**Внимание! Не стань жертвой мошенников!**

Сотрудники банка никогда по телефону или в электронном письме не запрашивают:

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

Сотрудники банка также не предлагают:

* установить программы удаленного доступа на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);
* 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 «защищенный счет»;
* зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Если лица, представившиеся сотрудниками банка, предлагают совершить указанные действия, то, скорее всего, это мошенники, срочно прекратите с ними разговор!

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 карты, на сайте банка или в оригинальных банковских документах.

В случае смены номера мобильного телефона или его утери свяжитесь с банком для отключения и блокировки доступа к СМС-банку и заблокируйте сим-карту, обратившись к сотовому оператору.