Автор: Administrator
12.04.2024 06:00 - Обновлено 15.04.2024 15:03

Цифровизация позволила сделать нашу жизнь значительно комфортнее. Теперь с помощью онлайн-сервисов можно оплачивать коммунальные услуги, записываться на прием к врачу и даже управлять собственной недвижимостью. При этом вместе с технологиями развиваются и схемы обмана пользователей. Эксперты Росреестра пояснили, как собственники могут самостоятельно защитить сведения о своих объектах недвижимости. Для защиты собственности специалисты рекомендуют внести информацию об адресе электронной почты в ЕГРН. В этом случае правообладатель может оперативно получать из Росреестра информацию о любых действиях с его недвижимостью. Указать адрес электронной почты можно при подаче заявления на осуществление учетно-регистрационных действий. Для этого адрес электронной почты нужно указать в нужной графе заявления. Если права уже зарегистрированы, но в ЕГРН отсутствует адрес электронной почты, подать заявление о внесении данных сведений можно в любом офисе МФЦ, в личном кабинете на сайте Росреестра, а также по почте – в таком случае подпись на заявлении должна быть нотариально удостоверена. Еще один способ защиты своей недвижимости – подача заявления о невозможности государственной регистрации перехода, ограничения (обременения), прекращения права на принадлежащие объекты недвижимости без вашего личного участия. В ЕГРН будет внесена соответствующая запись, и документы, поданные без личного участия собственника (например, по доверенности), рассматриваться не будут. Их возвратят обратно заявителю. Исключением являются случаи, когда основанием для учетно-регистрационных действий является вступившее в силу решение суда или требование судебного пристава-исполнителя. В этом случае обозначенная выше запись в ЕГРН не учитывается. Такое заявление можно подать в отделениях МФЦ, в личном кабинете на сайте Росреестра (в этом случае нужно иметь сертификат усиленной квалифицированной электронной подписи), а также в офисах Федеральной кадастровой палаты (если заявление подается экстерриториально). Это можно сделать и по почте – тогда подпись на заявлении должна быть нотариально удостоверена. Не стоит забывать о базовых правилах информационной безопасности: • храните пароли и конфиденциальные данные в автономном режиме; • проверяйте безопасность подключения к сайтам и используйте только защищенное соединение (в адресной строке браузера перед адресом сайта должен стоять зеленый замок и должно быть прописано HTTPS); • оставляйте личные данные только на сайтах с защищённым соединением; • защитите свои учетные записи с помощью надежных паролей и двухфакторной аутентификации, не используйте одинаковый пароль для разных ресурсов; • ни в коем случае никому не сообщайте свои пароли и другие личные данные; • не нажимайте на подозрительные ссылки и не заходите на подозрительные сайты; • не открывайте вложения от неизвестных отправителей, а все вызывающие недоверие письма отправляйте в папку «спам»; • своевременно обновляйте свое устройство и приложения; • выбирайте сети с защищенным подключением и не используйте общественные сети Wi-Fi для передачи конфиденциальной информации; • дважды проверяйте достоверность информации онлайн.