РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО КОДА В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

В рамках Договора с Обществом с ограниченной ответственностью «Современные Фонды Недвижимости» (далее - ООО «СФН», Общество) клиентам Общества предоставляется возможность совершать операции и получать информацию через Удаленные каналы обслуживания, к которым относятся:

- Личный кабинет клиента на сайте Общества (далее - Личный кабинет);

Использование Удаленных каналов обслуживания сопряжено с возможными рисками получения несанкционированного доступа к конфиденциальной информации лицами, не обладающими правом доступа к ней. К конфиденциальной информации Клиента относятся:

- информация об имуществе, принадлежащем Клиенту;
- информация о совершенных операциях с имуществом Клиента;
- информация, содержащаяся в оформленных Клиентом распоряжениях;
- информация, необходимая для удостоверения Клиентами права распоряжения имуществом;
- информация о доходах, выплаченных Обществом Клиенту за налоговый период;
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении деятельности негосударственного пенсионного Общества.

Уведомление Общества об изменении и, соответственно, неактуальности обрабатываемых Обществом персональных данных Клиента является ответственностью Клиента. В случае изменения персональных данных Клиента, обрабатываемых Обществом, Клиент или его представитель обязан уведомить об этом Общество путем направления соответствующего обращения и предоставить в Общество актуальные сведения.

Ниже приведены рекомендуемые Обществом меры по снижению рисков получения несанкционированного доступа к конфиденциальной информации Клиента.

Важно! Передача третьему лицу (в том числе работнику Общества) Логина и Пароля от Личного кабинета, Сбербанк ID или иной контрольной информации, предназначенной для доступа и подтверждения операций через Удаленные каналы обслуживания, предоставляет данному лицу доступ к конфиденциальной информации. Обезопасьте себя от подобных действий.

При любых подозрениях на мошенничество (получение от Общества SMS/Push/e-mail-сообщения о якобы совершенной операции или SMS/Push/e-mail-сообщение, которое вызывает сомнения), следует незамедлительно обратиться в Контактный центр Общества по номеру телефона, указанному на официальном сайте Общества:

- 900 (бесплатно с мобильных номеров на территории России)
- +7 (495) 500-55-50 / 8 (800) 555 55 50 (для звонков по всему миру, стоимость звонка – по тарифам вашего оператора связи).

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В ЛИЧНОМ КАБИНЕТЕ НА САЙТЕ ОБЩЕСТВА

Вход в Личный кабинет осуществляется с помощью Сбер ID. Для входа в Личный кабинет не требуется вводить никакой дополнительной информации.
Внимание! Если для входа в Личный кабинет предлагается дополнительно ввести любую другую информацию или дополнительные данные (данные платёжных карт, данные паспорта или иных документов, другую информацию), это указывает на мошенничество! В таких случаях необходимо немедленно прекратить сеанс работы в Личном кабинете и срочно обратиться в Общество по номерам, указанным на официальном сайте Общества:

- 900 (бесплатно с мобильных номеров на территории России)
- +7 (495) 500-55-50/ 8 (800) 555 55 50 (для звонков по всему миру, стоимость звонка – по тарифам вашего оператора связи).

При работе в Личном кабинете (https://my.sfn-am.ru/login) всегда проверяйте, что с сайтом установлено защищенное соединение справа или слева (в зависимости от используемого Вами браузера) в адресной строке браузера должно быть изображение запертого замка, обозначающее наличие защищенного соединения.

При работе с Личным кабинетом должны использоваться только надежные и проверенные точки доступа Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi. Точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями мошенников, направленными на получение доступа к конфиденциальной информации.

Для исключения компрометации конфиденциальной информации и хищения средств, запрещено подключать к услугам Общества номера телефонов, оформленные на третье лицо.

Запрещено устанавливать на устройства, которые используются для доступа к Личному кабинету, приложения, полученные по ссылкам от не проверенных или неизвестных источников.

Общество не рассылает ссылки или указания на установку приложений через сообщения SMS, Push, MMS или e-mail.

На всех устройствах, используемых для доступа к Личному кабинету (стационарный или переносной компьютер, мобильное устройство):

должно использоваться современное антивирусное программное обеспечение и выполняться регулярное должно производиться обновление баз данных (сигнатур);

- должна регулярно выполняться полная антивирусная проверка устройства для своевременного обнаружения вредоносных программ;

- должны своевременно устанавливаться обновления операционной системы, рекомендуемые компанией производителем;
- должен осуществляться контроль конфигурации устройства и установленных приложений;
- по возможности, должно использоваться дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты устройства: персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ»-рассылок и пр.

Доступ в Личный кабинет должен завершаться путем выбора пункта «Выход» в меню.

ЗАЩИТА ОТ SMS/PUSH/E-MAIL МОШЕННИЧЕСТВА

Мошеннические SMS/Push/e-mail сообщения, как правило, информируют о совершенном переводе (списании) денежных средств или содержат другую информацию, побуждающую перезвонить на указанный в SMS/Push/e-mail сообщении номер телефона, пройти по ссылке или открыть вложенный файл для уточнения информации. Зачастую такие сообщения замаскированы под официальные сообщения Общества, а мошенники представляются сотрудниками службы безопасности или специалистами службы технической поддержки Общества и в убедительной форме предлагают срочно провести какие-либо действия или предоставить конфиденциальную информацию.

В случае получения подозрительных SMS/Push/e-mail сообщений запрещено:

- перезванивать на номера телефонов, проходить по ссылкам, указанным в подозрительном сообщении, или открывать прилагаемые файлы и архивы;
- предоставлять конфиденциальную информацию (Фамилия Имя Отчество, данные паспорта или иных документов, реквизиты платёжных карт (номер карты, срок ее действия, ПИН, CVV2/CVC2/ППК2), Контрольная информация, Логин (Идентификатор пользователя) и Пароль от Личного кабинета), в том числе посредством направления ответных SMS/Push/e-mail сообщений.

Следует незамедлительно обратиться в контактный центр Общества по номеру телефона, размещенному на официальном сайте Общества:

- 900 (бесплатно с мобильных номеров на территории России)
- +7 (495) 500-55-50/ 8 (800) 555 55 50 (для звонков по всему миру, стоимость звонка – по тарифам вашего оператора связи).