Памятка клиенту по обеспечению информационной безопасности при работе с системами дистанционного банковского обслуживания.

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

1. Использовать для входа в систему ДБО только официальные сайты Банка:
   - https://online.bktb.ru
   - https://icb.kubantorgbank.ru
2. Всегда проверяйте, что при выполнении финансовых операций или при передаче персональных данных используется шифрованное соединение (как на картинке выше). Чтобы проверить шифруются ли данные, посмотрите на ссылку страницы, где вводятся данные. Адрес должен начинаться с “https://”, а не с http://.
3. Не открывайте письма, вложения и не переходите по ссылкам из писем, отправитель которых вам неизвестен.
4. Никому не сообщайте ваши данные для доступа в систему ДБО (логин, пароль, код из СМС), в том числе сотрудникам Банка.
5. Меняйте пароль для доступа в систему ДБО не реже одного раза в три месяца.
6. Используйте пароли длиной не менее 8 символов. В пароле обязательно должны присутствовать буквы верхнего и нижнего регистров, а также цифры и специальные символы.
7. 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.
8. Не посещайте сайты сомнительного характера (содержимого).
9. 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».
10. Используйте на вашем рабочем месте только лицензионные и актуальные версии операционных систем и программного обеспечения.
11. Используйте средства защиты информации (антивирус с автоматическим обновлением баз, средства от НСД, межсетевой экран).
12. Не используйте на своём рабочем месте средства уделенного администрирования.
13. Не оставляйте ключевые носители без присмотра или подключенными к компьютеру, когда не работаете с системой ДБО.

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

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

16. Не используйте стандартный pin-код.

17. При компрометации электронной подписи незамедлительно сообщите в Банк по телефону 8(861)212-60-80 доб. 6.

18. При некорректной работе системы ДБО незамедлительно сообщите в Банк по телефону 8(861)212-60-80 доб. 4.