УМВД России по Смоленской области
УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ГОРОДУ СМОЛЕНСКУ
(УМВД России по г. Смоленску)

ул. Попова, д. 20-в, Смоленск, 214020

Директорам средних школ Заднепровского района г. Смоленска МБОУ «СШ № 3», МБОУ «СШ № 5», МБОУ «СШ № 7», МБОУ «СШ № 10», МБОУ «СШ № 13», МБОУ «СШ № 15», МБОУ «СШ № 18», МБОУ «СШ № 19, МБОУ «СШ № 22», МБОУ «СШ № 23», МБОУ «СШ № 24», МБОУ «СШ № 32», МБОУ «СШ № 36», МБОУ «СШ № 40», МБОУ «СШ № 30», директорам СФФК, санаторно-лесная школа, МБОУ «О(с)Ш № 1»

27.03.23 № 2923

на № _____ от _____

Информирую Вас, что в современных условиях одним из наиболее распространенных видов преступлений (а также наиболее трудно раскрываемых) являются различные формы мошеннических действий, в том числе совершаемые с использованием информационно-телекоммуникационных технологий, и так называемые «социальные» мошенничества.

Самыми распространенными схемами аферистов являются:

«Разблокировка!»

Одной из самых распространенных мошеннических схем является смс-переписка или телефонные переговоры злоумышленников с пострадавшим от имени сотрудников банка. Обманным путем мошенники узнают код авторизации для входа в личный кабинет мобильного приложения банка. Затем со своего мобильного телефона заходят в приложение и переводят деньги.

Что делать?

Официальный представитель банка позвонит клиенту или отправит сообщение со специального номера, зарегистрированного на финансовую организацию. К примеру, у Сбербанка это трехзначный номер 900. Этот номер должен быть знаком клиенту, потому что с него он обычно получает смс-информирование о движении денежных средств на счете. Злоумышленники не смогут отправить смс с этого номера. В любом случае, даже если звонит официальный представитель банка, ему нельзя

сообщать пин-код, трехзначный CVV-код на обратной стороне карты, код авторизации, присланный по смс, логин и пароль от личного кабинета в интернет-банке. Такую информацию могут запрашивать только мошенники. Помните, что ни один банк самостоятельно не блокирует карту - сделать это можете только вы. Сотрудники банка никогда не запрашивают пароли и коды смс-подтверждений по телефону - никогда никому их не сообщайте! Внимательно относитесь к смс и e-mail-сообщениям от имени банка, в которых содержится информация о блокировке вашей карты, никогда не перезванивайте по номерам, указанным в этих сообщениях! Никогда не переходите на сайт банка онлайн по ссылкам с незнакомых сайтов и социальных сетей. При покупках в интернете пользуйтесь проверенными сервисами оплаты.

«Близкие в беде!»

Мошенники путем перебора номеров звонят и сообщают, что «ваш родственник попал в ДТП или в полицию» и просят денег для откупа. Далее в разговор вступает другой мошенник, который представляется сотрудником полиции и уверенно сообщает, что уже не раз помогал людям таким образом. Деньги необходимо привезти в определенное место и передать конкретному человеку либо за ними приедет их знакомый человек.

Что делать?

Не паникуйте и не торопитесь собирать деньги. Скажите, что не имеете в наличии денег. Прервите разговор и попытайтесь связаться с тем родственником, который якобы попал в беду. Задайте вопросы личного характера. Хотя бы, как зовут ваших родственников и их близких. Не впускайте в свой дом незнакомца, даже если он представился сотрудником социальной службы или государственной структуры. Попросите его предъявить удостоверение. Не стесняйтесь тут же, не пуская посетителя в дом, проверить данные по телефону.

«Распродажа!»

Вам звонят в дверь, очень словоохотливые люди представляются сетевыми агентами каких-то фирм и предлагают товар в два раза дешевле. Остерегайтесь их, так как товар может быть ворованным или некачественным. Сигнал опасности: ощущение, что вам неожиданно и несказанно повезло.

Что делать?

Будьте скептиком, не верьте объяснениям «выставочная партия», «все распродаем и заканчиваем торговлю» и т.д. Даже если уверены, что имущество не краденое, задумайтесь о возможных последствиях и откажитесь от покупки. Помните, что вы рискуете стать фигурантом уголовного дела за приобретение предметов, заведомо добытых преступным путем, а также лишиться и денег, и товара.

«Купля-продажа и услуги по объявлению!»

25-летняя девушка разместила объявление о продаже журнального столика на одном из интернет-сайтов. Через некоторое время к ней

позвонил покупатель, и стороны договорились, что оплата будет осуществляться путем перевода на банковскую карту продавца. Девушка направила номер банковской карты покупателю и стала ждать. А дальше произошло снятие 1000 рублей с ее счета, затем 2000 рублей, а далее карта была заблокирована - злоумышленники запросили превышающую лимит карты сумму, что привело к ее блокированию. Таким образом, оставшаяся сумма на карте была спасена.

Что делать?

Никому не сообщайте персональные и конфиденциальные данные, банковские реквизиты, ПИН, защитные (CVV/CVV2) коды. Обязательно установите на банковской карте дневной лимит снятия наличных денег, чтобы злоумышленники не могли снять все денежные средства с вашего счета. Зачастую все виды мошенничества связаны с невнимательностью или неосведомленностью граждан, излишней доверчивостью и самоуверенностью, поэтому будьте предельно бдительны!

«Вирус съест деньг!»

Хакеры заражают смартфон вирусной программой, которая получает доступ к персональным данным владельца. Нередко она проникает на мобильное устройство вместе с каким-нибудь бесплатным приложением или через смс. Если на телефоне установлен мобильный банк, вирус может с помощью команд смс-банкинга сделать перевод средств с карты. При этом владелец даже не заподозрит неладное, так как все произойдет для него незаметно. Вредоносная программа сама совершит перевод и сама же подтвердит от имени потерпевшего операцию.

Что делать?

В целях безопасности владельцам смартфонов, «привязавших» банковскую карту к телефону либо установивших мобильное приложение интернет-банка, рекомендуется пользоваться антивирусом, скачивать приложения только из официальных магазинов, не переходить по ссылкам из смс.

В основном предметом преступных посягательств являются денежные средства.

Незащищенной от мошеннических действий злоумышленников категорией граждан являются лица пожилого возраста.

Основными способами воздействия мошенников на пожилых людей являются психологическое давление и манипуляции. Многие пожилые люди, пострадавшие от мошеннических действий, знают о том, что такие виды обмана существуют, и все равно попадаются на уловки преступников. Пожилые люди очень доверчивы и быстро забывают о предупреждениях.

Главным методом борьбы и профилактики подобных преступлений является информирование населения, особенно старшего поколения, о наиболее распространенных схемах мошенничества.

В целях предупреждения совершения социальных мошенничеств, в том числе совершаемых дистанционным способом, а также в целях

информирования граждан о способах совершения преступлений и мерах, способствующих их предотвращению, **прошу Вас довести информацию об основных видах мошенничества до преподавательского состава, а также родителей обучающихся по возможности.**

Также прошу Вас, разместить прилагаемую памятку «Осторожно мошенники» на информационных стендах организации и разослать при помощи мессенжеров.

О проделанной работе направить ответ (с указанием количества проинформированных граждан) на адрес электронной почты sgavriuseva@mvd.ru в кратчайший срок.

Приложение на 1 листе – информационная памятка «Осторожно мошенники».

Зам начальника отдела полиции № 2 С.М. Ивашкин

УМВД России по Смоленской области предупреждает

Не дайте мошенникам шанса!

«Сотрудники службы безопасности банков не звонят своим клиентам»

- Номера: +7(495)...,8(800)...работают только на входящие звонки;
- Не сообщайте персональные данные, реквизиты своей банковской карты;
- Прервите разговор и перезвоните по официальному номеру банка

«Купля-продажа через Интернет»

- Продавец просит у Вас предоплату за товар, не переводите денежные средства, не убедившись в наличии данного товара

«Компенсация»

- Неизвестный сообщает, что может вернуть денежные средства, которые ранее были похищены, не сообщайте полные реквизиты своей банковской карты

«Родственник в беде»

- Неизвестный сообщает, что Ваш родственник стал виновником ДТП или совершил преступление, не переводите денежные средства для «решения» проблемы

02 Незамедлительно обращайтесь в полицию! **102**

ВНИМАНИЕ!

УЧАСТИЛИСЬ СЛУЧАИ МОШЕННИЧЕСТВА!

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

- сотрудником Банка;
- сотрудником службы безопасности Банка;
- сотрудником полиции, ФСБ, прокуратуры;
- сотрудником больницы;
- сотрудником благотворительной организации;
- покупателем либо продавцом;

И НАЗВАТЬ ПРИЧИНУ ЗВОНКА:

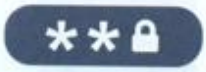
- ваша карта заблокирована;
- с вашей карты (счета) происходит несанкционированное списание денежных средств;
- на вас оформлен кредит или на ваше имя взят займ;
- вам положена отсрочка по кредиту или пособие;
- просят внести предоплату за товар или услугу.

ОН МОЖЕТ ПОПРОСИТЬ:

Перевести деньги:

- на специальный счет или карту, где они будут в безопасности.

Пароль:



- от интернет-банка;
- из SMS-сообщения *(для входа в интернет-банк или подтверждения операции).*

Данные карты:

- номер карты;
- CVV/CVC-код;
- PIN-код;
- срок действия карты.

НЕ

- НЕ ВЫПОЛНЯТЬ УКАЗАНИЯ ВЫМЫШЛЕННЫХ СОТРУДНИКОВ БАНКА, ПОЛИЦИИ, ФСБ, ПРОКУРАТУРЫ!
- НЕ ПЕРЕВОДИТЬ ДЕНЕЖНЫЕ СРЕДСТВА НА НЕСУЩЕСТВУЮЩИЕ БЕЗОПАСНЫЕ СЧЕТА!
- НЕ СООБЩАТЬ НИКОМУ ДАННЫЕ БАНКОВСКОЙ КАРТЫ!

УМВД РОССИИ ПО СМОЛЕНСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ

БУДЬТЕ БДИТЕЛЬНЫ!