Вопрос: Одолели предложения представителей банков обезопасить деньги, реструктурировать долг, установить программы удаленного доступа на мобильное устройство и т.п. Как вести себя в таких ситуациях?

Ответ: Цель подобных предложений – похитить деньги с банковского счета.

Исходите из того, что сотрудники банка никогда по телефону или в электронном письме не запрашивают:

персональные сведения (серию и номер паспорта, адрес регистрации, ФИО владельца карты);

реквизиты и срок действия карты;

пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;

логин, ПИН-код и CVV-код банковских карт.

Они также не предлагают:

установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки;

перейти по ссылке на СМС-сообщения;

включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;

под их руководством перевести для сохранности денежные средства на «защищенный счет»;

зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Банк может инициировать общение с клиентом только по поводу консультаций по своим продуктам и услугам. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на сайте банка или в оригинальных банковских документах. Иные номера не имеют никакого отношения к банку.

Используйте только надежные каналы связи с банком, например: форму обратной связи на сайте банка, онлайн-приложения, телефоны горячей линии, группы или чат-боты в мессенджерах (если таковые имеются), а также официальные банковские приложения из магазинов App Store, Google Play, Microsoft Story.