МВД России

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО РОСТОВСКОЙ ОБЛАСТИ
(ГУ МВД России по Ростовской области)

ул. Большая Садовая, 29, Ростов-на-Дону, 344082

Министру труда и
социального развития
Ростовской области

Е.В. Елисеевой

344010, г. Ростов-на-Дону,
ул. Лермонтовская, 161.

02.06.21 № 11/2878

на № _____ от _____

О направлении информации

Уважаемая Елена Владимировна !

В связи с участившимися случаями совершения преступных посягательств на имущество граждан, с использованием информационно-телекоммуникационных технологий, направляю Вам основные способы совершения преступлений данной категории для проведения просветительской работы среди граждан, находящихся на социальном обслуживании и в «группе риска».

Приложение на 5 листах.

Заместитель начальника полиции
по оперативной работе В.Г. Серебрянников

Министерство труда и социального развития Ростовской области
344010, г. Ростов-на-Дону, Лермонтовская, 161
от № 24-967/к
04 06 2021 г.

Не дай себя обмануть!

Полицейские рассказывают простые правила, чтобы не стать жертвой мошенников.

Сотрудники полиции призывают жителей Ростовской области быть бдительными! Видов мошенничества немного, но их вариаций достаточное количество, причем все они выгодны для мошенников. Даже при небольших финансовых потерях конкретного человека (15-150 рублей) срабатывает эффект масштаба, когда жертвами становятся тысячи людей. Один из самых распространенных видов мошенничества – телефонное. По телефону злоумышленники говорят, что родственник или другой близкий человек попал в беду:

- он попал в серьезное ДТП;

- совершил преступление и находится в правоохранительных органах;

- попал в больницу и ему прямо сейчас требуется дорогостоящая операция.

После того, как жертва ошарашена плохой новостью, мошенники продолжают давить на нее и предлагать прямо сейчас «решить вопрос» и спасти близкого. Нередко для подтверждения своих слов трубка передается «родственнику», который плачет и просит спасти его. Большинство людей, пострадавших от таких ситуаций, потом уверяли, что это был голос их близкого человека. На самом деле мошенники используют состояние шока, в котором находится потенциальная жертва.

Затем преступники называют сумму, которую необходимо передать посреднику, перевести на карту или положить на номер телефона.

Не дайте себя обмануть!

Столкнувшись с подобной ситуацией, необходимо соблюдать простые правила:

- никогда и никому не отправляйте и не передавайте деньги;

- позвоните своему близкому человеку;

- позвоните в органы внутренних дел, больницу и проверьте полученную по телефону информацию.

Если вы все-таки стали жертвой мошенников, незамедлительно обратитесь в ближайший отдел полиции.

Представляясь службой безопасности банка…

Сотрудники полиции напоминают о том, как не попадаться на уловки злоумышленников.

Еще одна разновидность телефонного мошенничества - «Ваша карта заблокирована». На мобильный телефон приходит СМС о блокировке карты, начислении денежных средств, либо о списании комиссии за неуплату кредита. Для подтверждения или отмены операции необходимо связаться по указанному в сообщении номеру. На том конце провода трубку снимает мошенник. Основная его цель напугать жертву и заставить скорее совершить нужное действие, мошенники придумывают разные сценарии. Говорят, что банк заблокировал счет, начислил штраф за кредит или что проведена подозрительная операция. Далее злоумышленник просит продиктовать номер карты и трехзначный код, указанный на обратной стороне. После чего на номер телефона жертвы поступает СМС с кодом. Преступник, поторапливая ни о чем не подозревающего гражданина, просить назвать полученный код. В некоторых случаях телефонные мошенники просят абонента подойти к банкомату и там совершить несколько манипуляция, в результате которых со счета жертвы будут похищены деньги.

В других случаях мошенник сам звонит жертве. Номер входящего звонка очень похож на номер банка, а звонящий представляется «сотрудником службы безопасности банка». Мошенник сообщает о сомнительном переводе денежных средств с банковской карты либо о сбое системы. Преступник спрашивает у абонента подтверждение по данному переводу. Получив отказ, он предлагает отменить данную операцию, однако для этого он просит у вас полные данные карты, CVV- или CCV-код, код из СМС или пароли от Сбербанк Онлайн. Это нужно якобы «для сохранности ваших денег».

Результат в обоих случаях не заставит себя долго ждать – деньги с карты перейдут на счет мошенников.

Чтобы избежать подобного рода преступлений необходимо:

- при поступлении подобных смс ни в коем случае не сообщайте персональные данные неизвестным лицам. Даже если они представляются сотрудниками банка;

- при получении сообщений от банков, мобильных операторов о проблемах со счетом, обязательно перезвоните по официальному номеру банка и уточните нужные сведения. Банк никогда не запрашивает подобным образом информацию.

- не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам;

- сразу завершайте разговор. Сотрудник банка никогда не попросит у вас данные карты или интернет-банка.

Если вы все-таки стали жертвой мошенников, незамедлительно обратитесь в ближайший отдел полиции.

«Вы выиграли приз…»

Сотрудники полиции в очередной раз объясняют гражданам, как не стать жертвой мошенников. Еще одна уловка, к которой прибегают преступники – сообщение о якобы полученном выигрыше (путевки, квартиры, бытовая техника, компьютеры и различные гаджеты). Суть его состоит в том, что совершаются e-mail или смс-рассылки с текстом о получении адресатом ценной вещи. Важная деталь, которая сразу же обращает на себя внимание - для получения выигрыша организаторы просят сделать перевод некоторого количества денег либо перейти по ссылке для заполнения анкеты.

В качестве причины могут называть:

- выплату налогов;

- уплату таможенной пошлины;

- компенсацию транспортных расходов;

- проверку подлинности личности, работоспособности карты или электронного кошелька.

В сравнении со стоимостью приза размер требуемой к переводу суммы выглядит незначительным. После ее получения мошенники перестают оставаться на связи либо входят во вкус и предлагают совершить дополнительный платеж для оформления ценного выигрыша.

Меры, чтобы себя обезопасить:

При получении сообщения о внезапном крупном выигрыше стоит вспомнить, подавали ли вы заявку на участие.

Не нужно говорить «организаторам» данные своих банковских карт или спешить переводить деньги за якобы оплату членского взноса, оформления документов или чего-то другого.

Не переходите по ссылкам в полученных электронных письмах и смс.

Если вы столкнулись с подобными мошенническими схемами, незамедлительно обратитесь в полицию.

Вирусная рассылка сообщений

Сотрудники ГУ МВД России по Ростовской области продолжают предостерегать граждан от различных махинаций, к которым прибегают кибер-мошенники. Нередко злоумышленники для похищения денег используют номера телефонов с сайтов по продаже товаров и услуг, либо нелегально покупают базы номеров. В дальнейшем, используя специальную программу, мошенники рассылают смс-сообщения с определенной ссылкой, переходя по которой устройство заражается вредоносной программой. «Вредонос» собирает и передает своему владельцу данные необходимые для хищения денег с банковского счета либо со счета мобильного оператора.

Мошенники придумывают разнообразные предлоги, чтобы подтолкнуть ни о чем не подозревающего человека перейти по предложенной ссылке. Например, «ваша карта заблокирована, перейдите по ссылке для ее разблокировки», «мне прислали твою фотографию, я и не мог подумать, что ты так поступишь (далее следует текст ссылки)», «меня заинтересовало твое предложение о продаже (платья, дивана, телевизора и т.д.) далее следует ссылка».

Единственное правило, которому следует придерживаться гражданам, чтобы обезопасить свои сбережения, это не переходить по сомнительным ссылкам в сообщениях.

Если в отношении вас были совершены противоправные действия незамедлительно обратитесь в ближайший отдел полиции.

Срочно переведи деньги, потом объясню

Сейчас практически каждый человек имеет страничку в различных социальных сетях. Однако смекалка мошенников находит все новые комбинации для незаконного обогащения. Злоумышленники взламывают аккаунты пользователей социальных сетей, изучают переписки и стили общения человека со знакомыми. А затем производят рассылку друзьям потерпевшего с просьбой занять определенную сумму денег на один день. В любой из социальных сетей вам может прийти сообщение от знакомого, где он рассказывает драматичную историю, которая вызывает желание помочь (попал в ДТП, тяжело болен сам или родственник и т.д.). Как правило, информацию проверять не спешат, воздействуют на эмоции, пользователь верит, что нужна помощь и ее оказывает, пересылая деньги мошенникам.

Способ разоблачения подобных махинаций – это проверка информации. Не поленитесь потратить время, чтобы совершить звонок знакомому, который обратился за помощью. Либо вы можете задать контрольный вопрос, который будет знать только этот человек.

Если вас все-таки обманули, обратитесь в полицию. Чем быстрее вы оповестите органы внутренних дел о совершенном в отношении вас преступлении, тем выше вероятность задержания подозреваемого по горячим следам.