Рекомендации по снижению рисков информационной безопасности при работе с системой дистанционного банковского обслуживания и рисков повторного осуществления перевода денежных средств без добровольного согласия клиента

Уважаемый Клиент, для выполнения непрерывного процесса обеспечения информационной безопасности при работе с системой дистанционного банковского обслуживания (ДБО) настоятельно рекомендуем соблюдать следующие правила информационной безопасности:

1. Использовать для входа в систему ДБО только официальный сайт РНКО «ИНЭКО»: https://inecobank.ru

2. Всегда проверяйте, что при выполнении финансовых операций или при передаче персональных данных используется шифрованное соединение. Чтобы проверить шифруются ли данные, посмотрите на ссылку страницы, где вводятся данные. Адрес должен начинаться с «https://», а не с «http://».

3. Используйте только доверенные компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным ПО и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного ПО, своевременно обновляйте лицензионную операционную систему и браузеры.

4. Исключайте возможность работы в системе ДБО из публичных мест, предоставляющих доступ в сеть Интернет (кафе, в гостях, на стадионах и т.д.)

5. Никому не сообщайте ваши данные для доступа в систему ДБО (логин, пароль, код из СМС), в том числе сотрудникам кредитной организации.

6. Меняйте пароль для доступа в систему ДБО не реже одного раза в три месяца.

7. Используйте пароли длиной не менее 8 символов. В пароле обязательно должны присутствовать буквы верхнего и нижнего регистров, а также цифры и специальные символы.

8. Не используйте в качестве пароля комбинацию, как-то связанную с датой рождения, псевдонимом и (или) кличкой домашнего животного, собственным именем или именем родственника, телефонными номерами.

9. Используйте виртуальную клавиатуру для ввода пароля/кода.

10. Не посещайте сайты сомнительного характера (содержимого).

11. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

12. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора.

13. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагируйте на ошибки.

14. Запретите в межсетевом экране соединение с интернет по протоколам FTP, SMTP. Разрешите соединения SMTP только с конкретными почтовыми серверами, на которых зарегистрированы ваши электронные почтовые ящики.

15. Не давайте разрешения неизвестным программам выходить в сеть Интернет.

16. При работе в сети Интернет не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.

17. Используйте средства защиты информации (антивирус с автоматическим обновлением баз, средства от НСД, межсетевой экран).

18. Не используйте на своём рабочем месте средства удаленного администрирования.

19. Не используйте стандартный pin-код.

20. Не оставляйте ключевые носители без присмотра или подключенными к компьютеру, когда не работаете с системой ДБО.

21. Храните ключевые носители (смарт-ключи, флэш-карты и другие носители с записанными ключами) в месте, недоступном посторонним лицам. Исключите хранение ключей на жестком диске, в сетевых каталогах и прочих общедоступных ресурсах.

22. Храните в тайне пароль доступа к ключу, исключите его запись на стикерах, носителях ключей и т.п.

23. Обязательно сверяйте текст SMS-сообщений/PUSH-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS-сообщении/PUSH-сообщении указан пароль/код для подтверждения платежа, который вы не совершали или вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по вашему счету платеж, ни в коем случае не вводите его в системе ДБО и не называйте его, в том числе сотрудникам кредитной организации.

24. В случае утери мобильного устройства, на который приходят разовые пароли/коды, немедленно заблокируйте SIM-карту и (или) войдите в Интернет-банк (веб-версию) и удалите устройство из списка зарегистрированных устройств для получения PUSH-сообщений.

25. Запишите контактный телефон вашего банка в адресную книгу или запомните его. В случае если в личном кабинете ДБО вы обнаружите телефон, отличный от записанного,

в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в РНКО «ИНЭКО» по ранее записанному вами телефону.

26. Избегайте регистрации номера вашего мобильного телефона, на который приходят SMS-сообщения с разовым паролем/кодом, в социальных сетях и других открытых источниках.

27. Завершайте работу с системой ДБО корректно с помощью кнопки «Выход».

28. Мошенники могут использовать методы социальной инженерии (смс, звонки, электронные письма), не сообщайте свои данные (логин, пароль, одноразовые пароли из смс, кодовые фразы) звонкам «Из Банка».

29. При компрометации электронной подписи незамедлительно сообщите в РНКО «ИНЭКО» по телефону +7(4932)593959.