Приложение 4

Основные виды преступлений в сфере информационно-телекоммуникационных технологий, зарегистрированных в УМВД России по г. Сургуту:

✓ **Мошенники звонят (в том числе с федеральных номеров «8800…», «8495…», с номеров, принадлежащих федеральным органам власти РФ) с абонентских номеров и, представляясь сотрудником Центробанка, поясняют гражданину, что его карта заблокирована, или по банковской карте происходит несанкционированное списание денежных средств, или несанкционированное оформление кредита, и, во избежание проблем, необходимо следовать инструкциям банковского работника, сотрудника правоохранительных органов, оказать им содействие, оформить «зеркальный кредит», перевести деньги на «сохранные», «безопасные» счета (ячейки)…**

- сотрудники банка, тем более Центрального банка России, не звонят своим клиентам по поводу подозрительных операций, не просят назвать номера карт, cvc-коды, смс-сообщения…

- сотрудники банка никогда не общаются с клиентами в мессенджерах, не просят озвучить данные карты, пароли, суммы

- не существует «резервных», «безопасных», «запасных» счетов. Если вам звонят сотрудники банков, правоохранительных органов и сообщают о каких-либо несанкционированных операциях, кладите трубку! Не вступайте в разговор, и, тем более, не сообщайте какую-либо информацию!

- сотрудники полиции никогда по телефону не сообщают, что в отношении вас возбудили уголовное дело (или хотят возбудить), или вы стали потерпевшим по уголовному делу и необходимо совершить определенные действия… Даже если звонят с федеральных номеров, сотрудники правоохранительных органов никогда по телефону не просят оказать содействие в установлении преступников, в том числе, в банковских учреждениях.

✓ **Вам позвонили якобы ваши близкие или сотрудники полиции и сообщили, что родственник попал в беду (совершил аварию, подозревается в совершении преступления), требуются деньги для решения проблем. Злоумышленники просят перевести деньги на счет, на номер телефона, или отправляют курьера.**

- прекратите разговор и перезвоните родственнику, членам его семьи (маме, папе, сестре…), убедитесь, что все в порядке.

- начните задавать звонившему простые вопросы, ответы на которые он знать не может: даты рождения, кличка животного, рост, размер обуви, и т.д.)

- запомните, таким образом вы проблемы не решите. Кроме того, за дачу взятки должностному лицу предусмотрена уголовная ответственность по ст.291 УК РФ «Дача взятки».

✓ **Приобретение товара через сайты бесплатных объявлений («Авито», «Юла», «Дром» и т.д.), где злоумышленник поясняет, что товар есть в наличии, однако для его получения необходимо выслать либо стопроцентную предоплату, или половину стоимости товара, если указана большая сумма**

оплаты, может выслать гражданину, по просьбе последнего, фото товара, либо товарно-транспортную накладную о том, что товар действительно находится в одной из транспортной компании с чеком об оплате.

- если вы продаете товар, то для перевода денег достаточно только номера телефона или номера банковской карты.

- нельзя по просьбе покупателя переходить по каким-либо ссылкам для безопасной оплаты.

- нельзя сообщать cvc-коды, код из смс сообщений.

- если вы покупаете товар, то не отправляйте 100% предоплату, прежде чем отправлять деньги за товар, сначала убедитесь в его наличии и достоверности продавца! (если нет возможности это сделать, лучше откажитесь от покупки).

✓ **Мошенники взламывают «личный кабинет» на сайте Госуслуг. Преступники звонят, представляются сотрудниками МФЦ, сайта госуслуг, просят продиктовать коды из смс, получают доступ в «личный кабинет» и полную информацию о владельце, в том числе, паспортные данные, снилс и т.д.**

- сотрудники сайта государственных услуг, МФЦ не звонят клиентам, даже в случае взлома «личного» кабинета.

- сотрудники сайта государственных услуг, МФЦ не запрашивают ваши персональные данные, данные банковских карт, смс-коды и т.д.

- необходимо прервать разговор, зайти в личный кабинет и поменять пароль.

✓ **Займы в МФК и оформление кредитов, результат – испорченная кредитная история.**

- необходимо постоянно осуществлять мониторинг кредитной истории физического лица в личном кабинете на Госуслугах. Данная услуга бесплатно представляется указанным порталом 2 раза в год. Можно обратиться в любое отделение банка, клиентом которого вы являетесь, и осуществить внесение сведений по ограничению операций на кредитование по видам: на микрофинансирование, на потребительское кредитование на любую сумму, на ипотечное кредитование.

✓ **Инвестирование.**

- нельзя переходить по рекламной ссылке, оставляя заявку в «брокерской компании». Солидные брокерские компании не привлекают клиентов посредством рекламных ссылок в социальных сетях, мессенджерах.

- не регистрируйте «личный» кабинет, и не устанавливайте программное обеспечение, предлагаемое менеджером финансовой организации

- не соглашайтесь на предложение брокера сопровождать ваши финансовые вложения

- вам могут позволить вывести некоторую сумму с прибылью, но только для того, чтобы вы инвестировали еще большую сумму.

Варианты текста для баннеров:

Баннер 1:
Резервного или безопасного счета, "зеркального" кредита в банках не существует!

Баннер 2:
Не помогайте позвонившему "сотруднику" правоохранительных органов в выявлении недобросовестных работников, установлении преступников!

Баннер 3:
Не инвестируйте денежные средства на сомнительных площадках, обещающих высокий доход за короткое время!

Варианты:

Вариант 1

Стоп! Нельзя!
- сообщать cvc-код, смс-код из сообщения!
- переходить по ссылке, устанавливать программы;
- инвестировать под руководством "финансового" работника;
- передавать деньги для "решения" вопроса

Вариант 2

Цель мошенников:
- узнать cvc-код, код из смс-сообщения, данные карты;
- убедить перевести деньги на резервный, безопасный счет (ячейку);
- убедить установить программу, перейти по ссылке;
- убедить передать деньги для "решения" вопроса