ПАМЯТКА о мерах по предупреждению хищений денежных средств с банковских счетов, при использовании банковских карт.

Вариантов совершения мошеннических действий достаточно много, постоянно появляются новые – это телефонный звонок сотрудникам банка, потенциального « покупателя» с предложением пройти к ближайшему банкомату и совершить манипуляции с банковской картой во избежание каких либо негативных последствий и т.д.

Наиболее популярные способы мошенничества с банковскими картами: - СМС сообщения или телефонный звонок о блокировке банковской карты или несанкционированном списании денежных средств со счета и т.п, с требованием перейти по ссылке, перезвонить по указанным телефону или сообщить данные банковской карты

- телефонный звонок «работника службы безопасности банка» с обеспокоенностью тем, что с вашего счета совершен подозрительный денежный перевод на адрес определённого человека и для сохранения денежных средств, лжеработнику банка необходимо совершить какие то действия, а для этого ему необходимо сообщить данные свое банковской карты.

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 – кодбанковских карт.

Сотрудники банка 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,

При использовании мобильного телефона соблюдайте следующие правила:

при установке приложений обращайте внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к сети «Интернет»;

отключите в настройках возможность использования голосового управления при заблокированном экране.

Применяя сервисы СМС-банка, сверяйте реквизиты операции в СМСсообщении с одноразовым паролем от официального номера банка. Если реквизиты не совпадают, то такой пароль вводить нельзя.

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. Иные номера не имеют никакого отношения к банку.

Следует использовать только надежные официальные каналы связи с кредитно-финансовым учреждением. В частности, форму обратной связи на сайте банка, онлайн-приложения, телефоны горячей линии, группы или чатботы в мессенджерах (если таковые имеются), а также официальные банковские приложения из магазинов App Store, Google Tay, MicrosoR Store,

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

- подключения к общедоступным сетям Wi-Fi;
- использования ПИН-кода или CVV-кода при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);
- сообщения кодов третьим лицам (в противном случае любые операции, совершенные с использованием ПИН-кода или CVV-кода, считаются выполненными самим держателем карты и не могут быть опротестованы).

При оплате услуг картой в сети «Интернет» (особенно при привязке к регулярным Платежам или аккаунтам) требуется всегда учитывать высокую вероятность перехода на поддельный сайт, созданный мошенниками для компрометации клиентских данных, включая платежные карточные данные. Поэтому необходимо использования только проверенных сайтов, внимательного прочтения текстов СМС-сообщений с кодами подтверждений, проверки реквизитов операции.Для минимизации возможных хищений при проведении операций с использованием сети «Интернет» рекомендуется оформить виртуальную карту с установлением размера индивидуального лимита, ограничивающего операции для данного вида карты, в том числе с использованием других банковских карт, выпущенных на имя держателя карты.

Когда банк считает подозрительными операции, которые совершаются от имени клиента, он может по своей инициативе временно заблокировать доступ к сервисам СМС-банка и онлайн-кабинета. Если операции совершены держателем карты, для быстрого возобновления доступа к денежным средствам достаточно позвонить в контактный центр банка.

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 малейших подозрений насчет предпринимаемых попыток совершения Мошеннических действий следует незамедлительно уведомлять об этом банк.

Будьте бдительны!