В целях защиты информации от воздействия программных кодов, приводящего к нарушению штатного функционирования устройств и оборудования, а также в рамках информирования о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом (у клиента) устройства, посредством которого им совершались действия в целях осуществления финансовой операции (далее – устройство), контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода, ООО УК «Бореа групп» (далее – Управляющая компания) **настоятельно рекомендует**:

- Установить актуальное приложение для защиты Ваших персональных устройств (персональный компьютер, планшет, мобильное устройство), которое защитит от вирусов и шпионских программ Ваши приложения. Такие антивирусные программы предназначены для блокировки опасных сайтов, которые могут содержать вредоносный код и устанавливать вредоносное ПО на Вашем устройстве. Своевременно обновляйте установленное антивирусное приложение. Также рекомендуем использовать антивирусные приложения проверенных и положительно зарекомендовавших себя производителей.
- Использовать на устройстве исключительно лицензионное ПО, не устанавливать ПО, полученное из сомнительных источников.
- Не открывать вложения в письмах электронной почты, полученные от неизвестных Вам отправителей. Если отправитель Вам известен – в любом случае рекомендуется проверить полученный файл антивирусной системой.
- Не посещать сайты сомнительного содержания с устройств, используемых для входа в личный кабинет пользователя услуг Управляющей компании.
- Не проводите конфиденциальные транзакции с использованием общедоступного «Wi-Fi».
- Приобрести отдельную сим-карту для работы с мобильным банком и никому не сообщать в публичном пространстве этот мобильный номер.
- Никогда и никому не сообщать свои конфиденциальные данные, в том числе, но не ограничиваясь, совокупностью логинов и паролей, ПИН-коды, CVV/ CVC-коды, данные электронной подписи и пр. Сотрудники Управляющей компании никогда не требуют указанную информацию.
- В случае сомнений перезванивать лично в Управляющую компанию по номеру, который указан на официальном сайте. Игнорируйте сообщения о необходимости перезвонить в Управляющую компанию по указанному в сообщении номеру, так как существуют мошеннические сервисы подмены номеров, звоните в Управляющую компанию самостоятельно.
- Не выкладывать фотографии и сканы Ваших документов в соцсети (например, паспорт, электронные билеты, чеки за оказанные услуги и т.п.): дополнительная информация только помогает мошенникам.
- Быть бдительными и осторожными, если люди, представляющиеся сотрудниками Управляющей компании, требуют от Вас каких-либо быстрых действий, пытаются напугать, т.к. это распространенные приемы мошенников.
- Не передавать Ваш мобильный телефон и (или) другие устройства третьим лицам, т.к. они могут установить на него ПО, содержащее вредоносный код, а в случае кражи или утраты злоумышленники могут воспользоваться Вашим устройством для совершения противоправных / мошеннических действий. В связи с этим при утрате, краже мобильного устройства максимально оперативно заблокируйте сим-карту.

Управляющая компания информирует о следующих возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления:

- риски разглашения конфиденциальной информации, персональных данных (например, информации об активах, персональной информации и пр.);
- совершение финансовых операций с активами клиента третьими лицами, не обладающими правом их осуществления, а также совершение ими иных действий (например, внесение изменений в регистрационные данные клиента, изменение параметров услуг и пр.);
- вредоносное воздействие на устройства и оборудование.

При любом подозрении на мошенничество незамедлительно обратитесь в Управляющую компанию!