AI 新手三大坑与避坑清单

资料编号：L1-3 ｜ 免费资料包 · 认知地基 ｜ 来来自媒体工作室出品

适用：开始用 AI 干活、想搞自动化的人

说明：以下三个坑，我全踩过，不是网上抄来的。每条=我当时怎么想的 + 后来怎么栽的 + 现在怎么改。

坑一 • 贪多：一次装一堆工具，哪个都没吃透

当时怎么想：刚发现 WorkBuddy 能装技能（skill），一口气装了十几个——出稿的、做图的、整理表格的、提链接的，看着满满一屏，觉得自己武装到牙齿。

后来怎么栽的：真干活时反而懵了——这个功能在哪个技能里？两个技能功能重叠用哪个？每个都是半吊子，最后常用的只有一两个，其余全是摆设，还占内存、拖速度。

现在怎么改：**先用透一个，再装下一个。** 一个技能至少真实用满一周、确定离不开了，才考虑加新的。工具清单同理：对话工具留 1-2 个、生图留 1 个、工作台留 1 个，够了。

记住：**工具是拿来出活的，不是拿来集邮的。** 你需要的不是"几十个工具"，是"每个工具都有一个用熟了的案例"。

坑二 • 全自动：把发布、上架、付款全交给 AI

当时怎么想：自动化多省事啊——让它每天自动发文、自动上架商品、自动回复客户，我躺着收钱。

后来怎么栽的：我公众号发内容时用过诱导关注的词，被平台判违规处理过（申诉整改才恢复）。那次让我后脊发凉：**如果当时是"全自动"直接发出去的，违规的后果连补救的机会都没有。** 还有一次差点让它自动上架商品，价格参数填错的话，就是真金白银的损失。

现在怎么改：定死一条规矩——**自动化只做到"草稿"这一步，发布、上架、付款永远人工终审。**

- - 发文 → 推到草稿箱，我自己看一遍再发
- - 上架 → 生成好所有素材，我核对价格再传
- - 涉及钱、承诺、隐私的回复 → 必须留人工审核

记住：**自动化替你干 80% 的活，剩下的 20% 是"看一眼再点发布"。这一眼，值回所有风险。**

坑三 • 给密码：把账号密码、验证码交给 AI

当时怎么想：有个工具说能"全自动帮我管理多平台账号"，省得我每天登录，差点就填了密码授权。

后来怎么醒的：我给自己立过一个铁律：**AI 和自动化只碰"能公开的部分"**——写文案可以、整理表格可以、推草稿可以；但账号密码、验证码、支付、实名，这些**永远自己来**。工具权限越大，被滥用时后果越重。网上的"改版工具"更要警惕，可能夹带私货。

现在怎么改：

- - 任何要账号密码、验证码的环节，一律自己操作，不让自动化碰
- - 从正规渠道装工具（官方仓库/官方发布页），装完重要文件先备份
- - 发现工具要"读取全部账号数据"，默认拒绝

> 记住：**AI 再像人，它也是程序。密码这种事，只在你自己的手指尖上。**

可打印避坑清单（每周自查一次）

用前问三句

- - ☐ 这个工具/技能，我是真要用，还是只是"想拥有"？
- - ☐ 这件事让 AI 干，最坏会坏到什么程度？我兜得住吗？
- - ☐ 它要的权限，是不是超出了它该干的活？

自动化红线

- - ☐ 发布类动作：只到草稿，人工终审 ✓
- - ☐ 上架/改价/付款：全部人工，AI 只备料 ✓
- - ☐ 账号密码/验证码：永不给 AI、不给插件 ✓
- - ☐ 涉及承诺、收益、疗效的话术：人工过一遍再发 ✓

日常习惯

- - ☐ 关键信息（数字/书名/法规）用前自己核一遍 ✓
- - ☐ 重要文件先备份，再让 AI 批量操作 ✓
- - ☐ 工具只从正规渠道装 ✓

一句话收尾

> **AI 是加速器，不是方向盘。** 加速的事交给它，方向盘——发布权、密码、钱——永远握在自己手里。

> 完整版资料 + 每周新课 + 一群同路人，都在共学群里。
>
> 进群方式：从来来任意一篇内容找到入口，或直接私信问。欢迎转发；请勿商用。

完整版 + 每周更新，进共学群领取

加「AI 小白·进阶学习交流群」→ 群公告下载全套资料

欢迎转发给需要的朋友，请勿商用
