Рекомендации по обеспечению безопасности при работе с системой интернет-банкинга для физических лиц «Магнус-Онлайн»

Система интернет-банкинга «Магнус-Онлайн» обеспечивает вас надежной системой безопасности для управления своими счетами. Однако при использованиии сети Интернет всегда существует риск получения несанкционированного доступа к системе не уполномоченными лицами. Данные рекомендации помогут Вам повысить уровень безопасности при работе с системой «Магнус-Онлайн».

Соединение и работа с системой «Магнус-Онлайн» осуществляется через сеть Интернет в защищенном режиме с помощью протокола SSL (Secure Sockets Layer).

В качестве электронной подписи (ЭП) в системе «Магнус-Онлайн» признаётся использование одноразовых кодов, получаемых посредством SMS.

При работе с «Магнус-Онлайн», для повышения безопасности, необходимо следовать следующим рекомендациям:

- Ни при каких условиях не сообщайте информацию о вашем пароле/ЭП никому, включая сотрудников Банка.
- Проверяйте, что соединение действительно происходит в защищенном режиме SSL, в правом нижнем углу или адресной строке вашего вэб-браузера должен быть виден значок закрытого замка.
- При переходе на сайт Банка по ссылке из поисковой системы обращайте внимание на специальный знак, отображающий достоверность ссылки на основе официальных данных с сайта Центрального Банка.
- В систему «Магнус-Онлайн» переходите с официального сайта Банка (мошенники могут имитировать интерфейс входа в систему в целях получения доступа к вашим данным).
- Ни в коем случае не сохраняйте информацию о вашем пароле на любых носителях, включая компьютер, не осуществляйте отправку паролей по электронной почте. Если у вас возникли подозрения, что кто-либо владеет информацией о вашем пароле, Вам необходимо с помощью обращения в Банк (по тел. (495) 662-45-45 /760) заблокировать учетную запись.
- После окончания работы в «Магнус-Онлайн» обязательно закройте окно системы с помощью кнопки Выход.
- Убедитесь, что ваш компьютер не поражен какими-либо вирусами. Установите и активизируйте антивирусные программы. Старайтесь их постоянно обновлять. Обращаем внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам конфиденциальной информации.
- Установите и используйте персональный брандмауэр (firewall) на вашем компьютере для входа в сеть Интернет, это позволит предотвратить несанкционированный доступ к информации на вашем компьютере.
- Периодически проверяйте перечень установленного программного обеспечения на компьютере, с которого осуществляете взаимодействие с системой iBank на предмет наличия программного обеспечения, установку которого вы не

производили. Появление подобного программного обеспечения на вашем компьютере может свидетельствовать о доступе к нему посторонних лиц.

- Используйте только програмное обеспечение (интернет-браузеры) и операционные системы, для которых производитель обеспечивает поддержку и предоставление обновлений по устранению известных ошибок и уязвимостей.
- В случае утери доступа к средству электронной подписи (потеря телефона, потеря сим-карты, получение доступа к сим-карте или телефону посторонними лицами) обязательно уведомите Банк для блокировки учетной записи.