Рекомендации по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия клиента

Уважаемый Клиент!

Обращаем внимание на необходимость строго соблюдения перечисленных в настоящем документе мер при осуществлении перевода денежных средств.

1. Перед вводом учетных данных для доступа в систему дистанционного банковского обслуживания (далее – ДБО) на сайте АО «Ури Банк» (далее – Банк) необходимо убедиться, что соединение установлено с официальным сайтом Банка. Для этого необходимо проверить правильность указания адреса сайта Банка (https://bank.woori.ru) в строке браузера и наличие сертификата безопасности (https в адресной строке).
2. Если замечено необычное поведение ДБО или какие-то изменения в интерфейсе необходимо связаться с Банком и выяснить, не связано ли это с обновлением системы. В случае подозрений на несанкционированные изменения в ДБО немедленно прекратить работу в системе и уведомить Банк о приостановлении работы (блокировке ключа электронной подписи).
3. Следует регулярно контролировать состояние своих счетов, проводить контроль сумм и получателей платежных документов. Незамедлительно информировать Банк обо всех подозрительных или несанкционированных операциях в ДБО.
4. При использовании для доступа к ДБО рекомендуем:

• включать на устройстве автоматическую блокировку экрана на период бездействия с вводом пароля для разблокировки устройства;

• применять на устройстве лицензионные средства антивирусной защиты, обеспечить своевременную загрузку обновления баз антивирусного программного обеспечения;

• использовать на устройстве лицензионное программное обеспечение из доверенных источников (например, с сайтов разработчиков);

• обеспечить на устройстве автоматическое обновление программного обеспечения;

• исключить возможность удаленного сетевого доступа к устройству, в том числе с помощью программ TeamViewer, AnyDesk, Ассистент и т.д.;

• исключить на устройстве посещение интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения;

• не хранить на устройстве используемые для входа в ДБО учетные данные, в том числе в защищенных заметках, файлах, в записках, на стикерах и т.д.;

• не открывать при работе на устройстве с электронной почтой письма, полученные от неизвестных источников, и особенно не открывать вложения и не переходить по ссылкам из таких писем;

• по возможности использовать выделенное устройство входа в ДБО только для работы ДБО.

5. При использовании ключей для работы с системой ДБО «BS-Client» рекомендуем:

• никому не сообщать пароль от ключа электронной подписи системы ДБО «BS-Client»;

• использовать сложные пароли, содержащие не менее 8 символов (буквы в верхнем и нижнем регистре, цифры и спецсимволы). Не используйте простые комбинации символов или личные данные.

• не передавать ключи электронной подписи сотрудникам технической поддержки для проверки работы системы ДБО, проверки настроек взаимодействия с Банком и т.п.;

• при увольнении ответственного сотрудника Вашей организации, имевшего доступ к ключу электронной подписи, обязательно уведомить Банк о необходимости блокирования данного ключа.