

Предупреждающая информация

**Уважаемые Клиенты!
Владельцы банковских карт КБ «РМБ» ЗАО и**

пользователи систем дистанционного банковского обслуживания!

Одним из приоритетов в области обслуживания наших Клиентов и предоставления сервисов дистанционного банковского обслуживания (ДБО), КБ «РМБ» ЗАО считает обеспечение безопасного проведения операций при пользовании банковскими картами КБ «РМБ» ЗАО, а также выполнения операций с использованием сети Интернет.

В последнее время участились случаи мошенничества, связанных с причинением материального ущерба клиентам различных кредитных организаций – пользователям банковских карт и систем ДБО.

В связи с этим КБ «РМБ» ЗАО считает необходимым обратить внимание всех своих Клиентов на меры предосторожности, которые необходимо соблюдать, чтобы не стать жертвой мошенников и избежать возможных негативных последствий, связанных с использованием банковских карт и систем ДБО:

1. Необходимо исключить возможность неправомерного получения Вашей персональной информации – не передавайте ее посторонним лицам.
2. Не используйте банковские карты в организациях торговли и сервиса, не вызывающих доверия.
3. При совершении операций с банковской картой без использования банкомата не выпускайте ее из поля зрения.
4. Не пользуйтесь устройствами, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.
5. Не используйте ПИН-код при заказе товаров или услуг по телефону/факсу или по сети Интернет.
6. Пользуйтесь услугой SMS-информирования о проведенных операциях с вашим банковским счетом.

ВНИМАНИЕ!

Никогда не вводите ПИН-коды для своих банковских карт при любых операциях в сети Интернет. Для проведения интернет-транзакции ПИН-код не требуется. Пользуйтесь только теми web-сайтами, которым Вы доверяете!

Никогда не отвечайте на сообщения, полученные по электронной почте или SMS, в которых под какими-либо предложениями (техническое перевооружение, обновление программного обеспечения или сверка баз данных и т.п.) предлагается отправить по SMS или ввести с клавиатуры компьютера ваши персональные данные (ФИО, номера банковских карт, ПИН-коды CVC/CVV коды и т.п.).

При утере, краже карты, во избежание возможности ее использования третьими лицами необходимо немедленно позвонить в круглосуточную службу поддержки клиентов и заблокировать карту по телефону, указанному на обратной стороне карты – 7 (495) 232-37-23. Блокировка карты производится после идентификации по кодовому слову.

Сообщаем Вам список стран наиболее подверженных мошенническим операциям при использовании банковских карт: Тайланд, Шри-Ланка, Болгария, Турция, Украина, Испания, Франция, Италия.

Отмечаются также случаи неправомерного получения реквизитов банковских карт при проведении операций через банкоматы. Мошенники могут использовать накладные устройства на клавиатуру банкомата и на устройство для приема карт (картридер).

Накладка на клавиатуру



Накладка на картридер



Кроме этого, мошенники могут использовать даже "фальшивые" банкоматы. Данные банкоматы незаконно устанавливаются, как правило, в неконтролируемых кредитными организациями местах и внешне не отличаются от настоящих.

ВНИМАНИЕ!

Обращайте внимание на наличие посторонних устройств на клавиатуре и картридере банкомата. Нормальная клавиатура обычно не отличается по уровню естественного износа от прочих частей банкомата.

Фальшивая – выглядит, как правило, более новой. По возможности, не пользуйтесь банкоматом, вызывающим сомнения!

Старайтесь пользоваться банкоматом, установленным в КБ «РМБ» ЗАО, либо в других вызывающих доверие местах (государственные учреждения, крупные торговые центры, аэропорты, гостиницы и т.п.)

БЕЗОПАСНОСТЬ ПРИ РАБОТЕ В ИНТЕРНЕТЕ

1. Убедитесь, что Ваш компьютер не заражён какими-либо вирусами. Установите и активизируйте антивирусные программы, старайтесь их постоянно обновлять. Только постоянное обновление антивирусных программ позволит Вам своевременно обнаружить и предотвратить появление вируса.
2. Рекомендуется использовать программное обеспечение, которое отслеживает и борется с программным обеспечением Spyware. Spyware — вид программного обеспечения, который пытается запомнить Ваши клавиатурные последовательности и передать их третьим лицам.
3. Рекомендуется использовать межсетевой экран (firewall) при входе в Интернет или установить персональный межсетевой экран (firewall) на Вашем компьютере. При использовании межсетевого экрана (firewall) несанкционированный вход в систему Вашего компьютера через Интернет будет весьма затруднен или предотвращён.
4. Используйте программное обеспечение (операционные системы, приложения) из проверенных и надёжных источников. Откажитесь от использования и инсталляции программного обеспечения из непроверенных источников.
5. В случае подключения через модем обратите, пожалуйста, внимание на набираемый номер. В случае обнаружения несовпадения номера удалите неизвестный Вам номер.
6. Сконфигурируйте Ваш обозреватель таким образом, чтобы установки настройки кэширования не допускали сохранения конфиденциальных страниц (SSL-page).
7. Контролируйте свою электронную почту, не открывайте сообщения от неизвестных адресатов, не передавайте свои личные данные. Никогда не открывайте подозрительные файлы, присланные вам по электронной почте. Не отвечайте на электронные письма, в которых якобы от имени Банка, Вас просят предоставить персональную информацию. Никогда не следуйте по ссылкам в таких письмах (даже на сайт банка), т.к. они могут вести на мошеннические сайты.
8. Проверяйте адреса Интернет-сайтов, к которым вы подключаетесь, т.к. злоумышленники могут использовать похожие названия для создания мошеннических ресурсов.
9. Избегайте пользоваться услугами Интернет-ресурсов сомнительного содержания; зачастую они создаются специально для получения информации о банковских картах и последующего ее неправомерного использования.
10. Совершайте покупки только со своего компьютера, не пользуйтесь Интернет-кафе и другими доступными средствами, где могут быть установлены программы-шпионы, запоминающие вводимые вами конфиденциальные данные.
11. Выбирайте нетривиальные пароли, которые не связаны с вашим днем рождения или другими персональными данными. Если возможно, выбирайте символично-цифровые пароли. Не записывайте пароли и никому не сообщайте их. Если Вы боитесь забыть свой пароль, придумайте понятную только Вам систему его записи (например, в виде номера телефона или адреса в телефонной книжке).