-ния банкоматов

Совершая операции, не прислушивайтесь к советам незнакомых людей и не принимайте их помощь.

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

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 обращайте Ваше внимание на необходимость использования только проверенных сайтов, внимательного прочтения текстов СМС-сообщений с кодами подтверждений, проверки реквизитов операции.

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.

Прокуратура Карагайского района Пермского края
с. Карагай, ул. К. Маркса, д. 22, Пермский край, 617210

Прокуратура Карагайского района Пермского края

Как не стать жертвой преступлений и предупредить хищения с банковских карт

2021 г.

Реалии нашей жизни свидетельствуют о всё возрастающем числе хищений денежных средств с банковских карт, чему способствует недостаточная осведомленность граждан в области информационных технологий и пренебрежительное отношение к элементарным правилам безопасности.

В целях предотвращения противоправных действий по снятию денежных средств с банковского счета необходимо исходить из следующего.

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

- персональные сведения (серия и номер паспорта, адрес регистрации, ФИО 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.

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 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.

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 чат-боты, в мессенджерах (если таковые имеются), а также официальные банковские приложения из магазинов App Store, Google Play, Microsoft 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 иди 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 использовании банкоматов отдавайте предпочтение тем, которые установлены в защищенных местах (например, в госучреждениях, офисах банков, крупных торговых центрах).

Перед использованием банкомата осмотрите его и убедитесь, что все операции, совершаемые предыдущим клиентом, завершены; что на клавиатуре и в месте для приема карт нет дополнительных устройств; обращайте внимание на неисправности и поврежде-