Рекомендации по безопасному использованию банковских карт

1. Общие меры безопасности

- После получения карты поставьте свою подпись на специальной полосе для подписи, расположенной на оборотной стороне карты.

При отсутствии подписи карта может быть не принята к оплате в торгово-сервисном предприятии за границей, а также повышается риск использования карты злоумышленниками в случае ее утраты или кражи.

- Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям.

Храните карту в безопасном месте, не оставляйте её без присмотра (в автомобиле, в номере гостиницы, в иных местах, где посторонние лица могут воспользоваться Вашей картой).

- Для минимизации рисков финансовых потерь установите ограничения (лимиты) по суммам и количеству операций по карте.

- Не передавайте карту другим лицам, в т.ч. родственникам и знакомым.

С целью исключения Ваших потерь от несанкционированного использования Вашей карты при совершении операции оплаты, никогда не выпускайте карту из поля зрения и требуйте от сотрудников торгово-сервисных предприятий, чтобы все операции с использованием карты совершались в Вашем присутствии.

- Подключите услугу «SMS-уведомление» и контролируйте проведение операций по вашим счетам.

Не оставляйте мобильный телефон без присмотра или выключенным на долгое время. В случае утраты мобильного телефона срочно заблокируйте сим-карту телефона.

- Если на ваш мобильный телефон или e-mail пришло сообщение о блокировке карты, выигрыше по карте или о списании/зачислении суммы, о которой вам ничего не известно, не звоните по номерам телефонов и не переходите по ссылкам, указанным в сообщении.

Не проводите никаких действий с картой и не сообщайте ее CVV2/CVC2, срок действия, данные получаемых SMS-уведомлений (3D-Secure), лицам, представляющимися сотрудниками Банка или правоохранительных органов.

В разговоре с Клиентом, сотрудник Банка никогда не просит назвать реквизиты карты (за исключением последних 4-х цифр номера карты, ФИО, кодовое слово).

Любую информацию уточняйте только через Call-центр ООО «Инбанк».

- Контакты Call-центра ООО «Инбанк» указаны на обратной стороне банковской карты ООО «Инбанк», а также на официальном сайте Банка https://www.in-bank.ru
- Запишите телефонные номера Call-центра и всегда имейте эту информацию при себе, хранящейся отдельно от карты. Она может понадобиться Вам для экстренной блокировки Вашей карты, если карта будет утеряна или украдена.
- В случае утери, кражи или компрометации банковской карты, незамедлительно обратитесь в Call-центр ООО «Инбанк» и заблокируйте карту.

2. ПИН-код и как обеспечить его конфиденциальность

ПИН-код – это *персональный идентификационный номер* держателя банковской карты, удостоверяющий право распоряжения денежными средствами на счете. ПИН- код состоит из четырех цифр.

При совершении операций в банкоматах ПИН-код является аналогом собственноручной подписи держателя карты. Операции, совершенные с его использованием, считаются разрешенными держателем карты.

Обеспечить конфиденциальность Вашего ПИН-кода поможет следование следующим рекомендациям:

- ни в коем случае не сообщайте Ваш ПИН-код, а также место, где он может храниться другим лицам, в т.ч. близким родственникам, знакомым, сотрудникам Банка. Помните, что владельцем карты являетесь Вы и только Вы несете персональную ответственность за все операции, совершенными с использованием Вашей карты;

- категорически запрещается записывать ПИН-код на карте и/или хранить карту вместе с листком, на котором указан ПИН-код. При необходимости, ПИН-код можно сменить в банкомате;

- при вводе ПИН-кода не допускайте, чтобы кто-либо наблюдал за Вами. Для исключения возможности компрометации Вашего ПИН-кода при помощи видеокамер, установленных/используемых в мошеннических целях, рекомендуется при вводе ПИН-кода прикрывать клавиатуру банкомата рукой;

- дверь в помещение, где расположен банкомат, может быть оборудована электронным замком, открываемым с помощью карты. Помните, что он должен открываться без ввода ПИН-кода. Если Вам предлагают ввести ПИН- код, то перед вами устройство, установленное мошенниками;

- никогда не сообщайте свой ПИН-код при совершении операций по карте через сайты сети Интернет, при опросах/ информировании по телефону, электронной почте и т.д., в том числе лицам, представляющимися сотрудниками Банка. О попытках узнать Ваш ПИН-код, сообщайте в Call-центр ООО «Инбанк»;

- ПИН-код не подлежит восстановлению. Он генерируется в случайном порядке и не сохраняется в информационной системе Банка. Если Вы забыли ПИН-код, карту необходимо перевыпустить. Если Вы заблокировали карту, трехкратно набрав неправильный ПИН-код, обратитесь в Call-центр ООО «Инбанк».

3. Рекомендации по соблюдению безопасности при использовании банковских карт

3.1. На мобильном устройстве

- Рекомендуем отключить в настройках телефона/планшета возможность чтения SMS на заблокированном экране, а также использование голосовых помощников при заблокированном устройстве.

- Используйте мобильное приложение, которое необходимо устанавливать только из официальных магазинов приложений - Google Play или App Store.

- В случае утери или кражи устройства с привязанными банковскими картами (токенами), необходимо заблокировать эти карты, обратившись в Call-центр ООО «Инбанк».

- Не храните в устройстве данные по картам в явном виде, а также не передавайте устройства третьим лицам, никому не сообщайте пароли для разблокировки устройств.

3.2. При работе с банкоматами

- При выборе банкомата, в котором Вы собираетесь провести операцию с использованием банковской карты, желательно избегать плохо освещенных и безлюдных мест.

Для получения наличных средств безопаснее пользоваться банкоматами, расположенными в отделениях известных банков, крупных торговых центрах, госучреждениях.

- Осмотрите банкомат перед использованием на предмет наличия посторонних устройств на клавиатуре и месте приема карт.

- Не используйте банкомат в присутствии подозрительных лиц и не принимайте помощь от незнакомцев (даже если у Вас застряла карточка или возникли проблемы с проведением операции).

- При вводе ПИН-кода всегда закрывайте рукой клавиатуру.

- Не отвлекайтесь, пока не получите деньги и карту из банкомата.

Мошенники в момент выдачи денежных средств могут отвлечь держателя карты, тем самым давая возможность другому мошеннику, стоящему рядом, забрать денежные средства, выданные банкоматом.

- В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от его использования, отменить совершаемую операцию, нажав на клавиатуре соответствующую кнопку, и дождаться возврата банковской карты.

- Если банкомат изъял карту, немедленно заблокируйте ее, обратившись в Call-центр ООО «Инбанк».

Для получения вашей карты, изъятой банкоматом Вам необходимо обратиться в банк, обслуживающий банкомат, по номеру телефона указанному на банкомате.

- Если денежные средства полностью или частично не выданы/не внесены в банкомат, то необходимо обратиться в Call-центр ООО «Инбанк».

3.3. При оплате через терминалы

- Не упускайте карту из виду, настаивайте на проведении всех операций только в Вашем присутствии.

- Убедитесь, что сумма, отображаемая на терминале соответствует сумме вашей покупки.

- Сохраняйте все документы по проведенным операциям, в том числе и по неуспешным. При неуспешной попытке оплаты по карте требуйте чек с отказом. Если чек не распечатан, требуйте, чтобы отказ был подтвержден письменно.

- Не используйте карту для оплаты, если кассир или торговая точка не вызывают у Вас доверия.

3.4. При оплате в Интернете

- Для оплаты товаров и услуг в сети Интернет выпустите виртуальную карту или используйте отдельную банковскую карту, предназначенную только для данной цели. Установите лимиты по сумме и количеству операций в сети Интернет по этой карте.

- Совершайте покупки только со своего компьютера, не пользуйтесь Интернет-кафе и другими общедоступными WiFi-сетями, где могут быть установлены программы-шпионы, запоминающие вводимые Вами конфиденциальные данные.

Установите на свой компьютер лицензионное программное обеспечение, в том числе антивирусное, и регулярно производите его обновление. Это поможет защитить Ваш компьютер от вирусов и других деструктивных программ, а также от несанкционированного доступа к Вашим персональным данным.

- Убедитесь в правильности адресов Интернет-сайтов, к которым подключаетесь для совершения покупки, так как похожие адреса могут использоваться для осуществления неправомерных действий. Если есть какие-либо подозрения относительно Интернет-страницы или Вы не хотите предоставлять персональные данные, то покиньте страницу, произведите покупку в другом месте.

- При проведении операций в Интернет-магазинах проконтролируйте, что магазин имеет опубликованные обязательства по защите данных клиента, и на сайте присутствуют контактные данные организации. По возможности убедитесь в правильности адреса и телефона, указанных на сайте.

- Пользуйтесь проверенными интернет-магазинами, в надежности, которых вы уверены.

Один из способов получения реквизитов карт, используемых мошенниками, заключается в создании «поддельного» интернет-магазина, где данные карты могут быть скомпрометированы.

- При обращении к сайту интернет-магазина, необходимо убедиться, что в начале адресной строки браузера, перед адресом https://*******.ru, расположена иконка с изображением замка 🔒, означающего, что подлинность сайта подтверждена и соединение защищено.

- Для обеспечения безопасного проведения интернет-операций рекомендуем проводить платежи на сайтах, поддерживающих технологию безопасности 3D-Secure.

- Если Вами было произведено бронирование гостиницы через Интернет-сайт, но по каким-то причинам Вы не планируете воспользоваться ею, обязательно проведите отмену бронирования через тот же Интернет-сайт согласно указанным на нем процедурам.

3.5. Использование банковских карт за пределами РФ

Прежде чем отправиться в заграничную поездку:

- проверьте срок действия Вашей карты;
- проверьте доступный остаток средств на Вашей карте, чтобы точно знать, на какую сумму Вы можете рассчитывать, и заранее пополните свой счет в случае необходимости;
- убедитесь в том, что Вы хорошо помните свой ПИН-код, но ни в коем случае не пишите ПИН-код на карте;
- в странах Азиатско-Тихоокеанского региона (Малайзия, Таиланд, Сингапур, Тайвань, Филиппины, Индонезия, Шри-Ланка, Индия и др.), Африки (ЮАР), Центральной и Южной Америки (Мексика, Доминиканская Республика, Аргентина, Бразилия, Перу) рекомендуется по возможности использовать бесконтактные платежи. В этих странах высок риск копирования данных Вашей карты и изготовления ее дубликата. Для снятия наличных денежных средств рекомендуется использовать банкоматы известных банков, которые установлены в отделениях и крупных торговых центрах.