Nordea

Памятка
«О правилах безопасного использования системы Nordea online»

Соблюдение рекомендаций, содержащихся в настоящей Памятке, позволит Вам обеспечить максимальную безопасность использования системы дистанционного банковского обслуживания Nordea online (далее – Система).

1. Доступ в Систему осуществляется по адресу https://online.nordea.ru. Вход в Систему может быть осуществлен на сайте АО «Нордеа Банк» www.nordea.ru.
2. Обязательно убедитесь в правильности ссылки до входа в Систему, так как похожие адреса могут использоваться третьими лицами для кражи Ваших персональных данных и осуществления неправомерных действий с Вашими банковскими счетами/картами.
3. Вход в Мобильную версию Системы осуществляется через мобильное приложение «Nordea online», загруженное на мобильный телефон через магазин приложений App Store/ Google Play. Перед установкой приложения убедитесь, что его разработчиком является Center of Financial Technologies (Центр Финансовых Технологий).
4. Для входа в Nordea online требуется вводить только логин и пароль или код доступа (для мобильного приложения). Ввод персональных данных, номера мобильного телефона, данных банковской карты не требуется.
5. По возможности осуществляйте вход в Систему только с личного компьютера. В случае входа в Систему с чужого компьютера не сохраняйте на нем персональные данные. Помните, что риск неправомерного использования Системы увеличивается в случае входа в Систему с гостевых рабочих мест, например, в Интернет-кафе, в гостинице и др.
6. Перед подтверждением операции внимательно проверяйте данные (получатель, сумма и т.д.) в Push-уведомлении/SMS-сообщении, содержащем разовый пароль.
7. Избегайте регистрации номера мобильного телефона, на который приходят SMS-сообщения с разовыми паролями, в социальных сетях и других открытых источниках.
8. Принимайте меры для предотвращения риска изготовления дубликата Вашей сим-карты:
   - пользуйтесь номером телефона, который оформлен лично на Вас,
   - не используйте анонимные сим-карты,
   - не передавайте мобильный телефон или сим-карту в пользование третьим лицам,
   - обратитесь к Вашему мобильному оператору для запрета выпуска дубликатов сим-карты, а также совершения действий с Вашей сим-картой на основании доверенности.
9. После завершения работы осуществляйте выход из Системы, используя кнопку «Выйти».
10. При отсутствии действий в Системе в течение 15 минут или 10 минут в Мобильной версии Системы происходит автоматическое завершение сеанса работы. Для возобновления работы необходимо снова ввести логин и пароль или код доступа (для мобильного приложения).
11. Используйте лицензионное программное обеспечение на компьютере. Проводите обновление программ особенно в части информационной безопасности в соответствии с рекомендациями разработчиков.
12. Обязательно устанавливайте и своевременно обновляйте антивирусное программное обеспечение на компьютере и мобильном устройстве для защиты от хакерских атак.
13. Храните логин, пароль и мобильное устройство, на котором установлена Мобильная версия Системы, в недоступном для третьих лиц месте.
    Рекомендуется не хранить логин и пароль в памяти мобильного устройства, на котором установлена Мобильная версия Системы.
14. Никогда не передавайте логин и пароль неуполномоченным лицам, в том числе родственникам, знакомым или сотрудникам кредитной организации.

15. Ни при каких обстоятельствах не сообщайте никому пароли для входа в Nordea online, разовые пароли и данные банковских карт. Злоумышленники могут представляться сотрудниками банка, государственных органов или сотовых компаний.
16. Регулярно, не реже 1 раза в месяц, меняйте пароль для доступа в Систему.
17. Если логин и пароль стали известны третьим лицам, незамедлительно измените пароль в Системе. В случае отсутствия возможности изменить пароль обратитесь в АО «Нордеа Банк» для получения нового временного пароля или блокировки доступа в Систему.
18. В случае использования Мобильной версии Системы рекомендуется использовать разные устройства для входа в Систему и для получения разовых паролей.
19. В случае утраты мобильного устройства, на котором установлена Мобильная версия Системы, или подозрения на его компрометацию (например, если телефон находился или мог находиться в руках третьего лица) незамедлительно измените пароль и отключите отправку Push-уведомления на это устройство в Интернет-версии Системы.
20. В случае обнаружения несанкционированных операций по Вашим счетам, совершенных в Системе, незамедлительно обратитесь в АО «Нордеа Банк» для блокировки доступа в Систему и оформите Заявление о несогласии с операцией, совершенной в Системе.
21. Не отвечайте на электронные письма (в том числе от имени АО «Нордеа Банк»), в которых запрашиваются Ваши персональные данные. Не следуйте по ссылкам, указанным в подобных письмах, включая ссылки на Систему, так как они могут вести на сайты-двойники.
22. Рекомендуется иметь при себе контакты АО «Нордеа Банк» (например, в записной книжке, мобильном телефоне):
    84959212101 – для звонков по Москве
    88002003477 – бесплатный номер единой справочной службы для регионов
    Contact_Center_Support@nordea.ru
    www.nordea.ru