

Безопасность

Как распознать официальный сайт и защитить кабинет от мошенников.

Официальный адрес: <https://boscofinance.by>. Перед вводом данных проверяйте точное написание домена. Приложение устанавливайте только по официальной ссылке БоскоФинанс.

Подтверждение через МСИ

Переход к Межбанковской системе идентификации должен начинаться только из защищённого личного кабинета БоскоФинанс. На странице МСИ проверяйте защищённое соединение и не передавайте коды подтверждения сотрудникам, помощнику или третьим лицам. БоскоФинанс не просит установить программу удалённого доступа для идентификации.

Никому не сообщайте

Пароль, код из SMS или Authenticator, резервный код 2FA, PIN и CVV/CVC карты. Сотрудник и онлайн-помощник не должны просить эти сведения в чате, по телефону или в мессенджере.

Защитите устройство

- используйте уникальный длинный пароль и менеджер паролей;
- обновляйте систему и браузер, включите блокировку экрана;
- не входите через открытый Wi-Fi и чужие устройства;
- не устанавливайте программы удалённого доступа по просьбе неизвестных лиц;
- не переходите по ссылкам из подозрительных сообщений.

Если заметили подозрительную активность

Смените пароль с доверенного устройства, выйдите из кабинета на чужом устройстве, обратитесь на info@boscofinance.by и сообщите время, канал связи и описание события. Не пересылайте пароль и коды даже в обращении.

Как защищён сайт

Используются HTTPS и HSTS, защищённые атрибуты cookie, CSRF-защита, хеширование паролей, ограничение попыток входа, журналирование событий и обязательная двухфакторная аутентификация администраторов. Эти меры снижают риск, но не заменяют осторожность пользователя.