ПАМЯТКА О РИСКАХ ПРИ ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

Уважаемые Клиенты!

напоминаем Вам о необходимости следовать следующим требованиям по обеспечению информационной безопасности при работе в системе «Интернет-Банк-Клиент»:

Не передавать неуполномоченным лицам логины и пароли и ПИН-коды для входа в систему «Интернет-Банк-Клиент», а также носители электронной подписи (USB-ключи или SMART-карты).

Обеспечить сеансовый режим работы с USB-ключами (подключать USB-ключ к компьютеру **только на время работы** в системе «Интернет-Банк-Клиент»).

Обеспечить надежное хранение носителей электронной подписи вне сеансов работы в системе «Интернет-Банк-Клиент» (USB-ключи или SMART-карты должны храниться в сейфах или иных местах хранения, доступ к которым ограничен).

Обеспечить исключение возможности использования неуполномоченными лицами компьютера, с которого ведется работа в системе «Интернет-Банк-Клиент», а также просмотра ведущихся на нем работ.

Регулярно контролируйте состояние своих счетов и незамедлительно информируйте обслуживающее подразделение Банка обо всех подозрительных или несанкционированных операциях.

Обеспечить для всех компьютеров, с которых ведется работа в системе «Интернет-Банк-Клиент» **выполнение следующих требований к системному и прикладному программному обеспечению:**

- наличие современной лицензионной операционной системы (с настроенной автоматической установкой обновлений);
- отсутствие нелицензионных программ;
- наличие эффективной системы антивирусной защиты (лицензионной и регулярно обновляемой);
- отсутствие программ удаленного доступа (TeamViewer, Ammy Admin и т.п.).

Обеспечить для всех компьютеров, с которых ведется работа в системе «Интернет-Банк-Клиент» **выполнение следующих настроек:**

- Отключить учетные записи «Гость» / «Guest»;
- Установить пароли достаточной сложности на все учетные записи под которыми можно зайти в операционную систему;
- Установить пароль высокой сложности на встроенную учетную запись «Администратор» / «Administrator» (или отключить ее в случае неиспользования);
- Отключить возможность подключения к удаленному рабочему столу.
- Не открывайте почтовые вложение от неизвестных отправителей, в них могут содержаться вредоносные файлы.

Запретить на всех компьютерах, с которых ведется работа в системе «Интернет-Банк-Клиент» **доступ к следующим Интернет ресурсам и сервисам:**

- Социальные сети («В контакте», «одноклассники», «Мой мир» и т.д.);
- Интернет- мессенджеры (ICQ, Skype, Viber и т.п.);
- Сайты развлекательного характера;
- Торрент-клиенты и т.п.

Настоятельно рекомендуем **подключить услугу «СМС-информирование»** которая позволяет в реальном времени получать информацию об операциях по счетам.

Незамедлительно **информировать Банк при отсутствии возможности подключения к сайту системы «Интернет-Банк-Клиент»** (предварительно удостоверившись в работоспособности подключения к сети Интернет).

Проводить смену ключей электронной подписи по истечении срока действия ключа с периодичностью, установленной Банком.

Кроме того, необходимо **в обязательном порядке перегенерировать ключи электронной подписи** и проводить смену паролей для доступа к системе «Интернет-Банк-Клиент» в случаях увольнения или смены лиц, допущенных к этим ключам, а также руководителей, которые подписывали решения (доверенности) о допуске пользователей к ключам электронной подписи.

Незамедлительно информировать Банк в случае компрометации или при возникновении подозрений о компрометации ключей электронной подписи.

Поддерживать в актуальном состоянии контактную информацию, указанную при заключении договора на «Интернет-Банк-Клиент» и своевременно сообщать обо всех изменениях.

Помните!

Вся ответственность за конфиденциальность и сохранность логинов, паролей, а также носителей электронной подписи лежит на пользователе системы «Интернет-Банк-Клиент»!

Контактные телефоны:

Операционное обслуживание: **(8352) 309-351, 309-807**

Техническая поддержка: **(8352) 586-889, 309-393**

Информационная безопасность: **(8352) 309-826**