以为在网络上转角遇到爱，不料却掉进了爱情的“屠宰场”。

杀猪盘诈骗并不新奇，但受害者还是屡屡出现。近日央视报道，今年4月江苏常州警方接到报警，吴女士表示自己在婚恋网站认识的男友声称炒数字货币赚钱，结果被其骗走1500万元。经过近半年侦查，直到不久前常州警方抓获该诈骗团伙，370余起涉案总价值约1.2亿元。再如，近日钦州市公安局钦北分局打掉一个以“杀猪盘”形式实施诈骗的电信诈骗团伙，涉案金额高达300余万元。

腾讯110安全运营专家小雨今日告诉第一财经记者，去年时，杀猪盘受害者男女比例没有差异，但到了今年逐步向女性倾斜，杀猪盘诈骗举报者中女性近70%，骗子大多通过婚恋平台、交友软件找目标，精准定位受害者，手法链条环环相扣、结构完整。在今年的各类网络诈骗类型中，杀猪盘诈骗的受害者受损金额最大。

杀猪盘诈骗，只是网络诈骗的冰山一角。如今互联网诈骗的运作模式正在呈现专业化、公司化、链条化的趋势，犯罪手段也变得更加智能，并且已经逐渐形成了“恶意注册-引流-诈骗-洗钱”等各环节精细分工的完整链条。

在总结2020年网络诈骗新特征时，腾讯守护者计划安全团队专家海文对第一财经记者说，一是雇佣正常用户的账号参与诈骗环节。例如，通过“兼职众包”的方式，诱导用户拉黑产入正常的微信群，诱导用户传播引流信息，诱导用户提供收款码等。对于正常用户来讲可能只是做了一个兼职，但无形中成为黑产的“帮凶”。

特征二是多种黑产相互勾连。以杀鱼盘为例，其本质一种众包模式的诈骗，除了负责实施诈骗的“渔夫”外，还涉及到伪造虚假链接和APP的开发者、提供洗钱的虚假二维码制作者、承接二次诈骗的人员以及各平台的号商、推广人员、多个平台相关人员互相勾结，用户更加难以防范。

第三个特征是诈骗团伙升级新的黑灰产作案工具，包括不断跳变虚拟IP定位，增强侦察难度；用数字货币洗钱，也成为洗钱界新宠；引流兼职诈骗，也用起了AI电话外呼。例如，从技术上讲，诈骗团伙可以把作恶账号集体使用虚拟IP定位在昆明，甚至配上昆明的商户二维码消费记录，架空误导出一个在昆明作案的团伙图，就可实施诈骗。

难点在哪儿？

流量在哪儿，黑产就往哪里跑。当短视频平台占据越来越多的用户时长，网络黑产也早已盯上这些平台。例如，今年在短视频平台上，假靳东等冒充名人的事件备受社会关注。

这其实也是近年来网络诈骗的新特点：长链条、跨平台犯案。诈骗团伙分工协作，其中有些环节是在短视频平台或婚恋平台进行导流，有些环节则会在社交平台或网银、第三方支付平台实施诈骗，还有包括线上线下场景切换。不久前抖音安全中心总监周冉对第一财经表示，这类问题导致了网络诈骗取证难度大，以及追踪难度大。

而海文也提到，目前合作还没有既成的模式，一大挑战是各家能否建立黑数据互信的问题。

此外，网络诈骗的难点还包括智能化、链条化等问题。

海文告诉第一财经记者，从诈骗犯罪的上游黑产来看，机器学习、人工智能、大数据等热点技术已经被犯罪分子用于实施诈骗的各个环节中，比如黑产利用机器学习、人工智能技术突破互联网企业的验证码认证体系等等。尤其是发展到今年，犯罪分子的技术又进一步优化，上半年腾讯支持四川公安打击的若快打码平台，犯罪分子已经利用人工智能+部分人工的方式，来突破滑块验证码；利用秒拨平台随意跳转IP地址，更改终端硬件特征规避警方追踪等等。

而从诈骗犯罪的产业分工来看，在以往的网络诈骗案件中，犯罪分子往往团伙作案，彼此相识，分工协作，但近些年来犯罪分子的上下游分工越来越精细和专业，已经逐渐形成了从恶意注册开始，贯穿养号、引流、诈骗、洗钱环节的完整黑色产业链条。在这个黑色产业链条中，犯罪分子甚至彼此并不相识，利用互联网以提供服

务的方式分工配合，使得犯罪门槛越来越低。

为了更有效地阻断非法交易，财付通建立了决明风控系统平台，用于全方位防控与打击微信支付上异常资金流，基于黑产动态、诈骗双方用户行为分析，协助警方和相关政府监管部门对网络犯罪团伙进行打击。此外，微信支付也成立了反欺诈专项项目，在事前、事中、事后三个环节全链路打击诈骗。以事中交易为例，为了避免用户损失，微信有可能根据其系统评估，对高风险转账进行干预，主动让用户进入一定时间的冷静期。

在第一财经近期的采访中，多家平台呼吁：在行业层面，随着引流场景越来越多样化，平台责任不该局限于一个平台，运营商、互联网企业、金融机构等不只是要扫好各自门前雪， 如果能够与更多机构进行跨平台协同作战、联动打击，将更好地进一步解决网络诈骗问题。