«Осторожно, мошенники!»

В условиях развития цифровой экономики, электронных платежных систем персональных электронных устройств и Интернета стремительно возросло количество совершенных с их использованием преступлений.

Совершению данной категории преступлений способствуют доверчивость граждан, недостаточная их осведомленность и пренебрежительное отношение к элементарным правилам безопасности.

Для предупреждения противоправных действий по дистанционному хищению денежных средств важно запомнить следующее.

Сотрудники банка по телефону или в электронном письме не запрашивают:

- персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);
- реквизиты, срок действия, ПИН- и CVV-коды банковских карт;
- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;
- логин и пароль для входа в личный кабинет клиента банка.

Сотрудники банка также не предлагают:

- установить программы удаленного доступа (или иные сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов);
- 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 «защищённые» или «безопасные» счёта;
- зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Банк может инициировать общение с клиентом только для консультаций по предоставляемым услугам. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на официальных сайтах и банковских документах. Иные номера не имеют никакого отношения к банку.

Чтобы не стать жертвой дистанционного мошенничества следует использовать только официальные каналы связи:

- формы обратной связи на сайте банка и в мобильном приложении;
- телефоны горячих линий;
- группы или чат-боты в мессенджерах (если таковые имеются).

Важно помнить, что мобильные приложения банков следует скачивать через официальные магазины (App Store, Google Play и т.п.).

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

- подключения к общедоступным сетям Wi-Fi;
- использования ПИН- или CVV-кодов при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);

- сообщения названных кодов третьим лицам (в противном случае любые операции, совершенные с их использованием, считаются выполненными самим держателем карты и не могут быть опротестованы).

При использовании банкоматов отдавайте предпочтение тем, которые установлены в защищённых местах (например, в госучреждениях, офисах банков, крупных торговых центрах). Перед его использованием, осмотрите и убедитесь, что:

- все операции, совершаемые предыдущим клиентом, завершены;
- на клавиатуре и в месте для приема карт нет дополнительных устройств;
- отсутствуют неисправности и иные повреждения.

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

При использовании сотовых телефонов (смартфонов) соблюдайте следующие правила:

- при установке мобильных приложений обращайте внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и иных уведомлений, доступ к сети «Интернет»;
- отключите в настройках возможность использования голосового управления при заблокированном экране;
- не переходите по ссылкам из СМС-уведомлений, различных чатов и мессенджеров, не убедившись в их достоверности (перезванивайте людям их прислав шим);
- не перечисляйте денежные средства знакомым, родственниками и близким лицам на их просьбы о переводе денежных средств из СМС-уведомлений, различных чатов и мессенджеров, не убедившись в их достоверности (перезванивайте людям их прислав шим);

При использовании интернет-сервисов, в то числе для покупки и продажи товаров и оказания услуг (Авито, Юла и т.п.) запомните ряд простых правил:

- используйте средства общения, предоставленные данными сайтами;
- не переходить на «индивидуальное» общение с посторонними лицами с использованием личных номеров телефонов;
- не передавайте свои персональные данные, в том числа адрес проживания, контактные телефоны, банковские реквизиты и коды подтверждения банковских операций;
- используйте только порядок и формы оплаты, получения товаров, предусмотренные данными интернет-сервисами.

При оплате товара и услуг в сети «Интернет» (особенно при привязке к регулярным платежам или аккаунтам) требуется всегда учитывать высокую вероятность перехода на поддельный сайт, созданный для компрометации клиентских данных, включая платежные карточные данные.

Для минимизации возможных хищений при проведении операций с использованием сети «Интернет» рекомендуется:

- оформить виртуальную карту с установлением размера индивидуального лимита, ограничивающего операции, в том числе с использованием других банковских карт;
- внимательно читать тексты СМС-сообщений и иных уведомлений с кодами подтверждений, проверять реквизиты операций. Если реквизиты не совпадают, то такой пароль вводить нельзя.

Когда банк считает совершаемые от имени клиента операции подозрительными, 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 утери или смены номера телефона, привязанного к банковской карте, необходимо:

- связаться с банком для отключения услуги СМС-уведомления;
- заблокировать сим-карту, обратившись к сотовому оператору.

При возникновении малейших подозрений насчет предпринимаемых попыток совершения мошеннических действий следует незамедлительно уведомлять об этом банк.

Соблюдение приведенных мер и рекомендаций позволит предотвратить случаи дистанционного хищения денежных средств.