***Следственный комитет в очередной раз напоминает, с целью сохранности денежных средств, хранящихся на банковских картах, необходимо соблюдать ряд простых правил:***

1. никому не сообщайте личные данные, а также реквизиты своей банковской платежной карты (фамилия и имя держателя банковской платежной карты, 16-значный номер банковской платежной карты, который находится на лицевой стороне, срок действия банковской платежной карты, трехзначный код CVC2 (CVV2) на оборотной стороне банковской платежной карты);
2. не предоставляйте третьим лицам, сведения об учетной записи в интернет-банкинге и мобильном банкинге (логин, пароль, сенсорный ключ);
3. при поступлении звонков с «предупреждением» о мошеннических действиях и попытках получить реквизиты карты завершите разговор и перезвоните по официальному номеру контакт-центра банка по номеру, указанному на вашей карте;
4. никогда не вводите данные своей банковской платёжной карты, а также свои личные данные на сомнительных интернет-ресурсах;
5. будьте внимательнее при посещении новых сайтов в глобальной сети Интернет, обратите внимание на его имя в адресной строке браузера, чтобы убедиться, что используете официальный сайт;
6. храните в секрете PIN-код от своей банковской платежной карты;
7. в случае утери банковской платежной карты обратитесь в банк с целью блокировки своей банковской карты.

Следственный комитет в очередной раз призывает граждан быть бдительными и внимательными! Чтобы не стать жертвой подобных преступлений, следователи рекомендуют соблюдать следующие правила:

- не передавайте данные платежных банковских карт в том числе в ходе переписки в интернете или по телефону, третьим лицам;

- не переходите по подозрительным ссылкам и не открывайте подозрительные письма;

- осуществляйте оплату в интернете только на проверенных ресурсах.

Поделитесь данной информацией со своими друзьями, родными и близкими. Не дайте себя обмануть!

В целях предупреждения подобных преступлений следователи рекомендуют:

- для выхода в сеть интернет используйте устройства, на которых установлено специальное программное обеспечение, предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;

- используйте операционную систему с установленными обновлениями безопасности, актуальные версии другого программного обеспечения;

- при использовании известных вам сайтов, обращайте внимание на их внешний вид. Возможно вы зашли на их поддельные копии;

- вводите личную информацию только на веб-сайтах, работающих с использованием защищенных протоколов (обычно в браузере рядом с адресом такого сайта отображается значок замка на зеленом фоне);

- не используйте одинаковые логины и пароли на различных сайтах;

- не используйте слишком простые пароли, либо те, о которых можно легко догадаться (даты рождения, номера телефонов и т.д.);

- по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо вводить временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;

- остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;

- с осторожностью относитесь к письмам, в которых запрашиваются данные счетов (финансовые учреждения почти никогда не запрашивают финансовую информацию по электронной почте), никогда не отправляйте финансовую информацию по незащищенным интернет-каналам;

- при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно проверяйте данную информацию с использованием других каналов связи (личная встреча, телефонный звонок, мессенджер, поддерживающий голосовую связь). В крайнем случае идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам;

- если не используете банковскую платежную карточку для осуществления интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;

- при осуществлении интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности платежей, такие как 3-D Secure для международных платежных систем Visa и MasterCard или интернет пароль для платежной системы БЕЛКАРТ.

В случае совершения в отношении вас противоправных деяний, незамедлительно обращайтесь в органы внутренних дел по месту жительства, либо по месту обнаружения факта совершения преступления.