Рекомендации по безопасной работе в Личном кабинете

- Используйте только доверенные компьютеры с лицензионным программным обеспечением. Проверяйте свои устройства на вирусы. Регулярно обновляйте программное обеспечение.
- Используйте последние версии браузеров. Список рекомендуемых браузеров:
  - ✓ Google Chrome
  - ✓ Microsoft Edge
  - ✓ Яндекс.Браузер
  - ✓ Safari
  - ✓ Mozilla Firefox
  - ✓ Opera
- Не передавайте никому данные для входа в Личный кабинет (логин и пароль)
- Используйте сложные пароли, которые вы сможете запомнить, нигде не записывая.
- В целях безопасности рекомендуем менять постоянный пароль для входа в Личный кабинет не менее 1 раза в год.
- Для дополнительной защиты своего Личного кабинета подключите двухфакторную аутентификацию - опцию входа по одноразовому SMS-паролю. Он будет запрашиваться после ввода логина и пароля.
- Убедитесь, что в Личном кабинете в меню «Настройки» указаны Ваши актуальные данные, в том числе номер телефона.
- Всегда корректно завершайте работу в Личном кабинете через пункт меню «Выйти».

Правила безопасной работы в Личном кабинете

- Пароль для входа в Личный кабинет назначается Вами при первом входе и должен содержать не менее 8 символов, состоять из букв, цифр и специальных символов.
- Перед входом в Личный кабинет проверьте адрес web-страницы Личного кабинета. Перед началом работы убедитесь, что web-адрес в адресной строке начинается с «**https**». Личный кабинет доступен только по адресу **https://client.solidbroker.ru**.
- Если адрес сайта отличается от указанного выше, возможно, сайт - поддельный, созданный с целью совершения мошеннических действий. Не вводите на сайте свои личные данные (логин и пароль), если его подлинность вызывает подозрения.
- Для входа в Личный кабинет требуются только логин и пароль. Не сообщайте никому эти данные, нигде не оставляйте их в записанном виде.
  Помните! Мы не попросим Вас для входа в Личный кабинет вводить персональные данные, номер мобильного телефона, или данные Ваших банковских карт для дополнительной идентификации – только логин и пароль. В случае многофакторной аутентификации – дополнительно одноразовый SMS-пароль.
- Убедитесь, что телефон, на который Вы получаете одноразовые пароли для подтверждения операций, доступен только Вам.
- Если Вам пришло SMS с одноразовым паролем для подтверждения поручения, которое вы не совершали, известите Вашего менеджера! Ни в коем случае не вводите и никому не сообщайте пришедший SMS-пароль!

- Не реагируйте на сообщения, в которых Вас просят перезвонить по указанному номеру телефона для разблокировки учетной записи или восстановления доступа к Личному кабинету. Помните, что АО ИФК «Солид» не рассылает сообщений с просьбой уточнить данные поручения. Будьте бдительны и не отвечайте на подобные запросы.
- В случае поступления звонка от имени менеджера Компании с предложением ввести одноразовый пароль для входа в Личный кабинет (вместо SMS-пароля), или отмены проведенного Вами ранее поручения, либо под данным предлогом попытаться уточнить у Вас иные персональные данные - ни в коем случае не вводите и не сообщайте запрошенную информацию. Злоумышленники могут представится кем угодно.
- Если Вы сменили номер мобильного телефона – обязательно сообщите об этом Вашему менеджеру. В случае утери мобильного телефона, на который приходят SMS с одноразовым паролем, немедленно заблокируйте SIM-карту.

Если Вы обнаружили в Личном кабинете операции, которые не совершали, или подозреваете, что Ваши логин и пароль для входа в Личный кабинет стали известны третьим лицам, если Вы потеряли телефон, который обычно используете для подтверждения операций, пожалуйста, незамедлительно обратитесь к менеджеру Компании.