编辑：廖 琼
排版：封培林 校对：董颖佩

住房租赁新规今起正式施行

如何破解租房难题，专家给出意见

隔断房、甲醛房、押金难退、虚假房源……近年来，我国住房租赁市场不断发展，但也出现不少市场乱象，困扰广大租客与房东。自9月15日起，《住房租赁条例》正式施行，将进一步规范住房租赁活动，推动住房租赁市场迈向高质量发展。

“作为我国首部住房租赁领域行政法规，条例的施行标志着住房租赁市场从粗放发展迈向法治化、规范化新阶段，为破解‘重购轻租’难题、实现‘住有所居’民生目标提供了系统性制度保障。”北京房地产中介行业协会秘书长赵庆祥说。

当前，我国城镇租房人口超过2亿，在北上广深等一线城市，租房人口占常住人口比例超过40%。住房租赁市场的总量规模大，经营主体多元，产品类型和服务方式更加多样。

居住环境直接关系着居民的生活质量和身心健康。赵庆祥说，针对部分租赁房屋设施陈旧、卫生条件差、安全隐患多等现实痛点和隔断房、甲醛房等突出问题，条例要求用于出租的住房应当符合建筑、消防、燃气、室内装饰装修等方面的法律、法规、规章和强制性标准，且明确规定租住人数上限和人均最低租住面积应符合相关标准以及非居住空间不得单独出租用于居住，从源头上保障承租人能够获得安全、健康、相对舒适的居住环境。

针对押金难退这一常见纠纷，条例明确“出租人收取押金的，应当在住房租赁合同中约定押金的数额、返还时间以及扣减押金的情形等事项。除住房租赁合同约定的情形以外，出租人无正当理由不得扣减押金”，并规定住房租赁经纪机构和网络平台经营者不得代收、代付住房租金、押金。

值得注意的是，针对住房租赁合同备案，条例除了为出租人提供办理备案的通道，即通过住房租赁管理服务平台等方式向租赁住房所在地房产管理部门备案，还在出租人未办理时，给予承租人办理备案的权利，以满足承租人的现实需求。

专家表示，住房租赁合同备案有助于规范租赁合同管理，能进一步规范市场、稳定租赁关系，有效遏制随意涨租、克扣押金、暴力驱赶等乱象，打击“二房东”行为，提升房源质量与服务水平。此外，承租人可凭备案合同享受公积金提取等公共服务。

赵庆祥说，除了规范租赁双方的行为，条例将经营主体细分为个人出租人、住房租赁企业、住房租赁经纪机构、网络平台经营者四类，实施差异化监管，对相关经营主体“要做什么”“不能做什么”提出了要求：

住房租赁合同连续履行达到规定期限的，出租人按照有关规定享受相应的政策支持，承租人按照有关规定享受相应的基本公共服务。

住房租赁企业应当具备与其经营规模相适应的自有资金、从业人员和管理能力，发布的住房地址、面积、租金等房源信息应当真实、准确、完整，不得发布虚假或者误导性房源信息；住房租赁经纪机构应当具备与其经营规模相适应的自有资金、从业人员和管理能力，并将其从业人员名单向所在地县级以上地方人民政府房产管理部门备案；网络平台经营者应当核验住房租赁信息发布者的真实身份信息，未履行核验责任的，会受到相应处罚。

清华大学房地产研究中心主任吴璟说，条例有助于营造更加规范、公平的行业环境，防止“劣币驱逐良币”现象，推动出租人尤其是住房租赁企业持续提升租赁产品和服务品质，并促进住房租赁市场供给端机构化和长期化。

在监管层面，吴璟说，过去一段时间里各城市在保障性租赁住房方面已经投入大量资源，条例进一步对地方政府在住房租赁市场和租赁行业发展进程中应该做什么、应该怎么做给出了详细指引。条例从租赁市场监测和信息公布、对住房租赁活动流程的管理以及对住房租赁活动的监督执法等三个方面明确了地方政府的具体职责。在租金方面，条例要求“设区的市级以上地方人民政府应当建立住房租金监测机制，定期公布本行政区域内不同区域、不同类型住房的租金水平信息”。

“条例的施行是住房租赁法治化的重要里程碑。”赵庆祥说，下一步需重点推进三项工作：一是加快制定相关配套政策；二是全面深入开展条例的普法宣传；三是督促县级以上地方人民政府房产管理部门建设完善住房租赁管理服务平台。“如此，才能将条例的立法本意落地成为‘良法善治’，实现法治化引领住房租赁市场高质量发展。”

（新华社北京9月14日电）

工商银行柳州分行2025年网络安全宣传周活动

网络安全为人民 网络安全靠人民

——以高水平安全守护高质量发展

当前，黑客攻击手段持续升级，数据泄露事件频发，为切实提升全民网络安全防护意识与风险应对能力，筑牢信息安全防线，本文将通过网络安全典型案例剖析和安全提示，引导大众学习信息安全防护技巧，筑牢终端“安全锁”、守好数据“防火墙”、织密信息“防护网”。

信息安全面临的威胁与挑战

网络安全威胁不断升级

随着互联网的普及和数字化进程的加速，网络安全威胁日益增加。黑客攻击手段日益狡猾和复杂，包括钓鱼攻击、勒索软件、分布式拒绝服务攻击等网络犯罪，甚至利用0-day漏洞发起攻击，给个人和企业带来严重威胁和损失。

数据安全与隐私保护问题严峻

近年来，全球范围内个人信息泄露、企业数据外泄等事件频发，包含数据窃取或泄露、数据损毁、数据非法利用、数据非法出境等风险，涉及金融、医疗、教育等多个领域，严重威胁个人隐私和企业的安全运营。

终端用户安全不容小觑

尽管系统和网络都采取了严格的安全措施，但用户往往是安全链中最薄弱的环节。员工、前员工、合作伙伴等内部人员可能因误操作或采取恶意行为窃取数据、破坏系统或植入恶意软件，导致数据泄露、系统瘫痪等，给企业带来难以估量的损失。

风险案例剖析

网络钓鱼

攻击者通过伪装成可信任实体的方式，骗取用户的敏感信息。钓鱼攻击通常以欺骗性的电子邮件、诱使用户回复邮件、点击邮件正文的恶意链接或打开邮件附件植入木马或间谍程序，进而窃取用户敏感数据，或者在设备上执行恶意代码实施进一步的网络攻击活动。

安全提示：

1.谨防陌生邮件：发件人通常为乱码邮箱，伪装成官方邮箱、冒充熟人邮箱。

2.辨别邮件内容：主题可能包含账号锁定、包裹滞留、社保异常等诱导性关键词。

3.慎点邮件附件：一般含有“发票”“通知单”“详情请查收附件”等都可能藏病毒。

4.慎点邮件链接：链接通常诱导用户点击，并跳转至要求填写身份证号、密码等个人信息的页面。

口令攻击

攻击者通过利用各种技术手段，非法获取、破解或绕过用户身份验证，从而获得对保护系统、账户、网络或资源的未授权访问权限。

安全提示：

应避免设置弱密码、常用密码、默认密码以及易被猜到的密码；不得使用简单的加密或编码方式存储用户密码，同时应定期修改密码。

个人信息安全保护小贴士

◆网上购物谨防钓鱼网站，要仔细检查网络域名是否正确，不轻易接受和安装不明软件，不随意点击链接，不轻易提供账户、密码等信息。

◆将公私邮箱分开，不轻易泄露邮箱地址，不点击陌生邮件，不下载来历不明的附件，不点击可疑链接。

◆妥善保管处理快递单、车票、购物小票等包含个人信息的单据。

◆不轻易添加陌生人的微信，不在社交平台透露个人姓名、身份证、地址等个人信息。

◆不随意丢弃或出售未经处理包含个人信息的手机、电脑等电子设备。

◆对个人重要信息进行防护，比如在身份证复印件标注“仅限××业务使用”。

◆加强账户密码复杂性，使用包含数字、字母和符号的密码，并定期更换。

◆电脑、手机等电子设备应该安装安全软件，并定期进行安全扫描。

◆避免在不安全的环境中使用个人信息，如公共Wi-Fi。

（工商银行柳州分行）