密码修改、账号忘记等申诉，黑客通过收集大量被攻击者的信息，利用社会工程学的方法，让客服把目标账号的密码重置，从而获得重要账号。

张雪松举例，有一个“1 元购 iPhone”的案例，是明显的逻辑漏洞。“当时网站开发时，企业没有很好的流程设计，黑客通过篡改付费订单数据包，在传输过程中将 999 的价格改为 1 元，发送订单给客户，最后真的购买成功了。”张雪松说，我们在测试时建议这家企业，必须做二次验证和比对，防止薅羊毛行为发生。

《2018 网络黑灰产治理研究报告》（以下简称：《报告》）也剖析了治理网络黑产的新方法。2017 年下半年，阿里巴巴钓鱼网站检测系统开始对已知风险进行及时防控阻断，2018 上半年各钓鱼风险呈下降趋势，电商类欺诈下降 94%，公检法欺诈下降 48.9%。

对于“拖库”、“撞库”等多种网络犯罪行为，《报告》指出，阿里安全专门进行了日常化布防和拦截，一旦发生拖库撞库，从数据上就能感知。阿里巴巴数据显示，目前其识别出的机器行为弹出打扰率已控制在极低范围内。同时，阿里巴巴 DDoS 防御系统也已覆盖了阿里整体生态业务，仅 2017 年就累积防御了 2400 多次攻击。

那么，除了第三方安全机构，平台、用户、供应商该如何系统性地防范黑产攻击风险？张雪松认为，从企业安全角度分析，一方面企业要建立用户行为的分析监控措施，对于不活跃、异常的用户进行降级、降权处理，甚至通过深度认证、条件锁定、手势刷脸等方式联动规避，比如羊毛党账号，通常会有“集中性”“批量化”等通用规律，筛选出来，标记为异常账号，定期监控从而提高安全性。

当然，企业在做个人信息处理时，还可分别存储、隔离，将身份信息和其他可识别信息，区分开来，降低危险系数。比如，一些大平台已经采取“虚拟号隐藏”“骚扰号屏蔽”的方法了，但在高富平教授看来，打击黑灰产的关键仍在于，各方一定要把自己的员工管好，防止“内鬼”。

“如果没有内鬼泄露信息，黑客纯粹是少数，像腾讯、阿里等大平台对数据看得很紧，但因合作的产业链条很长，真正泄露的环节还是在合作伙伴。”高富平说，一旦数据交给合作伙伴，就会失控，单靠遵循法律及合同，本质上是一个不确定的事情。

据媒体报道，2018 年破获的一起验证码黑产案件中，网络黑灰产团伙就涉及与广西、贵州、四川等多省份运营商“内鬼”勾结，利用未投入市场未激活的“空号卡”，搭建平台连通运营商服务器用以注册账号、收发验证码。而这类运营商如果能被打掉的话，对于黑产来说，无疑是“斩首行动”。

站在用户角度，为防止账号泄露，要养成良好的上网习惯。比如不轻易注册账号、不要一个账号登录多个网站、公众 wifi 不要乱用、密码要定期修改等。此外，准备一个保护身份，在不重要的网站登录时，使用虚假身份、虚假姓名等，有必要时，还可准备一个副号，对外提供副号，从源头上就可做好信息安全筛选的第一关。

补法规：重新定义个人信息流通界限

既然防范的技术已经十分成熟，网络黑产为何仍然屡禁不止，无法彻底铲除？

高富平教授分析，除了技术层面对隐私的保护多集中在防范层面外，根源问题还在于整个社会的个人隐私文化的缺失。新浪曾发起一个微博投票，话题是关于百度 CEO 李彦宏的观点“中国人愿意用隐私换便利，你认可吗？”，投票结果有高达 82.4% 的人认为“我的隐私不容任何侵犯”。但实践证明，中国网民对个人隐私的保护意识往往是缺乏的，排除 App 供应商以无法正常使用 App 而逼迫用户同意隐私条款的情况，多数用户就算点击了“同意”，也会出于懒、省事，鲜少点开细究其中的条文细则，这必然会导致源头上的失控。

> **黑灰产应该分开打击或规制，**而我国目前的法律条文，并未达到理想状态且存在一定漏洞。