

Военно-градская обл. Котляри-Ковал 13. А.



Примите участие в конкурсе
создайте свой проект
19.01.21



630022459271

Генеральная прокуратура
Российской Федерации

Ул. Е. Дмитриева, 15а
Москва, Россия, ГСН-3, 125993

Прокурорам субъектов Российской Федерации, приравненным к ним специализированным прокурорам, прокурору комплекса «Байконур», ректору Университета прокуратуры Российской Федерации

23.12.2020 № 66-05/2020

ПАМЯТКА

О мерах по предупреждению хищений денежных средств при использовании банковских карт

В Генеральной прокуратуре Российской Федерации проанализированы специальные донесения о фактах хищений денежных средств с банковских карт работников органов прокуратуры Российской Федерации.

Результаты анализа свидетельствуют о возросшем числе поданных преступлений, которыми, как показывает практика, способствуют недостаточная осведомленность прокурорских работников в области информационных технологий и пренебрежительное отношение к элементарным правилам безопасности.

Для 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, 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.

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 передачу информации на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;

под их руководством перевести для сохранения денежные средства на «защитенный счет»;

Генеральная прокуратура Российской Федерации
Москва
№ 66-05-2020/ИИ-24610-20

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, 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 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 оспорены).

При использовании банкоматов отдавайте предпочтение тем, которые установлены в защищенных местах (например, в государственных, 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; обратите внимание на исправности и повреждении.

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

При использовании мобильного телефона соблюдайте следующие правила:

при установке приложений обращайтесь 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, сверьте реквизиты операции в СМС-сообщении 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 обращайтесь ваше внимание на необходимость использования только проверенных сайтов, внимательного прочтения текстов СМС-сообщений с кодами подтверждения, 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, выданных 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 уведомить об этом банк.

В связи с изложенным предлагаем неукоснительно соблюдать приведенные в настоящей памятке меры и рекомендации.

Заместитель Генерального прокурора
Российской Федерации

Г.Б. Лопатин