Информационный бюллетень №3 от 29 января 2020
Information bulletin # 3 as of January 29, 2020

ООО «Эйч-эс-би-си Банк (РР)»
ООО HSBC Bank (RR)

Вниманию Клиентов - Юридических Лиц
For the Attention of Corporate Customers

Уважаемые клиенты!

ООО «Эйч-эс-би-си Банк (РР)» (далее - «Банк») настоящим напоминает вам о необходимости следовать рекомендациям Банка в области обеспечения безопасности с целью минимизации риска кибер-угроз и мошенничества.

При разработке системы HSBCnet Группа HSBC применяет ряд современных передовых технологий и методов защиты:

- SSL шифрование данных – криптографический протокол, обеспечивающий безопасное соединение между веб-браузером и сервером системы.
- Сертификат безопасности сайта – система HSBCnet имеет сертификат безопасности, благодаря которому обеспечивается возможность установить подлинность сайта. При некорректном сертификате браузер ограничивает вход на такой сайт и отображается соответствующее предупреждение.
- Использование одноразовых паролей с помощью Устройства Защиты – для аутентификации в системе требуется дополнительное подтверждение с помощью одноразовых паролей, генерируемых Устройством Защиты или Программным Устройством Защиты, установленном на мобильном устройстве. Такое дополнительное подтверждение также может потребоваться для совершения некоторых действий в системе, например, для отправки платежных поручений в Банк.
- Автоматический выход из системы – в случае неактивности в HSBCnet в течение некоторого времени, производится автоматический выход из системы.
- Автоматическая блокировка учетной записи – после нескольких неудачных попыток входа в систему учетная запись будет автоматически заблокирована.
- Протоколирование действий – система ведет детальное протоколирование всех действий в системе.

Для дополнительного обеспечения безопасной работы в системе HSBCnet мы рекомендуем:

- внедрите в вашей организации собственные меры обеспечения непрерывности бизнеса;
- обеспечьте безопасность персональных компьютеров ваших сотрудников с помощью антивирусных программ. Пользователи HSBCnet могут безвозмездно воспользоваться предлагаемым эффективным антивирусным программным обеспечением Webroot SecureAnywhere;
- всегда держите Устройство Защиты, или мобильное устройство с установленным Программным Устройством Защиты при себе, не передавайте Устройство и код доступа к нему другим сотрудникам, сохраняйте код доступа от Устройства в тайне, не записывайте его непосредственно на Устройстве;
- если в вашей организации имеется возможность удаленной работы сотрудников, обеспечьте, чтобы ваши пользователи HSBCnet могли войти в HSBCnet со своего удаленного рабочего места.

Также, напоминаем, что сотрудники Банка никогда не попросят вас сообщить какие-либо учетные данные и пароли, сгенерировать защитные коды с помощью физических, а также программных Устройств защиты – по телефону или любыми другими способами. Просим вас всегда быть бдительными.

В случае возникновения вопросов вы можете связаться с Отделом по обслуживанию корпоративных клиентов по тел. +7 (495) 783-88-86 в рабочее время Банка.

С уважением, ООО «Эйч-эс-би-си Банк (РР)»

Информационный бюллетень №3 от 29 января 2020
Information bulletin # 3 as of January 29, 2020

ООО «Эйч-эс-би-си Банк (РР)»
ООО HSBC Bank (RR)

Вниманию Клиентов - Юридических Лиц
For the Attention of Corporate Customers

Dear clients,

ООО HSBC Bank (RR), hereafter referred to as the Bank, hereby reminds you that you should follow the Bank's security recommendations to mitigate the risk of cyber threats and fraud.

In development of HSBCnet system, HSBC Group uses some state-of-the-art technologies and security methods:

- SSL encryption – cryptographic protocol that provides secure connection between web browser and system server;
- Website security certificate – HSBCnet system has a security certificate that allows to authenticate the web site. If the certificate is invalid, the browser will restrict access to such web site and will display a warning;
- Use of one-time passwords on a Security device – authentication in the system requires additional confirmation by means of one-time passwords generated by a Security device or Soft token installed on a mobile device. Such additional confirmation may also be required for some actions within the system e.g. for sending payment orders to the Bank;
- Automatic log-off after a period of inactivity within HSBCnet;
- Automatic blocking of user account after several failed log-on attempts.
- Actions logging – the system keeps a detailed log of all actions within the system.

For your additional security in HSBCnet, we recommend that you do the following:

- Implement own business continuity measures in your organisation;
- Keep your employees' PCs safe by means of anti-virus software. HSBCnet users are offered to use, an effective anti-virus software Webroot SecureAnywhere free of charge;
- Always keep your security device or mobile device with installed Soft token to yourself, do not share your Security device or an access code with other employees, ensure secrecy of access code and do not record it directly on the device;
- If your employees can work remotely, make sure that your HSBCnet users are able to enter HSBCnet from their remote workstations.

Please also be reminded that employees of the Bank will never ask you to provide any login data or passwords or to generate security codes by means of physical security devices or software-based security devices - by phone or otherwise. We urge you to be vigilant at all times.

If you have any questions please contact our Client Service unit at +7 (495) 783-88-86 during business hours of the Bank.

With kind regards,

ООО HSBC Bank (RR)