- 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 приславшим);
- 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 приславшим);

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: