**ПРОФИЛАКТИКА МОШЕННИЧЕСТВА**

**Признаки мошенничества**

Злоумышленники стали чаще использовать многоходовую схему обмана для хищения денег у людей. Сначала потенциальной жертве поступает звонок якобы от сотрудника правоохранительных органов, например МВД России или Генеральной прокуратуры. Лжесотрудник сообщает об операции по задержанию преступников, которые пытаются похитить деньги с банковских счетов человека. Затем человека прямо во время разговора переключают якобы на специалиста Банка России. Это делается для подтверждения серьезности ситуации и создания иллюзии официальности. «Представитель Центробанка», по сценарию мошенников, поможет человеку перевести все накопления с личных банковских счетов на специальный «защищенный» счет в мегарегуляторе. На самом деле если человек будет следовать инструкциям лжесотрудников госведомств, то переведет деньги на счета мошенников, а также раскроет им свои паспортные данные и другую личную информацию.

Злоумышленники могут также выдавать себя за работников Роскомнадзора, Социального фонда России, службы поддержки Госуслуг и других структур.

**Что предпринять?**

Не существует специальных безопасных счетов, в том числе в Центробанке, на которые следует перевести деньги для сохранности.

Игнорируйте такие звонки и сообщения, от кого бы они не поступали. Банк России не работает с физическими лицами как с клиентами, не ведет их счета, не звонит им.

Банк России предупреждает, что переключение между различными ведомствами в рамках одного телефонного звонка невозможно. Если во время разговора вам предлагают пообщаться последовательно с сотрудниками разных госструктур — это признак мошенничества. Иногда лжесотрудники государственных служб могут перезванивать своей жертве через некоторое время.

Обращаем внимание, что настоящие работники государственных ведомств никогда не просят людей совершать какие-либо денежные операции по своим картам. При поступлении такого телефонного звонка прекратите разговор и положите трубку.

**Как не стать жертвой мошенников: общие рекомендации**

1. 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.

2. 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.

3. 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.

4. По возможности установите антивирус на все устройства и обновляйте его.

5. 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).

6. 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.



**Если вы стали жертвой финансового мошенничества:**

Шаг № 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.

Шаг № 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.

ПОМНИТЕ: если вы самостоятельно перевели деньги мошенникам или предоставили им банковские данные, то банк не обязан возвращать похищенную сумму.