Уважаемые клиенты ПАО «НИКО-БАНК»!

В связи с учащением попыток неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания (далее - ДБО) (пароли, секретные ключи средств шифрования и аналогов собственноручной подписи), о которых неоднократно сообщал Центральный Банк РФ, предлагаем Вам внимательно ознакомиться с представленными рекомендациями по обеспечению безопасности при работе с системами ДБО:

- **Установите и регулярно обновляйте лицензионное антивирусное программное обеспечение на Вашем компьютере.** Действие вирусов может быть направлено на перехват Вашей персональной информации и передаче её злоумышленникам;

ВАЖНО: Обновление антивирусных баз рекомендуется проводить в автоматическом режиме по мере их выпуска организацией-разработчиком. Необходимо обеспечить регулярные периодические проверки по поиску вирусов на автоматизированных рабочих местах используемых для ДБО.

- **Используйте только лицензионное программное обеспечение.**

ВАЖНО: Помните, использование нелицензионного программного обеспечения - это не только правонарушение, но и лазейка в системе Вашей безопасности, которой могут воспользоваться мошенники.

- **Своевременно устанавливайте обновления операционной системы своего компьютера,** рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполняйте обновления (патчи) операционной системы и браузера Вашего компьютера, так как данные действия значительно повысят его уровень безопасности;
- **Установите и настройте персональный брандмауэр (firewall) на Вашем компьютере.** Это позволит Вам запретить несанкционированный удаленный доступ к Вашему компьютеру из сети Интернет и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа. Дополнительно можно настроить брандмауэр на доступ только по адресам Системы ДБО;

ВАЖНО: Не сообщайте никому пароль для доступа к системам ДБО (включая работников Банка и сотрудников Вашей организации или Ваших родственников)!

- **После окончания работы в Системе ДБО обязательно корректно завершите работу (выйдите из Системы ДБО с использованием кнопки «Выход») и/или закройте браузер (приложение Internet Explorer и т.п.);**
- **Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях;**
- **Никогда не открывайте вложения в письмах от неизвестных отправителей;**
- **При работе в сети Интернет будьте бдительны, устанавливайте дополнительные программы и приложения, только если вы доверяете их разработчику;**
- **Не используйте рабочий компьютер (используемый для ДБО) для посещения развлекательных сайтов и сайтов с пиратским содержанием.**

ВНИМАНИЕ! При обнаружении Вами попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть осуществлены, просим Вас:

- **немедленно сообщить об этом в Банк по одному из следующих телефонов:**
  (3532) 34-90-32
  (3532) 20-55-42
- **блокировать технические средства, используемые для работы в системах ДБО;**
- **представить в Банк подробное письменное описание обстоятельств компрометации паролей или несанкционированного доступа.**

Убедительно просим Вас неукоснительно соблюдать рекомендуемые правила безопасности работы в системах ДБО.