БАНК НООСФЕРА

ПАМЯТКА
по обеспечению безопасности при работе в системе дистанционного банковского обслуживания

Для минимизации рисков при работе в системе дистанционного банковского обслуживания (далее – Система ДБО) необходимо соблюдать следующие правила:

- Не передавать третьим лицам информацию, которую они могут использовать для несанкционированного доступа к вашим данным, хранящимся в Системе ДБО, и исключить иные возможности получения указанной информации третьими лицами, в том числе сотрудниками Банка;
- Не хранить пароли, а также Сертификаты ключей электронной подписи на устройстве (компьютере), с которого осуществляется вход в Систему ДБО;
- Не использовать функцию автоматического запоминания пароля в памяти браузера устройства, с которого осуществляется вход в Систему ДБО;
- Регулярно менять пароль на вход в Систему ДБО;
- Использовать современные средства обеспечения информационной безопасности при работе в сети Интернет (программное обеспечение защиты от вредоносного кода, персональные межсетевые экраны и т. п.);
- Работу в Системе ДБО осуществлять при соединении с сетью Интернет в защищенном режиме. Признаком использования защищенного соединения является наличие в строке задач браузера значка закрытого замка;
- Использовать заранее оговоренные средства связи между Банком и Клиентом при осуществлении контактов по вопросам работы в Системе ДБО;
- Информировать Банк о малейших подозрениях на возможную компрометацию паролей на вход в Систему ДБО, а также ключей электронной подписи, об утере Устройства для хранения ключа электронной подписи, о пришедших SMS-сообщениях по операциям, которые вы не совершали и пр.;
- Приостанавливать доступ в Систему ДБО при длительных перерывах в ее использовании;
- Завершать работу в Системе ДБО с выходом из системы, а не выходом из браузера Интернет-страницы;
- Выполнять рекомендации Банка при работе в сети Интернет, установленные Правилами ДБО в АКБ «НООСФЕРА» (АО).

Рекомендации по защите от вредоносного кода:

- Использовать лицензионное и регулярно обновляемое программное обеспечение;
- Осуществлять обновление программного обеспечения и баз сигнатур устройства (компьютера) в автоматическом режиме;
- Систематически проверять устройство на вредоносный код, в том числе осуществлять ежедневное сканирование файлов и программных модулей;
- Не производить автозагрузку с внешних носителей, таких как флеш-карты, компакт-диски и прочее;
- Не посещать сомнительные сайты;
- При работе в сети Интернет использовать пользовательские учетные записи, а не учетную запись администратора устройства (компьютера).

Рекомендации для защиты от несанкционированного доступа с использованием злоумышленниками ложных ресурсов Интернет:

- Проходить по ссылкам Интернет-сайтов после проверки достоверности и правильности адреса сайта.
- Не вводить и не сообщать посторонним лицам, в том числе сотрудникам Банка(ов) пароли, ключи электронной подписи, истребуемые в запросах, полученных по электронной почте.
- Не производить соединение устройства через удаленный доступ с устройствами посторонних лиц, в том числе не принимать с web-сайтов программы, являющиеся компьютерными вирусами или "закладками", выполняющими в фоновом режиме работы скрытые функции, связанные с неправомерным получением персональной информации пользователей Системы ДБО.
- Не реагировать на SMS-сообщения, полученные от абонентов с неизвестными номерами, о необходимости позвонить по номерам телефонов или выполнить какие- либо действия с доступом к банковскому счету или к Системе ДБО.
- При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
- Использовать системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
- Запретить в межсетевом экране соединение с сетью Интернет по протоколам FTP, SMTP. Соединения SMTP осуществлять только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики.
- При работе в сети Интернет не соглашаться на установку каких-либо дополнительных программ от недоверенных издателей.