УВАЖАЕМЫЕ КЛИЕНТЫ – ПОЛЬЗОВАТЕЛИ СИСТЕМ «КЛИЕНТ-БАНК» И «ИНТЕРНЕТ-КЛИЕНТ-БАНК»!

ЗАО «СНГБ» (далее – Банк) настоящим доводит до Вашего сведения, что в последнее время наблюдается повышение активности мошеннических действий, направленных на совершение несанкционированных Клиентом операций в системах дистанционного банковского обслуживания «Клиент-Банк» и «Интернет-Клиент-Банк» (далее – система КБ/ИКБ).

Мошеннические операции являются результатом деятельности мошенников, которые, получив возможность управлять компьютером Клиента с установленной системой КБ/ИКБ, (в том числе удаленно и/или посредством заражения компьютера Клиента вирусами), осуществляют кражу паролей и ключей электронной подписи Клиента, вследствие чего получают доступ к управлению счетами клиента.

Одной из приоритетных задач Банка является повышение уровня безопасности работы Клиента при использовании системы КБ/ИКБ. Для решения этой задачи Банк регулярно осуществляет совершенствование системы информационной безопасности Банка, в том числе путем использования современных специализированных программ по выявлению нетипичных для Клиента операций, совершаемых с использованием системы КБ/ИКБ.

Однако безопасность использования системы КБ/ИКБ также зависит и от действий Клиента, направленных на защиту своих конфиденциальных данных!

Халатность Клиента и его пренебрежение к правилам безопасности при использовании системы КБ/ИКБ может привести к получению мошенниками доступа к информации по счетам Клиента и хищению его денежных средств!

В целях обеспечения безопасности при использовании системы КБ/ИКБ Банк **настоятельно рекомендует** соблюдать положения *Правил организации электронного документооборота с использованием систем «Клиент-Банк» и «Интернет-Клиент-Банк» Закрытого акционерного общества «Сургутнефтегазбанк»,* размещенные на официальном web-сайте Банка в сети Интернет по адресу: www.sngb.ru, в том числе (но не ограничиваясь):

во-первых, обеспечивать безопасность компьютера, с которого осуществляется работа с системой КБ/ИКБ (использовать лицензионное программное обеспечение, не устанавливать на компьютер программы удаленного доступа, использовать антивирус, ограничить доступ к компьютеру неуполномоченных лиц и пр.);

во-вторых, обеспечивать безопасность паролей (логинов) и ключей, используемых для доступа в систему КБ/ИКБ (хранить пароли, ключи в недоступном для третьих лиц месте, регулярно осуществлять смену паролей и пр.);

в-третьих, контролировать, что вход в систему ИКБ осуществлен с официального web-сайта Банка в сети Интернет по адресу: https://clbank.sngb.ru;

в-четвертых, соблюдать иные, рассылаемые Банком средствами системы ДБО, рекомендации по обеспечению безопасности.

В случае компрометации конфиденциальной информации (паролей, ключей) или подозрения на компрометацию необходимо незамедлительно обратиться в Банк по тел.: +7 (3462) 39-88-44, +7 (3462) 39-88-77.

НАПОМИНАЕМ!

Банк НИКОГДА не осуществляет рассылку сообщений (посредством e-mail, смс-сообщений) с просьбой предоставить (подтвердить) Вашу конфиденциальную информацию (пароли, логины и т.п.).

НИКОГДА не отвечайте на данные сообщения и незамедлительно сообщите о них в Банк по тел.: **8-800-200-88-04, 8-800-775-88-04**.

ВНИМАНИЕ!

В целях защиты интересов Клиента при совершении операций с использованием системы КБ/ИКБ Банк предлагает Вам специальную услугу:

- информирование посредством смс-сообщений или e-mail-рассылки об операциях по счету, в том числе об операциях, которые, по мнению Банка, являются нетипичными для Клиента.

Данная опция позволит Вам своевременно получать информацию об операциях, совершаемых по счету, и предотвратить несанкционированные Вами операции по счету.

Для подключения услуги необходимо заполнить Заявление и обратиться в Банк.

Будьте бдительны при работе с системой дистанционного банковского обслуживания!