**Правила безопасности при работе в Личном кабинете**

Вход в Личный кабинет осуществляется на основе предъявления системе аутентификационных данных – логина и пароль. Логином (или идентификатором) является адрес электронной почты, указанный в Заявлении о присоединения. Первоначальный пароль для входа в личный кабинет направляется на указанный адрес электронной почты и подлежит немедленной смене при первом входе. Логин и пароль относятся к категории конфиденциальной информации и поэтому подлежат защите.

Для осуществления входа в Личный кабинет необходимо использовать стойкие пароли. В пароле не должны использоваться легко вычисляемые сочетания символов (например, последовательно расположенные на клавиатуре символы: «12345678», «QWERTY», имена, фамилии, номера телефонов, даты и т.п.), а также общепринятые сокращения («ИС», «USER» и т.п.). В случае компрометации (утраты) немедленно примите меры для смены пароля.

Обеспечьте сохранность, неразглашение и нераспространение информации о пароле для доступа в Личный кабинет.

Используйте на Вашем компьютере только лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.), своевременно выполняйте обновления, рекомендуемые компанией-производителем.

Для исключения случаев заражения компьютерными вирусами необходима установка на компьютере и регулярное обновление антивирусных программ. В противном случае, возможно, что вводимая информация окажется доступной злоумышленникам, использующим и активно распространяющим в сети Интернет шпионские вирусные программы.

На регулярной основе контролируйте состояние ваших счетов и незамедлительно сообщайте обо всех подозрительных или несанкционированных операциях и иных изменениях в аутентификационных данных работникам Банка.

Исключите использование средств удаленного администрирования на Вашем ПК (TeamViewer, AnyDesk и т.п.).

Будьте бдительны и осторожны при использовании сети Интернет: внимательно проверяйте корректность адресов посещаемых сайтов, не нажимайте на баннеры и всплывающие окна и скачивайте файлы только когда полностью уверены в их безопасности. Ограничьте посещение сайтов сомнительного содержания. Убедитесь, что соединение защищено шифрованием (наличие замочка в адресной строке).

Для связи с Банком используйте контакты, размещенные только на официальном сайте Банка в сети Интернет.