Уважаемые Клиенты!

В целях предотвращения рисков, связанных с возможностью **несанкционированного доступа третьих лиц (лиц, не имеющим соответствующих полномочий):**

- к номеру мобильного телефона/адресу электронной почты/ПО «Личный кабинет» (https://lk.ivolgacap.ru/users/sign_up)/системе QUIK (далее - электронные каналы связи), посредством которых Вами осуществляется передача ООО ИК «Иволга Капитал» электронных заявок/поручений/требований на исполнение финансовой операции (сделок (операций) с финансовыми инструментами) с использованием секретного пароля; - к иной касающейся Вас конфиденциальной информации,

Вам необходимо предпринимать меры по исключению возможности несанкционированного доступа третьих лиц к используемым Вами электронным каналам связи для целей передачи документов и информации в ООО ИК «Иволга Капитал» (далее – Компания).

Помните!

Передача логина (идентификатора пользователя), постоянного пароля, одноразовых паролей, контрольной информации и кода клиента, предназначенных для доступа и подтверждения Ваших действий посредством электронных каналов связи, другому лицу означает, что вы предоставляете возможность другим лицам проводить операции с вашими активами. При любом подозрении о получении несанкционированного доступа третьих лиц к конфиденциальной информации, а также в случае утраты Вами данных для доступа к электронным каналам связи вам следует незамедлительно обратиться к сотрудникам Компании по указанным на официальном сайте ООО ИК «Иволга Капитал» в разделе «контакты» телефонам и адресам: Телефон: +7 (495) 150-08-90

EMAIL: info@ivolgacap.com

Риски, связанные с использованием электронных каналов связи и передачи электронных сообщений с использованием простой электронной подписи, включая риск несанкционированного доступа, Вы принимаете на себя в полном объеме.

Ниже приведены рекомендации Компании по защите Вашей информации в целях противодействия незаконным финансовым операциям, включая меры по предотвращению несанкционированного доступа к защищаемой информации:

1. Не сообщайте третьим лицам персональные идентификаторы пользователя и пароли, предназначенные для использования Вами электронных каналов связи: логин, постоянный пароль, одноразовые пароли, контрольную информацию, код клиента;

2. Не используйте в качестве места хранения логина и пароля (конфиденциальной информации) жесткий диск компьютера. Храните указанную информацию в надежном месте, доступ к которому посторонними лицами исключен, извлекая ее только во время сеанса работы с электронным каналом связи;

3. Используйте лицензионное программное обеспечение (операционная система, офисные приложения и др.), полученное из проверенных и надежных источников, своевременно устанавливайте все обновления программного обеспечения, повышающие безопасность;

4. Установите лицензионную антивирусную программу и регулярно обновляйте антивирусные базы данных. Проводите периодическое сканирование компьютера на наличие вирусов. Обратите внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о Вашем пароле;

5. Не используйте взломанные операционные системы и программное обеспечение, во избежание активации злоумышленниками вложенных в данное программное обеспечение вредоносных кодов или программ;

6. Используйте межсетевые экраны (firewall), разрешив доступ только к доверенным ресурсам сети Интернет и только для доверенных приложений. Используйте рекомендуемые настройки безопасности для вашего браузера;

7. На компьютере, используемом для работы с электронным сервисом не рекомендуется работать под учетной записью, обладающей правами администратора;

8. Отключите на компьютере, с которого осуществляется для работы с электронным сервисом в целях исполнения финансовых операций, гостевые учетные записи и возможность дистанционного управления;

9. На компьютере, используемом для работы с электронным сервисом в целях исполнения финансовых операций, не должно быть учетных записей (пользователей) с пустыми паролями.

Пароли должны удовлетворять следующим требованиям сложности:

- длина пароля должна быть не менее 6 символов;
- пароль должен содержать прописные и строчные буквы (a-z, A-Z), цифры, специальные символы (например: !*$%^*()_+|~-=\`{}[]:";'?./).

10. Не реже чем раз в 3 месяца меняйте пароль на учетную запись под которой производятся финансовые операции;

11. Не открывайте файлы и не переходите по ссылкам, полученным от неизвестных отправителей. Не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов;

12. При входе в ПО «Личный кабинет» необходимо убедиться, что в адресной строке web-браузера отображается именно адрес, начинающийся с https://lk.globalcapital.ru/users/sign_up. В случае, если отображаемый адрес отличается от указанного, следует отказаться от дальнейших действий и незамедлительно обратиться в Компанию.

13. Убедитесь в том, что соединение установлено в защищенном режиме, т.е. адресная строка в браузере начинается с https://. При этом в строке состояния или адресной строке браузера должен быть виден значок закрытого замка;

14. Включите систему фильтрации ложных web-узлов (антифишинг) в браузере; если браузер не имеет такой системы, обновите его;

15. Если при входе в Личный кабинет Вы заметили какие-либо несоответствия стандартным запросам или вам позвонили от имени Компании с предложением попытаться войти в систему еще раз, ввести или сообщить пароль, не вводите и не сообщайте никаких данных. Незамедлительно обратитесь в Компанию по телефону: +7 (495) 150-08-90;

16. Не используйте функцию автозаполнения в установках браузера. Это предотвратит использование данных (имя пользователя, пароль и т.д.) сторонними лицами;

17. Следует осуществлять информационное взаимодействие с Компанией только с использованием средств связи (мобильные и стационарные телефоны, интерактивные webсайты, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, предоставленных непосредственно Компанией;

Просим Вас незамедлительно обращаться в Компанию при возникновении подозрений на несанкционированный доступ третьих лиц по указанным на официальном сайте ООО ИК «Иволга Капитал»в разделе «контакты» телефонам и адресам:

Телефон: +7 (495) 150-08-90

EMAIL: info@ivolgacap.com

Помните, что соблюдение указанных правил и своевременное обращение в Компанию помогут существенно снизить угрозу использования ваших данных третьими лицами для мошеннических действий.

В свою очередь, **Компания применяет следующие меры** в целях предотвращения несанкционированного доступа к защищаемой информации:

1. использует для взаимодействия с клиентом посредством электронных каналов связи средства криптографической защиты информации, имеющие сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности;

2. обеспечивает комплекс мер, по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода;

3. осуществляет защиту:

   - информации, содержащейся в документах, составляемых при осуществлении финансовых операций в электронном виде сотрудниками Компании;
   - информации, необходимой Компании для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права Клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;
   - информации об осуществленных Компанией и его клиентами финансовых операциях.