**Еще раз о мошенничестве!**

В 2021 г. на территории Архангельской области в сравнении с предыдущим годом отмечено сокращение на 19,8 % количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий (с 4734 до 3795).

Несмотря на общее снижение числа дистанционных хищений, их количество довольно значительно – 18,4 % от всех зарегистрированных преступлений.

В связи с этим гражданам следует в каждом подозрительном случае телефонного или интернет-контакта с посторонними лицами проявлять надлежащую бдительность и соблюдать меры безопасности.

Для предотвращения противоправных действий по снятию денежных средств с банковского счета необходимо учитывать следующее.

Сотрудники банка никогда:

- не запрашивают по телефону или в электронном письме персональные сведения (паспортные данные), реквизиты и срок действия банковской карты, пароли и коды из СМС-сообщений для подтверждения финансовых операций или их отмены, логин, ПИН-код и CVV-код банковских карт;

- не предлагают установить программы удаленного доступа на мобильное устройство и не просят разрешить подключение к ним под предлогом технической поддержки;

- не предлагают перейти по ссылке из СМС-сообщения, включить переадресацию на телефон 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 для консультаций по продуктам и услугам кредитно-финансового учреждения. При этом, звонки совершаются с номеров, указанных на оборотной стороне банковской карты, на сайте банка или в оригинальных банковских документах. Иные номера не имеют никакого отношения к банку.

Следует использовать только надежные официальные каналы связи с кредитно-финансовым учреждением (форму обратной связи на сайте банка, телефоны горячей линии, официальные банковские мобильные приложения).

Необходимо учитывать, что держатель банковской карты обязан самостоятельно обеспечить конфиденциальность ее реквизитов и в этой связи избегать подключения к общедоступным сетям Wi-Fi, использование ПИН-кода или CVV-кода при заказе товаров и услуг через сеть «Интернет» и по телефону, сообщения кодов третьим лицам. В указанных случаях любые банковские операции, выполненные с их использованием, считаются совершенными самим держателем карты и не могут быть опротестованы.

Используйте банкоматы, которые установлены в защищенных местах (например, в госучреждениях, офисов банков). Перед использованием банкомата осмотрите его и убедитесь, что все операции, совершаемые предыдущим клиентом, завершены. Проверьте, что на клавиатуре и в месте для приема карт нет дополнительных устройств. Обращайте внимание на неисправности и повреждения банкомата.

При использовании мобильного телефона при установке приложений обращайте внимание на полномочия, которые они запрашивают, особенно, если они запрашивают доступ к отправке СМС-сообщений и к сети «Интернет».

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

Утратив свои банковские карты, незамедлительно примите меры к блокированию банковских счетов.

Ставьте пароль на свой мобильный телефон. Лучше устанавливать многофакторный пароль, который состоит из цифрового кода и биометрической идентификации.

Ни в коем случае не сообщайте контрольную информацию о своем счете неизвестным и малознакомым лицам, не вступайте в интернет-переписку с посторонними, настороженно относитесь к телефонным звонкам с незнакомых абонентских номеров.

В случае совершенного в отношении вас преступления в целях оказания содействия правоохранительным органам для его раскрытия сохраняйте чеки и смс-сообщения о проведенных банковских операциях с вашими денежными средствами, а также выписки с банковских счетов.

Лучше быть чрезмерно бдительным, чем хорошо обманутым.