ИНФОРМАЦИЯ ДЛЯ ПОЛЬЗОВАТЕЛЯ ДБО

Для обеспечения безопасности в процессе проведения операций посредством удаленного/дистанционного обслуживания и защиты данных:

1. Пользователь при использовании интернет-банкинга:

1) не должен раскрывать посторонним лицам логин, пароль и другие данные;

2) не должен хранить свой логин и пароль и другие данные на устройствах доступа (персональный компьютер, мобильный телефон и т.д.) или других незащищенных носителях;

3) необходимо периодически менять пароль, при этом не использовать пароли с низким уровнем защиты, такие как имя или дата рождения. Пароль должен содержать комбинацию, состоящую из не менее 8 знаков: букв (прописных и заглавных), специальных символов и цифр;

4) должен обеспечить конфиденциальность личной информации, а именно не раскрывать личную информацию (данные документа, удостоверяющего личность, адрес электронной почты и другие данные) посторонним лицам;

5) необходимо регулярно проверять историю операций и выписки для отслеживания ошибок или несанкционированных операций по счету и незамедлительно информировать поставщика услуг о любых случаях несанкционированных операций;

6) необходимо проверять правильность и безопасность веб-страницы, при этом:

- перед осуществлением любых онлайн-операций или предоставлением личной информации должен убедиться, что используется правильная веб-страница интернет-банкинга. Необходимо остерегаться фальшивых веб-страниц, созданных в целях мошенничества;

- необходимо убедиться в безопасности веб-страницы, проверив наличие Унифицированных Указателей Ресурсов (URL), которые должны начинаться с "https", а на статусе интернет-браузера должен появиться знак защищенного соединения;

- всегда вводить URL веб-страницы непосредственно в интернет-браузер и избегать перенаправления или ссылки на другие ненадежные страницы;

- по возможности использовать программу, которая автоматически шифрует или кодирует передаваемую информацию в процессе осуществления электронных операций;

7) должен защитить свое устройство доступа (персональный компьютер, мобильный телефон и т.д.) от несанкционированного доступа и вредоносных программ;

8) необходимо покинуть сайт, где осуществляются электронные операции, даже если устройство оставлено без присмотра на короткий срок, и не забывать выходить из системы после осуществления электронных операций;

9) необходимо ознакомиться с политикой безопасности системы интернет-банкинга:

- необходимо внимательно ознакомиться с условиями системы интернет-банкинга относительно осуществления платежей, переводов, дебетования/кредитования счета и другими условиями банковского обслуживания;

- перед вводом личной финансовой информации системы интернет-банкинга необходимо внимательно ознакомиться с условиями использования или распространения данной информации.

2. Пользователь при использовании мобильного банкинга, мобильного приложения:

- не должен раскрывать посторонним лицам свой PIN-код, пароль к системе удаленного/дистанционного обслуживания, пароль от электронной почты, иные сведения, которые могут способствовать несанкционированному доступу при удаленном/дистанционном обслуживании от имени пользователя;

- необходимо периодически менять свой PIN-код, пароль используемый для мобильного банкинга, мобильного приложения;

- не должен позволять посторонним лицам использовать свой мобильный телефон, через который осуществляется банковская операция;

- при потере или краже мобильного телефона незамедлительно сообщить поставщику услуг;

- не должен отправлять свою личную информацию, содержащую пароль или PIN-код, через электронную почту, социальные сети и другие средства электронного обмена данными;

- необходимо регулярно проверять историю операций и выписки для отслеживания ошибок или несанкционированных операций и незамедлительно информировать поставщика услуг о любых случаях несанкционированных операций;

- должен незамедлительно сообщить поставщику услуг при возникновении любых вопросов относительно безопасности доступа к системам удаленного/дистанционного обслуживания.