

多家银行宣布清理“沉睡账户”

账户里的余额还能取吗？



近日，多家银行发布公告称，将对长期不动户进行清理，包括个人长期不动户和单位长期不动户。各家银行对长期不动户的认定标准有所不同，但普遍针对低余额、长期无主动交易的账户。这些账户里的余额还能正常取出吗？如何避免账户成为“长期不动户”？

多家银行密集发布公告

兴业银行称，自10月15日起，该行将按照调整后认定标准每日滚动管控符合条件的账户，采取限制资金进出的保护措施。中国银行亦指出，将对符合相关标准的个人结算账户采取限制出账交易的管控措施，在重新识别客户身份后为其恢复账户功能。

据不完全统计，10月以来，凤台农村商业银行、葫芦岛银行、湖北枝江农商银行等多家地方商业银行均纷纷发文提示，银行将进一步清理个人长期不动户。

同时，一些银行对长期不动户认定标准进行了调整。兴业银行近日发布公告称，调整前，该行长期不动户认

定标准为账户余额100元(含)以下，无该行个人贷款还款、代销基金产品、理财产品、三方存管等签约关系且账户连续180天(含)以上未发生任何非结息交易的个人人民币银行结算账户(金融社保卡、公积金卡除外)。调整后，该行长期不动户认定标准为账户余额10元(含)以下，无该行个人贷款还款、代销基金产品、理财产品、三方存管等签约关系且账户连续365天(含)以上未发生任何非结息交易的个人人民币银行结算账户(金融社保卡、公积金卡除外)。从10月15日起，兴业银行按照调整后的认定标准每日滚动管控符合条件的账户。

C 原因：防范电信网络诈骗风险

长期不动户也叫“睡眠账户”，通常是指一定时间及以上未发生主动交易且账户内仍有余额的个人银行账户。业内人士表示，清理长期不动户是监管要求，更是防范电信诈骗、洗钱等违法行为的重要一环。

业内人士提示，长期不动户浪费金融资源，也使消费者面临电信

网络诈骗的风险。长期不动户会导致消费者的资金在银行账户中闲置，并且可能增加账户管理费等不必要支出，影响消费者财产权益。另外，消费者往往遗忘长期不动户有关情况，很难关注到账户变动，一旦个人敏感信息泄露，易被不法分子盗用进行洗钱、电诈等非法活动。

C 建议定期关注整理个人账户

综合来看，各家银行对长期不动户的认定标准并不完全一致，消费者若不能确认相关银行账户是否在清理范围内，需进一步向银行进行查询。

银行在清理长期不动户的过程中，客户可根据自身需求，选择继续使用账户或销户等。比如，兴业银行提示，如银行账户属于长期不动户认定范围但仍需使用的，客户需在该行管控之前任意办理一笔存取现、消费或转账业务，避免账户被限制使用造成不必要的麻烦。若账户已被限制使用，客户可持本人有效身份证件及银行卡(折)，至该行网点进行客户身份核

实，或通过手机银行重新激活使用。

储户平时该怎么管理自己的银行账户？业内人士建议：

第一，每个月应该用云闪付一键查卡的功能，花一分钟自查自己究竟有多少“沉睡卡”。

第二，把不用的卡都注销，只保留必要的账户。

第三，对确实要保留的卡定期存款10块。

专家提示，这不是麻烦，而是保护钱包的好习惯。不要把个人账户用于经营，不要用于出租、出借。这些都是常见的风险点，有时会形成大麻烦。

C 银行卡被冻结，可到银行网点恢复账户功能

多家银行人士表示，持卡人持本人身份证件、银行卡等前往银行网点办理卡片激活业务后，可将卡片中的资金取出。

此外，多家银行还提示，银行在清理长期不动户过程中不会要求客

户通过短信、电话等任何方式提供密码、短信验证码等敏感信息，不会发送与账户销户、销户清理等相关的手机链接，也不会以任何理由要求客户给指定账户进行资金操作。

(综合央视网、央广网、新京报)

全力守护“北京时间”安全 国家安全机关破获美国国家安全局重大网络攻击案

据国家安全部微信公众号消息，近期，国家安全机关破获一起美国重大网络攻击案，掌握美国国家安全局网络攻击入侵中国国家授时中心的铁证，粉碎美方网攻窃密和渗透破坏的图谋，全力守护“北京时间”安全。

国之重器不容有失

国家授时中心位于陕西省西安市，承担“北京时间”的产生、保持和发播任务，为国家通信、金融、电力、交通、测绘、国防等行业领域提供高精度授时服务，还为测算国际标准时间提供重要数据支撑。国家授时中心自主研发了世界领先的时间自主测量系统，还建设有国家重大科技基础设施——高精度地基授时系统，相关设施一旦遭受网攻破坏，将影响“北京时间”的安全稳定运行，引发网络通信故障、金融系统紊乱、电力供应中断、交通运输瘫痪、空天发射失败等严重后果，甚至可能导致国际时间陷入混乱，危害损失难以估量。

机关算尽原形毕露

经国家安全机关缜密调查发现，美国安局针对国家授时中心的网攻活动蓄谋已久，呈现递进式、体系化特点。2022年3月25日起，美国安局利用某境外品牌手机短信服务漏洞，秘密网攻控制国家授时中心多名工作人员的手机终端，窃取手机内存存储的敏感资料。2023年4月18日起，美国安局多次利用窃取的登录凭证，入侵国家授时中心计算机，刺探该中心网络系统建设情况。2023年8月至2024年6月，美国安局专门部署新型网络作战平台，启用42款特种网攻武器，对国家授时中心多个内部网络系统实施高烈度网攻，并企图横向渗透至高精度地基授时系统，预置瘫痪破坏能力。

国家安全机关发现，美国安局网攻活动多选在北京时间深夜至凌晨发起，利用美国本土、欧洲、亚洲等地的虚拟专用服务器作为“跳板”隐匿攻击源头，采取伪造数字证书绕

过杀毒软件等方式隐藏攻击行为，还使用了高强度的加密算法深度擦除攻击痕迹，为实施网络攻击渗透活动可谓无所不用其极。国家安全机关见招拆招，固定美方网攻证据，指导国家授时中心开展清查处置，斩断攻击链路，升级防范措施，消除安全隐患。

贼喊捉贼霸权嘴脸

近年来，美国强推网络霸权，一再践踏国际网络空间规则。以美国为首的间谍情报机关任性妄为，持续针对中国、东南亚、欧洲及南美洲等地实施网攻活动，入侵控制关键基础设施，窃取重要情报，监听重点人员，肆意侵犯他国网络主权和个人隐私，严重危害全球网络安全。美方还惯于利用其在菲律宾、日本以及中国台湾省等地的技术阵地发动网攻，从而达到隐藏自身、嫁祸他人的目的，可谓损招用尽。同时，美方还贼喊捉贼，屡屡渲染“中国网络威胁论”，胁迫他国炒

作所谓“中国黑客攻击事件”，制裁中国企业，起诉中国公民，妄图混淆视听，颠倒黑白。铁的事实证明，美国才是真正的“黑客帝国”，是网络空间的最大乱源。

国家安全机关提示

国家安全机关依法防范打击网络间谍活动，对国内机关、团体、企业事业单位和其他社会组织开展反间谍安全防范指导和检查。关键基础设施运营者要履行本单位反间谍安全防范工作主体责任，定期对从业人员开展网络安全教育、培训，采取反间谍技术安全防范措施，防范、制止境外网络攻击、入侵、窃密等间谍行为。公民和组织应当支持配合国家安全机关开展网络反间谍工作，针对发现的疑似网络间谍行为，及时通过12339国家安全机关举报受理电话、网络举报平台(www.12339.gov.cn)、国家安全部微信公众号举报受理渠道或直接向当地国家安全机关进行举报。

(央视网)