Рекомендации по защите информации

В соответствии с требованиями Банка России АО «АИГ» (далее – «Компания») информирует своих клиентов о возможных рисках получения несанкционированного доступа к защищаемой информации.

В результате несанкционированного доступа к защищаемой информации с целью осуществления финансовых и иных операций, лицами, не обладающими правом их осуществления, могут быть реализованы следующие негативные последствия:

- Совершение незаконных операций по страхованию, подключение и отключение услуг, внесение изменений в ваши регистрационные данные;
- Получение третьими лицами доступа к информации о застрахованных рисках и активах, условиях страхования, а также к персональным данным;
- Получение несанкционированного доступа к информации, содержащейся в документах при осуществлении операций по страхованию и получению страховой премии;
- Нарушение целостности или потеря информации на электронном носителе, что в свою очередь может привести к воспрепятствованию своевременного исполнения клиентом или Компанией своих обязательств по договору;
- Разглашение относящейся к клиенту информации конфиденциального характера:
  - о застрахованных рисках и активов;
  - условиях страхования;
  - персональных данных, содержащихся в договорах страхования;
  - и иной значимой информации.

В целях предотвращения рисков, связанных с получением несанкционированного доступа к защищаемой информации, в том числе при утрате клиентом (представителем клиента) устройства, с использованием которого совершались действия по осуществлению финансовых операций и своевременному обнаружению воздействия вредоносного кода, рекомендуем принять к сведению следующие меры и способы защиты:

- Используйте и храните устройства таким образом, чтобы исключить возможность его хищения и несанкционированного использования;
- Устанавливайте сложные пароли с длинной не менее 8 символов, буквами разного регистра, цифрами, специальными символами, избегайте легко угадываемых комбинаций (ФИО, дата рождения, 1234, qwerty и т. д.). Не используйте один пароль ко всем устройствам и системам;
- Обязательно блокируйте устройства;
- При утере устройств позаботьтесь о смене паролей доступа к системам;
- Обратитесь к своему сотовому оператору для блокирования сим-карты;
- Не сообщайте третьим лицам полученную в СМС-сообщениях и Push-уведомлениях информацию для совершения финансовых операции;
- Используйте лицензионное программное обеспечение, обрабатывающее защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» (Далее - программное обеспечение) и

приложения, скачанные только с официальных магазинов приложений (App Store / Google Play / Microsoft Store) или с сайтов производителей;

- Устанавливайте обновления безопасности используемого программного обеспечения;
- Используйте антивирусное программное обеспечение и встроенные средства межсетевого экранирования (брандмауэр);
- Не посещайте и не вводите конфиденциальную информацию на неофициальных, подозрительных Интернет-ресурсах, а также подозрительных мобильных приложениях;
- Не разглашайте конфиденциальную информацию по телефону или электронной почте, которая может повлечь несанкционированный доступ к системам, конфиденциальной информации или финансовым операциям;
- Используйте программное обеспечение для фильтрации нежелательной почты (спама);
- Не используйте подключение к публичным сетям связи (Wi-Fi) для осуществления финансовых операций или передачи конфиденциальной информации.