Телефонное мошенничество и как не дать себя обмануть.

В современной период происходит массовый переход на дистанционное банковское обслуживание, которое мошенники используют в своих интересах, перенаправив денежные средства в свою сторону.

Мошенничество совершается различными способами с применением различных средств, которые постоянно меняются и совершенствуются. В качестве примера распространённых видов мошенничества можно привести: звонки от якобы банка отом, что со счета снимаются денежные средства и необходимо срочно указать данные для блокирования производимой операции; использование СМС-сообщений, также отправленных якобы от имени банка, но совершенно с незнакомых номеров; звонки от лиц, представляющихся сотрудниками правоохранительных органов с указанием о необходимости срочного перечисления денежных средств, блокирования карт и т.п.; сообщения о выигрышах (денежном, вещевом и т.п.) с просьбой отправить в ответ СМС-сообщение или перезвонить, перевести денежную сумму для получения выигрыша.

Для того чтобы не стать такой жертвой, необходимо следовать определенным правилам:

- никому не сообщать пароль для входа в мобильное приложение банка; разовые пароли и подтверждения транзакций, которые могут быть получены на привязанный к счету мобильный телефон в виде СМС-сообщений в момент входа в систему или при необходимости подтверждения транзакции;

- если получен звонок с просьбой о срочной денежной помощи для известного гражданину лица (знакомого, родственника и т.п.), следует не принимать решение сразу, идя на поводу у позвонившего, а проверить полученную от него информацию, перезвонив вышеуказанным лицам, или связаться с ними иными способами;

- если получен звонок и лицо говорит, что сейчас со счета совершается перевод денежных средств, либо какая-то подозрительная операция, необходимо прекратить разговор и перезвонить оператору банка для проверки достоверности информации, либо самостоятельно заблокировать карту в мобильном приложении;

- нельзя перезванивать на номер, если он незнаком, и т.п.;

- нельзя сообщать таблицы разовых ключей (ТРК);

- запомните телефоны и электронные адреса банка, с которых вам поступает информация. В случае получения информации от имени банка с других номеров не отвечайте на них, обратитесь по известным вам координатам с тем, чтобы проверить, действительно ли к вам обращался банк;

- не пользуйтесь интернет-магазинами, про которые вы ничего не знаете (нет информации, отзывов);

- при получении звонков от якобы представителей правоохранительных органов с просьбой о переводе денежных средств, срочной блокировки карты и т.п. уточните ФИО, должность и место службы сотрудника, перезвоните в дежурную часть и уточните, действительно ли у них проходит службу такой сотрудник, при этом объясните суть обращения.

Также одним из способов обезопасить себя от телефонных мошенников является подключение систему СМС-оповещения обо всех операциях. Обязательно просматривайте все полученные сообщения. Запишите телефон службы поддержки банка в записную книжку вашего мобильного телефона, а также на всякий случай

на бумаге. В случае пропажи карты это поможет вам незамедлительно заблокировать карту и тем самым обезопасить свои деньги.

Помните, что пин-код вам может понадобиться только для совершения операций в банкоматах, платежных терминалах и при оплате товаров и услуг в магазинах и службах сервиса. Ни в коем случае не сообщайте свой пин-код по запросам в Интернете, звонкам незнакомых и знакомых людей. Пин-код не знают и не должны знать в том числе сотрудники банка.

Не оставляйте свою банковскую карту без присмотра.

Помните, что имя, фамилия, номер карты, срок ее действия, а также номер **CVV2/(CVC2)**, указанные на карте, являются важными элементами идентификации ее владельца. Не позволяйте чужим людям переписывать содержащуюся на карте информацию или фотографировать карту.

Если вам предлагают перевести деньги на карточку, помните, что для перевода денег с карты на карты через мобильное банковское приложение достаточно знать номер карты или номер мобильного телефона получателя денег. Никакой иной информации не требуется, ни в коем случае не сообщайте CVV2/(CVC2).

Если вы часто пользуетесь картой для приобретения товаров и услуг через Интернет, целесообразно выпустить для этих целей дебетовую карту с небольшим лимитом. Перед совершением покупки проверяйте сайт на надежность, а именно сколько времени зарегистрирован сайт, прочитайте отзывы об этом сайте на других сайтах, максимально возможно изучайте информацию перед совершением покупки. Так-же должно насторожить низкая цена на товар по сравнению с ценой на этот товар в других магазинах.

В случае если Вы предполагаете, что стали жертвой телефонного мошенничества, необходимопозвонить в дежурную часть по телефону 02 или 102, либо незамедлительно обратиться в органы внутренних дел с соответствующим заявлением. В заявлении следует максимально подробно рассказать о всех обстоятельствахпроизошедшего события.

Помощник прокурора района
О.В. Менс