Рекомендации клиентам АО «ИК «Газинвест» по соблюдению информационной безопасности в целях противодействия незаконным финансовым операциям.

АО «ИК «Газинвест» доводит до Вашего сведения:

- рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее – вредоносные коды);
- информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- информацию о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) Вами устройства, с использованием которого Вами совершались финансовые операции, контролю конфигурации указанного устройства и своевременному обнаружению воздействия на указанное устройство вредоносного кода.

При осуществлении финансовых операций следует принимать во внимание риск получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления. Такие риски могут быть обусловлены включая, но не ограничиваясь следующими факторами:

- Кража пароля и идентификатора доступа или иных конфиденциальных данных посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных для несанкционированного доступа;

- Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить финансовые операции от Вашего имени;

- Использование злоумышленниками утерянного или украденного телефона (SIM-карты) для получения СМС-кодов, которые могут применяться АО «ИК «Газинвест» в качестве дополнительной защиты финансовых операций;

- Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами АО «ИК «Газинвест», для получения данных и/или несанкционированного доступа к сервисам с этого устройства;

- Получение пароля и идентификатора доступа и/или кода из СМС и/или кодовых идентификаторов и прочих конфиденциальных данных путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником АО «ИК «Газинвест» или использует иную легенду и просит Вас сообщить ему эти секретные данные, или направляет поддельные сообщения с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;

- Перехват электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей конфиденциальной информации, если Ваша электронная почта используется для информационного обмена с АО «ИК

«Газинвест», или, в случае получения доступа к Вашей электронной почте, отправка сообщений от Вашего имени в АО «ИК «Газинвест».

В целях минимизации риска получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления (в том числе в результате воздействия вредоносных кодов), АО «ИК «Газинвест» рекомендует соблюдать ряд профилактических мероприятий.

Обеспечьте конфиденциальность:

- Храните втайне аутентификационные/идентификационные данные и ключевую информацию, полученные от АО «ИК «Газинвест»: пароли, СМС-коды, кодовые идентификаторы и т.д., а в случае вероятной компрометации немедленно примите меры для их смены и/или блокировки;
- Соблюдайте принцип разумного раскрытия конфиденциальной информации, в случае если у Вас запрашивают указанную информацию в привязке к сервисам АО «ИК «Газинвест», по возможности оцените ситуацию и уточните полномочия и процедуру по альтернативным каналам связи.

Проявляйте осторожность и предусмотрительность:

- Будьте осторожны при получении электронных писем со ссылками и вложениями, они могут привести к заражению Вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через электронную почту или интернет-ссылку на сайт, может получить доступ к любым данным и информационным системам на Вашем устройстве;
- Внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под АО «ИК «Газинвест» или его уполномоченных/доверенных лиц;
- Будьте осторожны при работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта;
- Будьте осторожны с файлами из новых или не «доверенных» источников (в т.ч. зашифрованными файлами/архивами, т.к. такого рода файлы не могут быть проверены антивирусным ПО в автоматическом режиме);
- Не заходите в системы удаленного обслуживания с не «доверенных» устройств, которые Вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;
- При подаче поручений и/или ином обращении в АО «ИК «Газинвест» осуществляйте звонок только по номеру телефона, указанному в договоре или на официальном сайте АО «ИК «Газинвест»;
- Имейте в виду, что, если Вы передаете Ваш телефон и/или иное устройство другим пользователям, они могут установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к сервисам и/или системам АО «ИК «Газинвест», которыми пользовались Вы. В связи с этим, при утере, краже телефона (SIM-карты), используемого для получения СМС-кодов или доступа к системам и/или сервисам АО «ИК «Газинвест» с мобильного приложения рекомендуется:

  1) незамедлительно проинформировать об этом АО «ИК «Газинвест»,

  2) целесообразно, по возможности оперативно с учетом прочих рисков и особенностей использования Вашего телефона, заблокировать и перевыпустить

SIM-карту, а также сменить пароли и коды доступа (кодовые идентификаторы) к сервисам и/или системам АО «ИК «Газинвест»;

- При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством, и/или заблокировать доступ, обратившись в АО «ИК «Газинвест» в соответствии с правилами, отраженными в договоре, приложениях к договору и иных документах, связанных с исполнением договора;
- Контролируйте свой телефон, используемый для получения СМС-кодов. В случае выхода из строя SIM-карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи;
- Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Вас.

При обмене информацией через сеть Интернет необходимо:

- Не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;
- Не вводить персональную информацию на подозрительных сайтах и других не известных Вам ресурсах;
- Ограничить посещения сайтов сомнительного содержания;
- Не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ у третьих лиц;
- Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
- Не открывать файлы, полученные (скачанные) из неизвестных источников.
- По возможности избегать подключений личных устройств к сервисам и/или системам АО «ИК «Газинвест» с использованием WiFi-доступа в публичных местах. Для мобильного доступа к сервисам и/или системам АО «ИК «Газинвест» отдавать приоритет использованию каналов операторов сотовой связи.

Обеспечьте защиту устройства, с которого вы пользуетесь услугами АО «ИК «Газинвест», к таким мерам включая, но не ограничиваясь могут быть отнесены:

- Использование лицензионного программного обеспечения;
- Запрет на установку программ, мобильных приложений из непроверенных источников;
- Наличие средств защиты, таких как: антивирусное ПО (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;
- Хранение, использование устройства таким образом, который позволит избежать рисков кражи и/или утери;
- Своевременное обновление операционной системы, особенно в части обновлений безопасности;
- Активация парольной или иной защиты для доступа к устройству, мобильным приложениям;
- Использование сложных паролей и их регулярная смена;
- Ограничение доступа к устройству, исключение (ограничение) возможности дистанционного подключения к устройству третьим лицам.
- Ограничение перехода по ссылкам и установки приложений/обновлений безопасности, пришедших в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени АО «ИК «Газинвест», если Вы сами не

инициировали запрос этой информации от АО «ИК «Газинвест». При возникновении сомнений свяжитесь с АО «ИК «Газинвест», используя контактные данные, указанные на официальном сайте АО «ИК «Газинвест».

Данные меры не гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

В связи с тем, что требования информационной безопасности также могут быть отражены в договорах, регламентах, правилах и иных документах АО «ИК «Газинвест», регламентирующих предоставление услуг, настоящие Рекомендации действуют в части не противоречащей положениям иных документов.

АО «ИК «Газинвест» рекомендует внимательно изучить договор, приложения к договору и иные документы, связанные с исполнением договора на оказание услуг, а также ознакомиться с разделами, посвященными информационной безопасности/конфиденциальности.