РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ
ПРИ РАБОТЕ В СИСТЕМЕ «ИНТЕРНЕТ-ТРЕЙДИНГА»

Уважаемый Клиент:

- Ответственность за хранение личных конфиденциальных данных, ключевого носителя с ключами ЭЦП и паролей возлагается на пользователя системы. Храните ключевые носители, логин и пароль в местах, к которым ограничен доступ третьих лиц.
- Ни при каких обстоятельствах не разглашайте свой логин и пароль, и ни при каких обстоятельствах не передавайте ключевой носитель с ключами ЭЦП - никому, включая сотрудников АО «Halyk Finance». ПАРОЛЬ, ключевой носитель с ключами ЭЦП для входа и работы с Системой - это Ваша личная конфиденциальная информация.
- Не используйте программное обеспечение, предоставляющее удаленный доступ и удаленное управление Вашим персональным компьютером/данными, а в случае обнаружения такого программного обеспечения необходимо его деинсталлировать и принять меры по смене пароля и перегенерации ключа ЭЦП.
- Не сохраняйте ваш пароль в интернет браузере и текстовых файлах на компьютере, либо на других электронных носителях информации, так как это может привести к его краже и компрометации.
- Во время доступа в систему «Интернет-трейдинга», не рекомендуется работать в операционной системе под учетной записью пользователя, который имеет расширенные права в операционной системе, например, «Администратор». Используйте политики безопасности операционной системы для ограничения прав доступа пользователю. Это поможет снизить риск реализации различных атак на рабочую станцию и причинения ущерба от возможных действий деструктивного характера злоумышленников.
- Максимально ограничьте доступ к компьютеру, на котором установлена система «Интернет-трейдинга».
- Ежедневно анализируйте информацию о принятых и непринятых Компанией электронных документах, а также немедленно информируйте Компанию о случаях несанкционированного перевода денег.
- При утере мобильного телефона, на который Вам отправляются SMS-сообщения или при неожиданном прекращении работы SIM-карты, Вам следует, как можно быстрее, обратиться к своему оператору мобильной связи и заблокировать SIM-карту, а также проинформировать об этом Компанию.
- Всегда выходите из системы «Интернет-трейдинга» через ссылку «Выход из системы», в этом случае Ваш сеанс будет прекращен немедленно и корректно.
- По завершению работы в системе «Интернет-трейдинга» отключите и извлеките ключевой носитель с ЭЦП из USB порта компьютера. Не оставляйте ключевой носитель с ключами ЭЦП постоянно подключенным к компьютеру. Подключайте его только при необходимости работы в системе «Интернет-трейдинга.
- Блокируйте компьютер и обязательно извлекайте из USB порта персонального компьютера ключевой носитель с ключами ЭЦП, если требуется покинуть рабочее место.

- Избегайте публичных мест с публичными точками доступа в интернет (таких как интернет-кафе и игровые клубы), для использования системы «Интернет-трейдинга», так как Вы не можете быть уверены, что на компьютерах данных заведений не установлены программы-шпионы, способные скомпрометировать Ваши конфиденциальные идентификационные и персональные данные. Осуществляйте операции со специально выделенного под эти цели персонального компьютера.
- Используйте для работы с системой «Интернет-трейдинга» только проверенные и надежные компьютеры.
- Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем.
- Используйте лицензионное антивирусное программное обеспечение и следите за его регулярным обновлением.
- Регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ.
- Используйте дополнительное лицензионное программное обеспечение: персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам-рассылок» и своевременно обновляйте их.
- Не запускайте программы, полученные не из доверенных источников. Особую опасность могут представлять программы, полученные по электронной почте или скаченные из Интернета.
- Компания владеет всей необходимой информацией и никогда, ни при каких обстоятельствах не осуществляет звонки по телефону, рассылку электронных писем, SMS-сообщений, с просьбой передать реквизиты счета, авторизационные данные, а также не распространяет по электронной почте программы и их обновления.
- В случае компрометации данных или обнаружения несанкционированных транзакций, Вам необходимо обратиться в Контакт-центр Компании по телефону: 8(727) 357 31 77.