Уважаемые Клиенты, во избежание мошеннических действий при использовании Системы электронного документооборота (СЭД) в том числе систем Интернет-Клиент, Банк-Клиент считаем необходимым напомнить вам некоторые меры безопасности:

– Ограничьте и контролируйте доступ к СЭД: установите на компьютер, с которого осуществляется использование СЭД, надежный пароль. Не записывайте и не передавайте его лицам, не имеющим доступ к СЭД. Если встаете со своего рабочего места, блокируйте компьютер.

– Позаботьтесь о защите компьютера, на котором установлена СЭД, от вирусов: поставьте лицензионный, регулярно обновляемый антивирус.

– Никогда не отвечайте на электронные письма от неизвестных адресатов. Не открывайте вложенные в такие письма материалы и не следуйте по «ссылкам», указанным в письмах, включая ссылки на сайт Банка. Не перезванивайте по телефонам, указанным в сообщении. Обращаться в Банк следует только по телефону, указанному в Договоре с Банком, или по телефону Единой справочной службы.

– Надежно храните свою электронную подпись (ЭП). Ни в коем случае не сохраняйте ключи ЭП на жёстких/сетевых дисках компьютера, в реестре операционной системы.
Токен, содержащий ЭП, необходим вам только при входе в СЭД и во время подписания платежного документа. Все остальное время ключ должен быть извлечен из компьютера и храниться в сейфе.

– Используйте дополнительные опции по повышению уровня информационной безопасности: фильтрацию по MAC-адресу, считыватель смарт карт SafeTouch, токены, дополнительное подтверждение перевода денежных средств введением кода с карты сеансовых ключей или полученного в СМС (для подключения дополнительных опций обратитесь в офис Банка).

– Подключите СМС-информирование о расходных операциях. Это позволит оперативно получать информацию обо всех операциях списания, совершаемых по счету.

– Контролируйте расходы и зачисления. Вы должны знать, сколько денег на счете было, сколько вы хотите использовать и сколько там должно остаться.

– При выявлении попытки несанкционированного доступа к вашему расчетному счету или подозрении на такую попытку, нужно отключить устройство доступа к СЭД. Вытащите токен, выдерните интернет-кабель, выключите компьютер, выньте шнур из розетки, у ноутбука нужно извлечь аккумуляторы. Незамедлительно позвоните в Банк (даже ночью) и сообщите о компрометации СЭД.

Рекомендуем также ознакомиться с документами, размещенными в постоянном доступе на сайте Банка:

Требования информационной безопасности при работе в СЭД;

Актуальные угрозы при работе с СЭД;

Рекомендации по безопасности.