Памятка Клиента при совершении операций с использованием банковской карты ПС «МИР» в информационно-телекоммуникационной сети «Интернет»

При работе в информационно-телекоммуникационной сети «Интернет» рекомендуется соблюдать общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на компьютерах.

Установить и своевременно обновлять на компьютере антивирусное ПО.

Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.

При выходе в информационно-телекоммуникационную сеть «Интернет» использовать сетевые экраны, разрешив доступ только к доверенным ресурсам Сети.

При работе в информационно-телекоммуникационной сети «Интернет» не соглашаться на установку каких-либо дополнительных программ.

В информационно-телекоммуникационной сети «Интернет» постоянно регистрируются новые модификации вредоносных программ, позволяющих злоумышленникам получить доступ к банковским счетам Клиентов. В целях безопасности настоятельно рекомендуется соблюдать следующие меры безопасности при использовании банковской карты в информационно-телекоммуникационной сети «Интернет».

Используйте для работы компьютер, на котором установлено современное антивирусное программное обеспечение и следите за его регулярным обновлением.

Не открывайте и не отвечайте на подозрительные электронные письма, внимательно проверяйте правильность указанных в письмах ссылок на сайты.

Прежде, чем вводить логин и пароль для входа в сервис ДБО «Интернет-Банк»:

– внимательно проверьте правильный адрес ДБО «Интернет-Банк», он должен быть https://faktura.ru/

– убедитесь в наличии символа замка в правом нижнем углу веб-страницы или справа/слева от адресной строки. Этот символ указывает на то, что веб-сайт работает в защищенном режиме.

Для входа в сервис ДБО «Интернет-Банк» требуется вводить только Ваш логин и пароль, а также разовый пароль для входа из SMS. **Запомните! Ваш номер мобильного телефона, номер Вашей банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации в ДБО «Интернет-Банк» не требуется, и указывать их не нужно!**

Никому, даже работникам Банка, ни при каких обстоятельствах не сообщайте свои пароли для входа в ДБО «Интернет-Банк» или для подтверждения платежей, номера Ваших карт, CVV2/CVC2 коды, номер Вашего мобильного телефона. **Запомните! Банк никогда не запрашивает эту информацию по телефону, в e-mail или SMS.**

Прежде, чем подтвердить платеж в информационно-телекоммуникационной сети «Интернет», внимательно проверьте в полученном SMS с разовым паролем информацию о сумме и получателе платежа. **Запомните! Разовым паролем можно только подтвердить платежную операцию. Не используйте его для отмены операций!**

Если Вы потеряли мобильный телефон, на который приходят SMS с разовым паролем, немедленно заблокируйте SIM-карту.

В случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в Банк согласно п.12.7 настоящих *Условий* с целью оперативного блокирования доступа!

На зараженных вирусом компьютерах пользователей сервиса ДБО «Интернет-Банк» (Faktura.ru) вирус проявляется следующим образом:

– для Клиентов, использующих смарт-карты: происходит циклический запрос PIN-кода к смарт-карте, при этом количество оставшихся попыток не уменьшается;

– для Клиентов, использующих ключи на файловых носителях, выводится сообщение: «Импорт нового закрытого ключа подписи».

<u>В целях информационной безопасности настоятельно рекомендуем:</u>

– Обратить особое внимание на необходимость строгого сохранения в тайне закрытого (секретного) ключа электронной цифровой подписи;

– Обратить внимание на увеличение риска хищения и дальнейшего неправомерного использования ключа электронной цифровой подписи и другой аутентификационной информации при доступе к сервису ДБО «Интернет-Банк» с гостевых рабочих мест (интернет-кафе и т.д.);

– Своевременно обновлять антивирусные базы;

– Настроить разовые SMS-пароли для подтверждения входа в систему и sms- и e-mail-уведомления о фактах и отправки платежных документов;

– Производить регулярный мониторинг дискового пространства компьютеров на предмет наличия вредоносного ПО;