Приложение №1
К Публичной оферте

Правила безопасности и хранения персональных данных

Держатели электронного кошелька должны соблюдать следующие правила для обеспечения безопасности персональных данных:

1. Не хранить свои данные для авторизации (пароль, ПИН) и другие персональные данные на устройствах доступа (персональный компьютер, мобильный телефон и т.д.) или других незащищенных носителях;
2. Не сообщать, не раскрывать и не передавать иным образом другим лицам данные для авторизации и другие персональные данные, не размещать их в доступных местах;
3. Нести персональную ответственность за несанкционированные транзакции в случае раскрытия доступа в личный кабинет или в мобильное приложение третьим лицам;
4. Периодически менять ПИН, пароль и не использовать простое сочетание символов и знаков, такие как имя или дата рождения;
5. Не раскрывать личную информацию (номер мобильного телефона, номер электронного кошелька, паспортные данные, номер банковского счета или адрес электронной почты, ПИН/ пароль) посторонним лицам;
6. Регулярно проверять историю операций и остаток на электронном кошельке для отслеживания ошибок или неавторизованных операций по электронному кошельку;
7. Не использовать для входа в личный кабинет случайно подобранные мобильные устройства, публичные или непроверенные компьютеры, установленные в общественных местах (компьютерные клубы, библиотеки и т.п.);
8. Перед осуществлением любых операций в личном кабинете (посредством персонального компьютера или мобильного телефона) убедиться, что используется подлинная страница веб сайта;
9. Убедиться в безопасности веб-страницы проверив значок защищенного соединения в виде закрытого замка в правом нижнем углу или в адресной строке Интернет браузера;
10. Всегда вводить URL (унифицированный указатель ресурсов) веб страницы непосредственно в веб-браузере. Избегать перенаправления или ссылки на другие ненадежные страницы;
11. Защитить свое устройство доступа (персональный компьютер, мобильный телефон, планшет, и т.д.) от несанкционированного доступа и вредоносных программ, при этом следить за регулярным обновлением антивирусной программы и ее постоянной работой;
12. Необходимо выполнить выход из личного кабинета или из мобильного приложения, где осуществлялись электронные операции, даже если устройство доступа оставлено без присмотра на короткий срок;
13. Не позволять другим лицам использовать свой мобильный телефон или иное устройство доступа, через которое осуществляется доступ и оплата с электронного кошелька;
14. Незамедлительно информировать Банк - Эмитент любым доступным способом (в письменной, электронной, устной форме) по контактам, указанным в настоящем Договоре о любых случаях неавторизованного использования электронного кошелька, проведении несанкционированных и/ (или) мошеннических операций третьими лицами;
15. При потере или краже мобильного телефона, на котором использовался электронный кошелек, незамедлительно сообщить Банку - Эмитенту любым доступным способом (в письменной, электронной, устной форме) по контактам, указанным в настоящем Договоре.