Памятка.

Необходимо помнить, что преступления в сфере информационных технологий совершаются различными способами, такими как:

телефонное мошенничество (например, при поступлении звонка с неизвестного номера сообщают о том, что родственник либо знакомый попали в беду и необходима помощь денежными средствами);

СМС-мошенничества (например, на мобильный телефон с незнакомого номера поступает СМС о выигрыше приза, может поступить СМС следующего содержания: «Мама, закончились деньги, срочно положи на этот номер»);

Мошенничества с пластиковыми картами (например, с незнакомого номера поступает сообщение о том, что банковская карта заблокирована и предлагается бесплатно позвонить на определенный номер, после чего неизвестный абонент спрашивает ПИN-код от банковской карты);

«Вирусные» хищения (па мобильный телефон потерпевшего заносится сторонняя вредоносная программа (ВИРУС), которая блокирует операциионную систему телефона и дистанционно управляет ею);

Мобильный банк (имеют место в случаях, если граждане, сменившие сменив телефонный номер, забывают отключить услугу «мобильный банк»);

Интернет—покупки (покупка товаров в сети «Интернет» через непроверенные сайты).

Цель мошенников под любым предлогом извлечь личную информацию. Для получения доступа к конфиденциальным данным владельца мнимые помощники используют телефонную связь как в автоматизированном режиме, так и напрямую от мнимого «операциониста» банковского сектора. Во многих случаях с неизвестного номера поступают телефонные звонки. Как только гражданин отвечает на звонок, сразу сообщают информацию о возникших проблемах с банковской картой, счетом - например, что она заблокирована, а служба безопасности банка предотвратила попытку несанкционированного списания. Затем звонящий предлагает помощь в сложившейся ситуации, на которую многие соглашаются. Граждан убеждают в срочном решении возникшей ситуации. Очень последовательно мошенники стараются получить от всю личную информацию о банковской карте, присылают новые пароли и ПИН коды в СМС-уведомлениях. Успокаивающим голосом «банковские работники» предлагают различные возможные варианты защиты.

Догадаться о том, что любезный помощник на другом конце провода является мошенником не всегда легко, но это возможно. Необходимо поблагодарить за бдительность и узнать должность, инициалы звонившего сотрудника кредитной организации и предпринять попытку дозвониться по горячей линии. Использовать для выяснения сложившейся ситуации лучше другой номер, потому что на сегодняшний день у вымогателей существуют

технологии, позволяющие перенаправлять все последующие звонки на телефонное устройство мошенников.

В целях исключения совершения мошенниками противоправных действий необходимо соблюдать следующие меры безопасности:

- хранить ПИН-код отдельно от банковской карты, не писать ПИН-код на карте, не сообщать ПИН-код другим лицам, в том числе, позвонившим с незнакомых номеров, не вводить ПИН-код при работе в сети «Интернет»; принимать незамедлительные меры по блокировке банковской карты в случае ее утери;

- для борьбы с вредоносными программами использовать антивирус.

Чтобы не стать жертвой мошеннических действий, достаточно позвонить в банковскую организацию по телефону, указанному на официальном сайте или на обороте карты, после чего уточнить у оператора, действительно ли кто-то пытается снять деньги, сообщите номер телефона мошенников.

Кроме того, не следует переходить по неизвестным ссылкам, не перезванивать по сомнительным номерам. Никому не сообщать персональные данные, в том числе пароли и коды доступа по средствам дистанционной связи. Не хранить данные карт на компьютере и в смартфоне.

Помните, в каждом случае необходимо проявлять предусмотрительность и должную бдительность при необходимости обращаться в правоохранительные органы.