**ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО – КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

С развитием информационных технологий злоумышленники широко используют сеть Интернет, позволяющую им действовать анонимно и создавать условия для хищения чужого имущества. Отмечается рост преступлений этой категории, совершенных путем телефонных звонков под видом сотрудников банка, кредитного учреждения, правоохранительных органов и организаций.

В большинстве случаев мошенники, представляясь сотрудниками специальных служб и организаций, используют методы социальной инженерии – введение потерпевшего в заблуждение путем запугивания, обмана или злоупотребления доверием для получения несанкционированного доступа к информации, электронным средствам платежа или побуждения владельцев самостоятельно совершить перевод денежных средств с целью их хищения.
Большинство из них составляют посягательства на безналичные денежные средства граждан, ответственность за которые предусмотрена статьями 158 и 159 УК РФ, а также факты неправомерного доступа к охраняемой законом компьютерной информации, сопряженного с ее блокированием, модификацией либо копированием (статья 272 УК РФ).

Наиболее распространенным способом хищения денежных средств является вид «телефонного мошенничества», когда потерпевшим звонят злоумышленники, представляясь сотрудниками кредитно-финансовых организаций или правоохранительных органов, после чего под предлогом предотвращения списания денежных средств предлагают перевести их на «безопасный счет». Потерпевшие, поддавшись влиянию, переводят имеющиеся у них денежные средства на банковские счета по реквизитам, представленным злоумышленниками. Также в ряде случаев мошенники могут указывать на необходимость взятия кредитов в банковских учреждениях в целях предотвращения возможности оформления кредитов злоумышленниками.

Другим распространенным способом совершения преступлений является схема с «продлением текущего договора на обслуживание sim-карты».
Злоумышленники, представляясь представителем сотового оператора, сообщают об истечении договора по мобильному номеру и если его не продлить, sim-карта будет заблокирована. Далее «оператор» предлагает «очень удобный» процесс продления договора - сообщить поступивший код от портала «Госуслуг». Далее жертве приходит СМС-сообщение с кодом доступа в личный кабинет портала «Госуслуги». Сообщая данный код доступа мошенникам – потерпевший, передает им доступ ко всей персональной информации на портале «Госуслуг». Кроме того, таким образом злоумышленники могут получить доступ и к личному кабинету мобильного оператора. Потерпевший может утратить не только доступ к нему, но и потерять деньги на мобильном счете, банковской карте; без его ведома, могут быть подключены услуги, позволяющие получить кредит.

По подобной схеме, представляясь сотрудниками страховой компании, территориального фонда ОМС, специалистами департаментов или министерств здравоохранения мошенники обманывают граждан, предлагая заменить полис обязательного медицинского страхования. Другой вариант этой схемы – скачать фейковое приложение Минздрава, которое на самом деле является вредоносной программой, взламывающей устройство.

Необходимо помнить, что полис ОМС есть у каждого гражданина, он бессрочный и не требует продления. Данные о полисе медицинское учреждение может получить в единой базе, поэтому предъявлять его при посещении врача не нужно.

Также находит распространение способ завладения денежными средствами потерпевших путем выдачи себя злоумышленниками за руководителей различных организаций. Мошенники создают ложные аккаунты в популярных мессенджерах от лица руководителей организаций. Страницы содержат их реальные данные (фамилия, имя, отчество, фото – эти сведения берутся из Интернета) и выглядят максимально достоверно. Используя фальшивые аккаунты якобы руководителей организаций злоумышленники, связываются с подчиненными тех лиц, чьи страницы были подделаны.

В России злоумышленники для хищения денег стали чаще использовать новый инструмент обмана - дипфейк-технологии. С помощью нейросети мошенники создают реалистичное видеоизображение человека. Затем сгенерированный образ рассылают его друзьям или родным через мессенджеры или социальные сети. В коротком фальшивом видеоролике виртуальный герой, голос которого иногда сложно отличить от голоса прототипа, рассказывает якобы о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на определенный счет. В некоторых случаях мошенники создают дипфейки работодателей, сотрудников государственных органов, известных личностей из той сферы деятельности, в которой трудится их потенциальная жертва. Чтобы создать цифровую копию конкретного человека, злоумышленники используют фото и видео, а также запись голоса, полученные в основном в результате взлома его аккаунта в социальных сетях или мессенджерах.

Проявляйте осторожность при получении от своего знакомого голосового или видеосообщения с просьбой о финансовой помощи – его аккаунт могли взломать злоумышленники. Иногда для рассылки таких сообщений мошенники создают поддельные страницы с именем и фото человека. Не спешите переводить деньги! Обязательно сначала позвоните тому, от чьего имени поступило сообщение, и перепроверьте информацию. Распознать дипфейк можно по неестественной монотонной речи собеседника, дефектам звука и видео, несвойственной мимике. Если возможности позвонить и убедиться, что человеку действительно нужна помощь, нет, задайте в сообщении личный вопрос, ответ на который знает только ваш знакомый.

## КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ: ОБЩИЕ РЕКОМЕНДАЦИИ

- Не сообщайте никому и никогда паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код. Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте ее в социальных сетях, на форумах и каких-либо сайтах в Интернете, а также не храните данные карт и PIN-коды на компьютере или в смартфоне.

- Если с неизвестного номера звонит сотрудник Центробанка, правоохранительных органов, государственной организации или банка с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет Центробанка и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку.

- Если подозреваете, что вам звонит мошенник, позвоните в банк по номеру телефона, указанному на обратной стороне карты или на его сайте, или в контакт-центр ведомства, сотрудником которого представлялся звонящий.

- Не совершайте каких-либо действий по счету, если вам звонят из Центробанка с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет, или с предложением об оформлении кредита. Банк России не открывает счета и не работает с гражданами.

  По возможности установите антивирус на все устройства и обновляйте его.

- Совершайте покупки в Интернете только на проверенных сайтах. Заведите специальную карту для онлайн-покупок и пополняйте ее ровно на ту сумму, которая нужна для оплаты. При совершении покупок обращайте внимание на наличие в строке браузера рядом с названием сайта значка безопасного соединения (замочка).

- Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, получить какую-либо выплату и тому подобное. Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

- Помните, что сотрудники государственных организаций, служб безопасности, правоохранительных органов никогда сами не звонят по телефону в мессенджерах Telegram или WhatsApp, и не предлагают решить какие-либо вопросы, связанные с Вашими финансами, уголовным преследованием, по телефону.

- Следует внимательно относиться к установке и разрешению программам на смартфоне доступа к SMS и приему звонков, так как среди них может оказаться шпионское программное обеспечение, крадущее Ваши данные.

**ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ ФИНАНСОВОГО МОШЕННИЧЕСТВА:**

1. Немедленно заблокируйте карту с помощью мобильного приложения или личного кабинета на сайте банка. Заблокировать ее также можно через контакт-центр банка (телефон указан на оборотной стороне карты) или в любом его отделении.

2. В течение суток после получения сообщения о списании средств напишите заявление в отделении банка о несогласии с операцией. Также обратитесь с заявлением о хищении денег в любое отделение полиции.