и ПАРОЛИ подтверждения операций, приходящие в СМС-сообщениях

В 80% случаев денежные средства переводятся на счета банковских карт злоумышленников, 30% составляют платежи на счета абонентских номеров с дальнейшей их легализацией путем перевода на банковские карты с использованием систем электронных переводов, таких как КИВИ, ЯНДЕКС, МОБИДЕНЬГИ, НСК.

Одним из важных факторов в противодействии мошенничествам является адекватность действий граждан (либо наоборот отказ от необдуманных шагов), реакция и самообладание при тех или иных обстоятельствах.

Престарелые граждане не всегда могут правильно оценить обстановку, поэтому УМВД по Курской области обращается к их детям и внукам – как можно чаще предупреждайте своих родителей о возможной опасности.

Если в отношении граждан все же было совершено мошенничество, следует незамедлительно обратиться в полицию, сообщив обстоятельства произошедшего и предоставив имеющиеся документы (расчетные чеки, распечатки звонков и т.п.).