«Осторожно, мошенники!»

В условиях развития цифровой экономики, электронных платежных систем персональных электронных устройств и Интернета стремительно возросло количество совершенных с их использованием преступлений.

Совершению данной категории преступлений способствуют доверчивость граждан, недостаточная их осведомленность и пренебрежительное отношение к элементарным правилам безопасности.

Для предупреждения противоправных действий по дистанционному хищению денежных средств важно запомнить следующее.

Сотрудники банка по телефону или в электронном письме не запрашивают:

- персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);
- реквизиты, срок действия, ПИН- и CVV-коды банковских карт;
- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;
- логин и пароль для входа в личный кабинет клиента банка.

Сотрудники банка также не предлагают:

- установить программы удаленного доступа (или иные сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов);
- перейти по ссылке из СМС-сообщения;
- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;
- под их руководством перевести для сохранности денежные средства на «защищённые» или «безопасные» счёта;
- зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Банк может инициировать общение с клиентом только для консультаций по предоставляемым услугам. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на официальных сайтах и банковских документах. Иные номера не имеют никакого отношения к банку.

Чтобы не стать жертвой дистанционного мошенничества следует использовать только официальные каналы связи:

- формы обратной связи на сайте банка и в мобильном приложении;
- телефоны горячих линий;
- группы или чат-боты в мессенджерах (если таковые имеются).

Важно помнить, что мобильные приложения банков следует скачивать через официальные магазины (App Store, Google Play и т.п.).

Необходимо учитывать, что держатель карты обязан самостоятельно обеспечить конфиденциальность ее реквизитов и в этой связи избегать:

- подключения к общедоступным сетям Wi-Fi;
- использования ПИН- или CVV-кодов при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);