ТЕКСБАНК

ПАМЯТКА КЛИЕНТА
по безопасному использованию банковских интернет-технологий

Уважаемые клиенты АО АКБ «ТексБанк»!

Согласно рекомендациям Банка России (письмо от 25.06.2009 № 76-Т) сообщаем о появлении в российском сегменте сети Интернет Web-сайтов, имитирующих интернет-представительства ряда российских кредитных организаций. Доменные имена и стиль оформления таких сайтов, как правило, сходны с именами подлинных Web-сайтов банков, а содержание прямо указывает на их якобы принадлежность соответствующим кредитным организациям. При этом посетителям таких сайтов сообщаются заведомо ложные банковские реквизиты и контактная информация. Использование подобных реквизитов, а также вступление в какие-либо деловые отношения с лицами, фактически представляющими ложные банки, связано с риском и может привести к нежелательным последствиям для клиентов кредитных организаций.

В связи с вышеизложенным, приводим контакты АО АКБ «ТексБанк» в сети Интернет:
Официальный сайт АО АКБ «ТексБанк»: www.texbank.ru
Администратор официального сайта АО АКБ «ТексБанк»: mailbox@texbank.ru
Служба персонала АО АКБ «ТексБанк»: personal@texbank.ru

Также обращаем Ваше внимание, что список адресов (доменных имен) официальных Web-сайтов кредитных организаций размещен на Web-сайте Банка России по адресу: http://cbr.ru/credit/CO_sites.asp.

В случае самостоятельного выявления клиентами ложных Web-сайтов банка, а также получения информации о них по электронной почте или иным способом просим сообщать о полученных сведениях Администратору официального сайта АО АКБ «ТексБанк» по адресу: mailbox@texbank.ru.

Также при пользовании банковским услугами в сети Интернет рекомендуем Вам соблюдать следующие правила безопасности

Общие рекомендации:

- Используйте на компьютере только лицензионное программное обеспечение.
- Работайте под учетной записью обычного пользователя. Используйте администраторские права только при необходимости. Отключите стандартную учетную запись «Гость».
- Используйте надежные, сложные пароли, содержащие различные буквы, цифры и спецсимволы (например, знаки препинания), а также сочетания заглавных и строчных букв. Рекомендуемая длина пароля – не менее 8 символов. Не используйте учетные записи с «пустыми» паролями.
- Своевременно обновляйте операционную систему.
- Установите и своевременно обновляйте на компьютере современное антивирусное программное обеспечение.
- Проводите полную еженедельную проверку компьютера на наличие вирусов.

- Установите и настройте на компьютере персональный межсетевой экран, разрешив доступ только к доверенным ресурсам сети Интернет.
- Не используйте функцию автозаполнения полей формы на сайте (логина, имени пользователя и пароля).

При работе с веб-сайтами:

- Убедитесь, что вы находитесь на подлинном сайте, так как злоумышленники могут использовать похожие названия для создания мошеннических ресурсов. В поле «адрес» браузера должен быть именно тот адрес сайта, который Вам нужен. Обратите пристальное внимание на написание похожих по начертанию символов в адресе.
- Избегайте пользоваться услугами Интернет-ресурсов сомнительного содержания; зачастую они создаются специально для получения информации о банковских картах и последующего ее неправомерного использования. Если при посещении сайта торговой компании у Вас возникли сомнения в надежности торговца, не предоставляйте ему информации о Вашей карте и Ваши персональные сведения, покиньте страницу, произведите покупку в другом месте. Не оставляйте реквизиты Вашей банковской карты на незнакомых или сомнительных сайтах.
- Будьте внимательны: сайты могут использоваться мошенниками в целях получения конфиденциальной информации (для заказа товара/услуги клиентам предлагается заполнить электронные формы и указать реквизиты банковских счетов, карт, включая ПИН-код, что категорически запрещено).
- Осуществляйте передачу конфиденциальной информации только через сайты, работающие в защищенном режиме. Для этого убедитесь, что в правом нижнем углу или рядом с адресной строкой браузера есть символ замка. Этот символ означает, что Ваши данные в процессе передачи будут защищены.
- Если при входе на защищенный сайт Вы получаете предупреждение браузера об ошибках в работе системы защиты сайта, то передавать конфиденциальную информацию через такой сайт небезопасно.
- Завершайте работу в платежных системах корректно, согласно инструкции по работе с системой.

При работе с электронной почтой:

- Не открывайте письма и вложения к ним, полученные от неизвестных отправителей.
- Не отвечайте на сообщения электронной почты с запросами Ваших личных данных (например, номера паспорта, номера банковской карты, ПИН-кода к ней, паролей и т.д.).
- Не переходите по содержащимся в сомнительных письмах ссылкам. Ссылки в сообщениях электронной почты могут открывать совсем другие сайты.
- Отправляйте конфиденциальную информацию по электронной почте в зашифрованном виде, так как обычные сообщения электронной почты не шифруются в процессе передачи и могут быть доступны третьим лицам, и использованы для нанесения Вам вреда.
- В случае необходимости передать свою конфиденциальную информацию доверенному получателю по электронной почте используйте средства криптографической защиты информации.

При использовании банковской карты

- Ни при каких обстоятельствах не сообщайте ПИН-код карты другим лицам, в том числе сотрудникам банка, и не вводите его на сайтах. ПИН-код должен быть известен только Вам, и может быть затребован только при совершении Вами операций на банкоматах, электронных терминалах банка и торгово-сервисных учреждений. Никогда не пишите ПИН-код на Вашей банковской карте.
- Не передавайте Вашу конфиденциальную информацию (паспортные данные, номер банковской карты и счета, пароли и т.д.) позвонившим Вам людям, вне зависимости от того, сотрудниками какой организаций они себя выдают.
- Для оплаты покупок в сети Интернет лучше использовать специальную банковскую карту (с отдельным счетом или ограниченным лимитом), предназначенную только для данной цели. Денежные средства на нее рекомендуется переводить непосредственно перед намерением совершить покупку в объеме немногим больше планируемых расходов.
- Не применяйте банковскую карту для покупок через сайты, не использующие специальные программные средства для защиты информации о банковской карте. Безопасные сайты отмечены знаком в виде закрытого замка.
- Пользуйтесь услугами только известных и проверенных торговых компаний. Предпочтение необходимо отдавать предприятиям, сайты которых подключены к программам Verified by Visa (Проверено Визой) и SecureCode (Безопасный Код) – в этом случае на сайтах будет размещена текстовая или символьная информация о сотрудничестве с международными платежными системами Visa и Mastercard. Убедитесь, что у Вас есть возможность связаться с торговцем в случае спорной ситуации или вопроса. Убедитесь в правильности контактной информации, приведенной на странице. Убедитесь, что магазин имеет опубликованные обязательства по защите данных клиента.
- Совершайте покупки только со своего компьютера, не пользуйтесь Интернет-кафе и другими бесплатными точками доступа в сеть Интернет, где могут быть установлены программы-шпионы, запоминающие вводимые Вами конфиденциальные данные.
- Всегда контролируйте Ваши операции, проверяя выписки по банковским картам.
- Подключитесь к системе информирования об операциях с банковской картой на мобильный телефон при помощи SMS-сообщений. Это позволит Вам быть в курсе всех покупок по карте, в том числе - несанкционированных Вами операций. В последнем случае вы сможете оперативно заблокировать карту. В случае обнаружения факта несанкционированного доступа к Вашему карточному счету через Интернет, необходимо подать соответствующее заявление в банк. После этого банк сможет представлять Ваши интересы в Международной Платежной Системе по вопросу возврата несанкционированно списанной суммы.
- Правильно уничтожайте бумажные и электронные носители информации, которые содержат Ваши конфиденциальные данные.
- Используйте для связи с банком только телефонные номера, указанные на официальном сайте банка www.texbank.ru.

Администрация АО АКБ «Тексбанк»