**Профилактика телефонного мошенничества**

На сегодняшний день к одному из самых распространенных видов мошенничества относится телефонное мошенничество, при котором задачей мошенника является получение у людей информации о номерах, кодах и других реквизитах карты или счета.

Человеку звонят или присылают СМС-сообщение с предложением под разными предлогами сообщить номер, PIN-код, CVV-код и другие реквизиты его банковской карты. Это может быть платеж, совершенный якобы ошибочно на карту, или сообщение о блокировке карты. Может также поступить звонок о необходимости экстренного платежа родственнику или другу, попавшему в затруднительное положение. Данные о реквизитах банковской карты позволят мошеннику произвести с нее списания денежных средств.

Чтобы не пострадать от мошенников, ни в коем случае не следует передавать информацию о своей банковской карте другим лицам, даже сотрудникам банка, и не перезванивать по телефонам, указанным в СМС-сообщениях.

В связи с этим рекомендуется удостовериться в надежности получателя средств, а также в необходимости оказания такой помощи конкретным лицам и только после этого совершать какие-либо платежи. Нужно постараться закончить разговор в тот момент, когда только возникает подозрение о том, что собеседник пытается Вами манипулировать. Обязательно сами перезвоните в банк.

Рассеянность или беспечность с мобильным устройством может обернуться мошенническим вторжением. Если вы потеряли телефон, к которому был подключен мобильный банк, или сменили номер и не оповестили банк об этом факте, то человек, которому достанется ваш номер или телефон, будет получать от банка информацию о состоянии вашего счета, включая одноразовые пароли для входа в интернет-банк.

Сегодня большинство банков для доступа в мобильный или интернет-банк или для подтверждения операций требуют ввода одноразового пароля. Этим способом банки стараются защитить своих клиентов от аферистов. Одним из последних достижений защиты расчетов с применением банковских карт является технология 3D-Secure, которая предусматривает ввод клиентом при оплате покупок в Интернете дополнительного защитного кода, поступающего по СМС-сообщению на мобильный телефон.

Как правило, эта технология позволяет защитить ваш счет от мошенников. Однако в тех случаях, когда у злоумышленников оказывается ваше средство связи (sim-карта или ее дубликат), счет фактически становится беззащитным.

Вот некоторые советы, как не стать жертвой мошенников.

Потеряв мобильный телефон с мобильным банком или сменив собственный номер, обязательно проинформируйте об этом банк.

Устанавливайте надежный пароль доступа в ваш смартфон.

Не отвечайте на СМС- или email-сообщение от банка, от Банка России, от правоохранительных органов.

Никому не сообщайте контрольную информацию о вашем счете.

Не делитесь своими персональными данными (Ф.И.О., мобильный телефон, адрес электронной почты и др.) с неизвестными или малоизвестными лицами.

Старший помощник прокурора

Аларского района

младший советник юстиции А.П. Николаева