**Памятка**

**по предупреждению хищений денежных средств с банковских карт**

Напоминаем, как защититься от хищения денежных средств с карты:

* Необходимо знать, что сотрудники банка и правоохранительных органов (следователи, дознаватели, оперуполномоченные и т.д.) никогда по телефону или в электронном письме; **не запрашивают:**

персональные сведения (серия и номер паспорта, 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-код банковских карт.

Если собеседник запрашивает данные сведения, не следует их предоставлять.

* Помните, что сотрудники банка и правоохранительных органов (следователи, дознаватели, оперуполномоченные и т.д.) также **не предлагают:**

установить программы удаленного доступа (или сторонние приложения) 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 собеседник предлагает совершить указанные действия, не следует их выполнять.

* Банк может инициировать общение с клиентом для консультаций по продуктам и услугам кредитно-финансового учреждения. При этом звонки совершаются с номеров, указанных на официальном сайте банка или в оригинальных банковских документах.

Следует использовать **только надежные официальные каналы связи** с кредитно-финансовым учреждением. В частности, форму обратной связи на сайте банка, онлайн-приложения, телефоны горячей линии, а также официальные банковские приложения.

* Совершая операции, не прислушивайтесь к советам незнакомых людей и не принимайте их помощь.
* Обращаю ваше внимание на необходимость использования только проверенных сайтов, внимательного прочтения текстов СМС-сообщений с кодами подтверждений, проверки реквизитов операции.
* 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.
* При возникновении подозрений насчет предпринимаемых попыток совершения мошеннических действий следует **незамедлительно прекратить** телефонный разговор с собеседником, обратиться по надежным официальным каналам связи или путем личного обращения в банк, а также в правоохранительные органы.

Прокурор Могойтуйского района А.А. Бадмаев