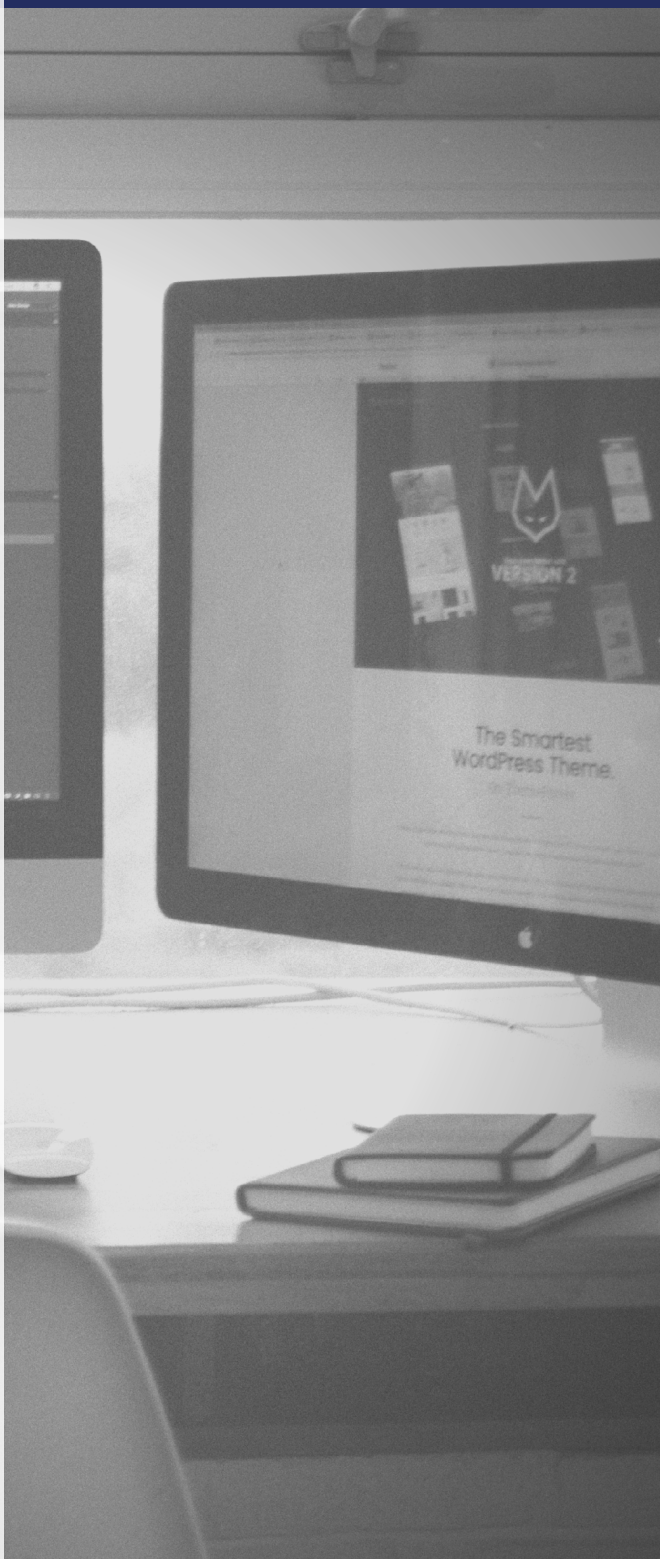
# ПОМНИТЕ О БЕЗОПАСНОСТИ!

Eurasian Bank

## Уважаемые клиенты!

**В связи с возросшей опасностью стать жертвой киберпреступников убедительно просим следовать следующим правилам при работе с системой дистанционного банковского обслуживания (ДБО)**



- Не сохраняйте пароль для доступа в систему ДБО в интернет-браузере и текстовых файлах на компьютере либо на других электронных носителях информации.
- Не передавайте свой пароль от системы ДБО третьему лицу, в том числе работникам банка.
- Избегайте подключений к веб-сайту системs ДБО по баннерным ссылкам или по ссылкам, содержащимся в электронной почте.
- Проверяйте, установлено ли защищенное SSL-соединение с официальным сайтом системы ДБО.
- Избегайте работы с другими веб-сайтами во время сеанса использования системы.
- Не забывайте завершать сессию после завершения работы в системе ДБО.
- Избегайте использование системы ДБО через публичные точки доступа в интернет и гостевые рабочие места (например, интернет-кафе).
- Используйте пароль, графический ключ либо биометрическую аутентификацию для разблокировки мобильных устройств.
- Если вы потеряли мобильное устройство, которое используете для получения SMS-сообщений от банка, или ваша SIM-карта внезапно перестала работать, незамедлительно свяжитесь с банком и обратитесь к своему оператору мобильной связи для блокирования использовавшейся SIM-карты.
- Информируйте банк о случаях несанкционированных транзакций в системе ДБО.
- Избегайте постоянной работы на вашем компьютере под учетной записью с административными полномочиями.
- Не запускайте программы, полученные из непроверенных источников (особую опасность могут представлять программы, полученные по электронной почте или из интернета).
- Не посещайте сайты и не открывайте электронные письма сомнительного характера.
- Используйте лицензионное программное обеспечение и своевременно устанавливайте критические обновления для операционной системы.
- Ежедневно производите обновления антивирусных сигнатур и производите регулярную полную проверку рабочей станции на наличие вирусной активности.
- Используйте дополнительные средства повышения безопасности (межсетевые экраны, программы поиска шпионских компонентов и т. д.).
- Ограничьте доступ к рабочей станции и прочим устройствам для третьих лиц.