Приложение №1

ИНТЕРНЕТ-МОШЕННИЧЕСТВО - ПАМЯТКА ДЛЯ ГРАЖДАН.

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

Несмотря на принимаемые правоохранительными органами меры, в Донецкой Народной Республике участились случаи дистанционных хищений с использованием информационно-телекоммуникационных технологий.

Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву раскрывать всю информацию о себе либо совершать те или иные действия, используют чувства (сострадание, обеспокоенность за близких, жалость), человеческие слабости (стяжательство, алчность) в своих корыстных интересах.

ОСНОВНЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА:

СИТУАЦИЯ 1.

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками полиции за совершение преступления (совершил ДТП, хранил оружие или наркотики, нанёс тяжкие телесные повреждения).

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз «помогал» людям таким образом. Но если раньше деньги привозили непосредственно ему, то сейчас деньги необходимо привезти в определенное место, передать какому-либо человеку, либо перевести на счет (абонентский номер телефона).

Не спешите выполнять эту просьбу. Прекратите разговор. Успокойтесь, перезвоните родным, наберите номер телефона родственника, с которым якобы произошла беда. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Хотя беспокойство за родственника или близкого человека мешает мыслить здраво, следует понимать: если незнакомый человек звонит Вам и требует привезти на некий адрес денежную сумму – это мошенник. Обязательно поговорите с кем-нибудь, прежде чем Вы примете решение дать взятку, что является преступлением.

СИТУАЦИЯ 2.

Вы получили смс-сообщение о том, что ваша банковская карта заблокирована.

Никогда не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.

Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.

СИТУАЦИЯ 3.

Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату.

Никогда не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.

Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.

СИТУАЦИЯ 4.

Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза.

Никогда не отправляйте деньги незнакомым лицам на их электронные счета. Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.

СИТУАЦИЯ 5.

Вы решили продать товар и после подачи объявления в ближайшие дни Вам звонит желанный покупатель и говорить, что готов оплатить сразу всю сумму за товар, но ему необходимо узнать номер Вашей карты и пароли, которые поступят в смс-сообщении или другие данные с карты.

Никогда никому не сообщайте номер Вашей карты, пароли из смс-сообщений и другие реквизиты карты, иначе с Вашей карты похитят денежные средства.

Для перевода денежных средств Вам, покупателю достаточно знать один номер Вашей карты и больше никакие сведения не требуются.

Также можно предложить способ оплаты, через платежные переводы в банках на Ваше ФИО, тогда у Вас похитит денежные средства будет невозможно!

СИТУАЦИЯ 6.

Общаетесь в интернете и имеете аккаунты в соцсетях? К Вам обратился знакомый с просьбой одолжить ему денежные средства?

Никогда не переводите деньги, не связавшись с другом по телефону и не выяснив причину его просьбы, даже если в сообщении он пишет, что не может говорить. Никогда не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред. Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно. Помните о том, что видео и аудиотрансляции, равно как и логин вашей сетевой переписки, могут быть сохранены злоумышленниками и в последствии использованы в противоправных целях.

СИТУАЦИЯ 7.

Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы.

Никогда не переходите по ссылке, указанной в сообщении.

Помните, что, перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.

МВД по Донецкой Народной Республике
ПРЕДУПРЕЖДАЕТ

Участились случаи телефонного мошенничества и краж в отношении пожилых людей.

Преступники, представляясь работниками социальных служб, медицинских организаций, фондов, похищают имущество, обменивают накопления пенсионеров на схожие купоны, обманывают с несуществующим обменом денег, обещают подарки, выигрыши, компенсации, предлагают купить на дому или заказать по почте дорогостоящие лекарственные препараты и медицинские приборы, «исцеляющие от всех болезней».

При покупке (заказе) товаров через Интернет, мошенники требуют предоплату, которую затем похищают.

ПОМНИТЕ: ЭТО ОРУДУЮТ МОШЕННИКИ!

Аферисты, представляясь детьми и внуками, звонят на домашние и мобильные телефоны, требуют деньги за помощь, якобы попавшему в беду (похищен, задержан сотрудниками полиции, сбил человека и т.п.).

Если при звонке на Ваш домашний телефон им отвечает Ваш ребенок, то мошенники под предлогом выигрыша какого-нибудь приза могут убедить ребенка продиктовать им номер Вашей банковской карты, при этом убеждая Ваших детей ничего не говорить родителям.

Будьте бдительны и ни в коем случае не передавайте деньги незнакомым людям, не пускайте в дом незнакомых, проведите разъяснительные беседы с Вашими детьми и престарелыми родителями.

В случае совершения подобных фактов немедленно сообщите в полицию по телефону «102».

К СВЕДЕНИЮ!

Официальный Telegram-канал Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России - «Вестник Киберполиции России» (https://t.me/cyberpolice_rus).

Если вы стали жертвой мошенников анонимный чат-бот - «Помощник Киберполиции» (**@cyberpolicerus_bot)** окажет Вам консультационную помощь.

МВД по Донецкой Народной Республике

Приложение №2

Сведения об основных способах обмана/вовлечения несовершеннолетних лиц!

1. Классическая мошенническая схема: «Ваш родственник попал в ДТП», в которой подростку предлагается работа в качестве курьера. Предложения такого рода распространяются в социальных сетях и популярных мессенджерах: «оказание помощи пожилым гражданам в осуществлении переводов денежных средств», за вознаграждение в виде так называемых «комиссионных» от суммы переведенных средств. Однако в погоне за деньгами молодые люди не думают о том, что такие «выезды на адреса» для курьеров заканчиваются задержанием, и как правило последующим заключением под стражу.

2. Телефонный звонок от «должностных лиц». Мошенники звонят подростку и представившись сотрудником полиции, службы безопасности либо других организаций, сообщают о сложившейся у их родителей «чрезвычайной ситуации», убеждая перевести деньги родителям, которым «угрожает опасность».

3. Злоумышленники связываются с детьми и сообщают им о выигрыше в онлайн-игре или возможности приобрести игровую валюту на платформе Roblox. В этом случае подростку рекомендуют предоставить данные банковских карт близких для якобы получения денежного приза.

4. Преступники уговаривают несовершеннолетнего установить программы для удаленного доступа к смартфонам родителей. Это делается под предлогом защиты или оказания помощи. Таким образом у мошенников появляется возможность управлять банковскими приложениями взрослых членов их семьи.

5. Мошенники заманивают подростков через объявления в интернете о «непыльной» работе, но с хорошей оплатой. Для отклика нужно оставить данные банковской карты, на которую поступят деньги. Затем ребенок должен перевести деньги на специальный счет. За услуги жертва якобы получит процент от суммы.

6. Преступники выходят на подростков с предложением о совершении диверсий, направленных на повреждение объектов военной инфраструктуры, правоохранительных органов, государственных учреждений или банков за щедрое вознаграждение.

7. Злоумышленники представляется сверстником (сверстницей) и с использованием социальных сетей или мессенджеров понуждает к отправке интимных фотографий, получив которые за их нераспространение требуют денежные средства либо выполнение неправомерных действий.

Как защитить детей:

Расскажите им, что обещания быстрой прибыли – всегда тревожный знак. Опишите подобные схемы и ответственность за совершаемые преступления. А также познакомьте с правилами цифровой гигиены.

Заведите специальную карту для детских покупок в приложениях, поставьте на ней низкий лимит трат, подключите уведомления обо всех операциях.

Дайте понять, что ко всем знакомствам в интернет-пространстве нужно относится критически.

Поговорите про опасность перехода по ссылкам, про вирусы и коды подтверждения.

Если ребенок играет с вашего устройства, настройте для него отдельный профиль без доступа к финансам.

Объясните, что нельзя отправлять свои личные данные, копии документов, фотографии банковской карты и деньги незнакомым людям.

Доверительно общайтесь с ребенком, будьте в курсе его планов и интересов, регулярно обсуждайте с детьми, какие опасности могут встретится в интернете и как их избежать.

Если Вам стало известно о фактах мошенничества, **обязательно звоните в полицию по телефону «102».**

К СВЕДЕНИЮ!

Официальный Telegram-канал Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России - «Вестник Киберполиции России» (https://t.me/cyberpolice_rus).

Если вы стали жертвой мошенников анонимный чат-бот - «Помощник Киберполиции» (**@cyberpolicerus_bot)** окажет Вам консультационную помощь.

МВД по Донецкой Народной Республике