

## **Уважаемые граждане!**

Соблюдение элементарных правил поможет вам не стать жертвой мошенников и сохранить личное имущество. Потерпевшими от преступных действий злоумышленников становятся не только излишне доверчивые пенсионеры, но и молодые люди. Поэтому стоит как можно чаще напоминать своим родственникам и знакомым о том, как действуют мошенники и объяснять, что ни при каких обстоятельствах не следует перечислять деньги незнакомым людям или сообщать свои персональные данные, логины, пароли и коды банковских карт. Приведем примеры.

### **«Мошенничество с предоплатой»**

В последнее время участились случаи совершения мошенничеств с использованием популярных сайтов и социальных сетей. Ситуации могут развиваться по нескольким направлениям:

— Мошенники размещают на сайте объявления о продаже по низким ценам каких-либо вещей, техники, транспортных средств, недвижимости и т.п., затем просят покупателя внести предоплату, а после перевода денежных средств номер лже-продавца перестает отвечать.

-Противоположная ситуация, когда гражданину, разместившему на популярных сайтах объявление о продаже своего имущества, поступает звонок от, якобы, потенциального покупателя. Мошенник предлагает перевести предоплату за товар и для этого запрашивает реквизиты банковских карт продавца, получая тем самым доступ к денежным средствам, находящимся на его счетах.

### **«Взлом аккаунта в социальных сетях»**

Мошенники, пользуясь беспечностью граждан, путем использования специального программного обеспечения, получают доступ к страницам пользователей социальных сетей. После чего злоумышленники от имени пользователя запускают рассылку сообщений всем контактам «взломанной страницы» с просьбой оказать материальную помощь в сложной жизненной ситуации или дать в долг.

### **«Ваша карта заблокирована»**

Еще один способ мошенничества, неоднократно освещаемый в СМИ, однако, не теряющий своей актуальности. Гражданину звонит незнакомец, представляясь сотрудником банка, и сообщает о блокировке банковской карты, либо на телефон приходит соответствующее СМС-сообщение. Чтобы решить эту проблему, злоумышленник, под предлогом уточнения информации, выясняет данные карты или вынуждает гражданина самостоятельно воспользоваться банкоматом, набрать определенную комбинацию цифр и, тем самым, совершить операцию по переводу своих денежных средств на сторонний счет.

### **«Ваш родственник стал виновником смертельного ДТП»**

Не перестает пользоваться успехом у аферистов старая стандартная мошенническая схема, когда злоумышленник звонит на стационарный или мобильный телефон, представляется сотрудником полиции и сообщает гражданину о том, что его сын (дочь) задержан (а) за совершение тяжкого преступления, либо кто-то из родственников стал виновником ДТП, в результате которого под колесами его автомобиля погиб человек. Для того, чтобы родственнику избежать уголовной ответственности, мошенник предлагает заплатить определенную сумму денег. Деньги, как правило, просят передать курьеру или перевести через платежный терминал на указанный расчетный счет или телефонный номер.

**ОТНЕСИТЕСЬ БОЛЕЕ ОТВЕТСТВЕННО К СОЗДАНИЮ ПАРОЛЕЙ И ЛОГИНОВ К СВОИМ ЛИЧНЫМ СТРАНИЦАМ, СТАРАЙТЕСЬ ЧАЩЕ ИХ МЕНЯТЬ И НЕ ИСПОЛЬЗОВАТЬ ОДИН ПАРОЛЬ ДЛЯ ВСЕХ ВОЗМОЖНЫХ СЛУЧАЕВ. НЕ СООБЩАЙТЕ НИКОМУ PIN-КОД И CVV2-КОД КАРТЫ (ЦИФРЫ С ОБРАТНОЙ СТОРОНЫ КАРТЫ), А ТАКЖЕ СРОК ЕЁ ДЕЙСТВИЯ И ПЕРСОНАЛЬНЫЕ ДАННЫЕ ВЛАДЕЛЬЦА. НИ ОДИН БАНК НЕ БУДЕТ ПО ТЕЛЕФОНУ ЗАПРАШИВАТЬ У ВАС ЭТИ РЕКВИЗИТЫ. ДЛЯ ЗАЧИСЛЕНИЯ СРЕДСТВ НА ВАШ СЧЁТ ДОСТАТОЧНО ЛИШЬ 16-ЗНАЧНОГО НОМЕРА, УКАЗАННОГО НА ЛИЦЕВОЙ СТОРОНЕ КАРТЫ.**

**НЕ СООБЩАЙТЕ НЕИЗВЕСТНЫМ ЛИЦАМ ПИН-КОД ДЛЯ ВХОДА В ВАШ ОНЛАЙН-БАНК — ДЛЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ ЭТО НЕ ТРЕБУЕТСЯ.**

**НЕ ИСПОЛЬЗУЙТЕ КАРТЫ СО СВОИМ ОСНОВНЫМ ФИНАНСОВЫМ КАПИТАЛОМ ДЛЯ ОПЛАТЫ ТОВАРОВ И УСЛУГ В СЕТИ ИНТЕРНЕТ.**

**НЕ РЕКОМЕНДУЕТСЯ ВХОДИТЬ В ИНТЕРНЕТ-БАНК С ЧУЖИХ КОМПЬЮТЕРОВ ИЛИ ИЗ НЕЗАЩИЩЕННЫХ ПУБЛИЧНЫХ СЕТЕЙ WI-FI.**

**НА ЛИЧНОМ КОМПЬЮТЕРЕ, СМАРТФОНЕ, ПЛАНШЕТЕ УСТАНОВИТЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И СВОЕВРЕМЕННО ЕГО ОБНОВЛЯЙТЕ.**

**НЕ СКАЧИВАЙТЕ ФАЙЛЫ ИЗ НЕПРОВЕРЕННЫХ ИСТОЧНИКОВ (ФАЙЛООБМЕННЫЕ СЕРВИСЫ, СОЦИАЛЬНЫЕ СЕТИ). НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ, ПОЛУЧЕННЫМ ОТ СОМНИТЕЛЬНЫХ ИСТОЧНИКОВ. НЕ ОТКРЫВАЙТЕ ФАЙЛЫ ИЗ ПОДОЗРИТЕЛЬНОЙ ЭЛЕКТРОННОЙ ПОЧТЫ.**

**В случае совершения в отношении Вас противоправных действий просим Вас незамедлительно обращаться в Дежурную часть МО МВД России «Аркадакский» по телефону: 8(84542) 4-19-54 или 02 с сотового телефона -102.**

ГУ МВД России по Саратовской области доводит до Вас озабоченность по поводу все большего распространения преступлений, совершаемых с использованием теле-коммуникационных технологий.

Только за прошедший год их число в области превысило 4,5 тысячи, что в 1,5 раза превышает данные за 2018 год. Более 90% из них составляют кражи и мошенничества, совершенные с использованием мобильной связи, Интернета и средств дистанционного управления финансами.

Аналогичная ситуация и в текущем году: уже более 600 граждан области подверглись таким посягательствам.

Спектр человеческих отношений, в которых мошенники подыскивают своих жертв, очень широк. Зачастую эти преступления поражают своей циничностью, поскольку они играют на самых сильных личных чувствах людей – милосердии, любви к ближним. При этом, в большинстве своем выбирают жертв из числа самых незащищенных, наименее социально адаптированных категорий граждан – стариков, инвалидов, подростков.

Преступники входят в доверие под видом социальных и медицинских работников, работников коммунальных служб, банков и правоохранительных органов, гадалок; знахарей и прочих.

Отличительная черта всех мошенников в том, что они ведут себя очень убедительно, как правило, являются хорошими психологами, в виду чего большинство потерпевших безропотно выполняли требуемые от них действия и сами переводили деньги совершенно незнакомым лицам, не проверяя преподнесенную мошенниками информацию.

Вместе с тем, элементарная внимательность и осторожность со стороны потенциальных жертв мошенников исключает саму возможность осуществления преступного умысла.

Нельзя позволять преступникам безнаказанно воспользоваться доверчивостью людей, среди которых могут оказаться наши родные и близкие!

В этой связи убедительно прошу Вас принять исчерпывающие меры в рамках Ваших полномочий для организации информирования населения, в первую очередь Ваших сотрудников, об имеющихся угрозах, проведении разъяснительной работы о правилах обеспечения личной безопасности в киберпространстве, в том числе при использовании средств дистанционного управления финансами.

Просим довести до рабочих и служащих Вашей организации, родственников и знакомых информацию:

**СОТРУДНИКИ БАНКОВ И ОРГАНОВ ВНУТРЕННИХ ДЕЛ, СОЦИАЛЬНЫХ СЛУЖБ И ДАЖЕ КОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ НИКОГДА НЕ БУДУТ ВЫЯСНЯТЬ У ВАС ДАННЫЕ ВАШИХ СЧЕТОВ И КАРТ И ТРЕБОВАТЬ КАКИХ-ЛИБО МАНИПУЛЯЦИЙ С НИМИ!!!**

**В СЛУЧАЕ ПОСТУПЛЕНИЯ ТЕЛЕФОННЫХ ЗВОНКОВ ИЛИ SMS-СООБЩЕНИЙ, В КОТОРЫХ ПОД РАЗЛИЧНЫМИ ПРЕДЛОГАМИ ОТ ВАС ТРЕБУЮТ ПЕРЕВЕСТИ ДЕНЬГИ ЛИБО ПЕРЕДАТЬ ДАННЫЕ О СЧЕТАХ И КАРТАХ, ИСПОЛЬЗУЙТЕ ВСЕ ВОЗМОЖНЫЕ СРЕДСТВА, ЧТОБЫ**

ПРОВЕРИТЬ ДАННЫЕ О ВАШЕМ СОБЕСЕДНИКЕ И ДОСТОВЕРНОСТЬ ИЗЛАГАЕМОЙ ИМ ИНФОРМАЦИИ. ДЛЯ ЭТОГО НЕОБХОДИМО ВОСПОЛЬЗОВАТЬСЯ ТЕЛЕФОНАМИ БАНКОВ, ОРГАНОВ ВНУТРЕННИХ ДЕЛ, ИНЫХ ОРГАНИЗАЦИЙ, РАЗМЕЩЕННЫМИ НА ОФИЦИАЛЬНЫХ САЙТАХ ЭТИХ УЧРЕЖДЕНИЙ, НА ОБРАТНОЙ СТОРОНЕ ВАШЕЙ БАНКОВСКОЙ КАРТЫ.

ЕСЛИ ВЫ ВОВРЕМЯ РАСПОЗНАЛИ МОШЕННИЧЕСТВО И НЕ ПЕРЕЧИСЛИЛИ ДЕНЕЖНЫЕ СРЕДСТВА ПРЕСТУПНИКАМ, СООБЩИТЕ В ПОЛИЦИЮ ОБ ЭТОМ ФАКТЕ, НОМЕРЕ ТЕЛЕФОНА ЗВОНИВШЕГО И ЛЮБУЮ ДРУГУЮ ИНФОРМАЦИЮ, КОТОРУЮ МОШЕННИК ВАМ УСПЕЛ СООБЩИТЬ.

Убеждены, что чем больше людей будет информировано об имеющихся в киберпространстве угрозах, тем меньше останется у преступников возможностей для хищений имущества.

Заранее благодарю за сотрудничество.