!!! Никому не сообщайте коды из SMS для подтверждения операций !!!

!!! Проверяйте адреса страниц в Интернете, на которых производите оплату !!!

!!! никому не сообщайте данные Вашей карты !!!

Если Вам поступил звонок с незнакомого номера, звонящий представляется сотрудником силовых структур или адвокатом, рассказывает, что Ваш родственник или знакомый в беде и срочно нужны деньги, чтобы «решить вопрос с полицией, прокуратурой, судом и т.д.), ни в коем случае не сообщайте звонящему Ваши персональные данные, сведения о хранящихся у Вас ценностях и деньгах (как наличных, так и на счетах банка). В первую очередь примите все меры, чтобы лично связаться с Вашим родственником, другом, его родными и знакомыми. С большой уверенностью можно утверждать, что Вам звонили мошенники! Если Вам не удалось связаться с родственником (другом), обратитесь в полицию!

В случаях, если Вам поступают звонки от имени «банковских работников» или сообщения в социальных сетях и мессенджерах якобы от «банков» либо сотрудников МВД РФ с информацией о финансовых операциях, прекратите разговор и позвоните по горячей линии в банк, либо в дежурную часть ОВД.

Обратите внимание на несколько важных правил работы с интернет-банком и мобильными приложениями.

Банки не используют для проведения консультаций с клиентами приложения: Skype, Viber, WhatsApp и Telegram, данные приложения предназначены только для консультации по продуктам банка. Помните, по каналам Skype,Viber, WhatsApp и Telegram работники банка не запрашивают данные (реквизиты) ваших банковских карт, пароли и коды из СМС!

Для минимизации риска телефонного мошенничества обращаем Ваше внимание, что сотрудники банков:

- не осуществляют звонки с просьбой предоставления персональных данных, номеров карт, одноразовых паролей из СМС для подтверждения финансовых операций;

- не просят коды из СМС для отмены совершённых «мошеннических операций»;

- не предлагают для сохранности перевести деньги на специальные счета или установить специальные программы для обеспечения удалённого доступа и управления компьютерами (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyy Admin, AeroAdmin, Яндекс-деньги, webmoney). Не переходите по ссылкам на незнакомые ресурсы и не устанавливайте программы для удалённого доступа и управления компьютерами, мошенники могут заразить ваш компьютер или телефон вирусом, получить удалённый доступ к Вашим личным данным и финансам.

Не сообщайте незнакомым людям номер своей банковской карты и не передавайте её в руки — в том числе официантам и продавцам.

При поступлении с неизвестных номеров звонков от имени «банковских работников», СМС или иных сообщений от якобы «банка» (например, «Ваша карта заблокирована», «Заблокирована сумма оплаты», «Есть проблемы с проведением операции» и т.п.), ни в коем случае не перезванивайте на указанные в сообщениях номера, не сообщайте данные банковских карт: срок действия, контрольный код с обратной стороны карты, СМС-коды подтверждения, а также персональные данные: серия и номер паспорта, адрес регистрации и пр.