#Киберграмотность

Памятка для населения «Не говори»:

Основным инструментом злоумышленников для хищения денег остается использование приемов и методов социальной инженерии, когда человек под психологическим воздействием добровольно переводит деньги или раскрывает банковские сведения, позволяющие злоумышленникам совершить хищение. Проблема мошенничества актуальна как в отношении физических, так и в отношении юридических лиц.

Телефонный звонок – ключевой инструмент мошенников, которые занимаются хищением денежных средств. Они постоянно придумывают все более изощренные схемы и сценарии для звонка, чтобы заполучить доступ к деньгам. Схемы злоумышленников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Чтобы вызвать доверие, они могут обращаться по имени и отчеству. С первых минут разговора мошенники начинают давить авторитетом и должностью. Приведем некоторые распространенные способы обмана:

1. Якобы сотрудник Пенсионного фонда, соцслужбы. Мошенники сообщают, что гражданину положены дополнительные выплаты, компенсации от государства или какого-нибудь фонда. Причем для получения этой выплаты никуда ходить не надо: все деньги переведут на карту, необходимо только продиктовать все ее реквизиты, в том числе код с обратной стороны.

2. Якобы сотрудник поликлиники, аптеки, медицинского центра. Мошенники соотносят информацию о проблемах со здоровьем гражданина и сообщают ему о появлении дефицитного и дорогого лекарства по специальной цене, которое надо срочно выкупить. Злоумышленники объясняют, что человек платит полную стоимость, а разницу в цене по скидке вернут ему на карту, реквизиты которой необходимо сообщить звонящему.

3. Якобы сотрудник банка (как правило, представителя службы безопасности). Сценарии могут быть разные: от классического «с вашей карты пытаются перевести деньги» до пугающего «по карте замечены подозрительные операции, и она заблокирована». В любом случае итогом будет просьба сообщить информацию по карте или счету, код из СМС-сообщения.

4. Якобы друг, родственник. Мошенник может представиться родственником/другом, попавшим в неприятную ситуацию, или ее случайным свидетелем, а также представителем правоохранительных органов, который готов помочь гражданину с решением проблемы. Схема довольно старая, но мошенники продолжают ею пользоваться, так как страх за близкого человека – это очень сильная эмоция.

Мошенники очень часто представляются якобы сотрудниками Центрального банка (Банка России). Гражданам звонят и от имени Центробанка сообщают, что по их карте зафиксирована подозрительная активность: пытаются перевести все деньги за рубеж.

Чтобы сохранить свои деньги и подтвердить, что это не сам человек совершает данную операцию, ему необходимо открыть в Центробанке «защищенный/безопасный/специальный» личный счет. Для этого уточняют паспортные данные, просят подтвердить данные по счету/карте, а для открытия счета просят подтвердить небольшой перевод на этот счет, который Центробанк якобы совершает для своих клиентов, то есть сообщить код из СМС.

Следует помнить, что Банк России не работает с физическими лицами. При поступлении телефонного звонка от Банка России немедленно прервите разговор.

Также иногда злоумышленники представляются сотрудниками правоохранительных органов. Такие мошенники долго и подробно рассказывают об обстоятельствах уголовного дела, участником которого, по их словам, гражданин является.

Далее для уточнения информации они просят сообщить личную и финансовую информацию. Это и является признаком того, что гражданин разговаривает с мошенником: правоохранительные органы не просят назвать по телефону финансовую информацию.

Помните, что настоящие сотрудники полиции никогда не запрашивают личные и финансовые данные по телефону.

Будьте бдительны!

Информационная кампания по повышению киберграмотности населения на территории Южного и Северо-Кавказского федеральных округов

«Не говори».

Отделение по Ростовской области Южного главного управления Центрального банка Российской Федерации проводит информационную кампанию по повышению киберграмотности населения на территории Южного и Северо-Кавказского федеральных округов «Не говори». Проведение информационной кампании проходит путем распространения тематического контента на информационных ресурсах, официальных аккаунтах в социальных сетях, а также на мультимедийных экранах.