本期主要分享一些思路。

钓鱼，网络钓鱼也好，现实钓鱼也好，都需要具备一些基本条件。

下面先举例子，再进行论述。

不知道各位有没有钓鱼的经历。

笔者在现实中也很喜欢钓鱼，是实实在在的钓鱼，不是那种钓鱼。

钓鱼有很多乐趣可言，尤其是上的那一瞬间，是非常具有成就感的。

因为鱼的种类不同，习性不同，因此钓不同的鱼，所使用的装备套件也是不一样的。

笔者在海上钓黄翅的时候，用的是生蚝。

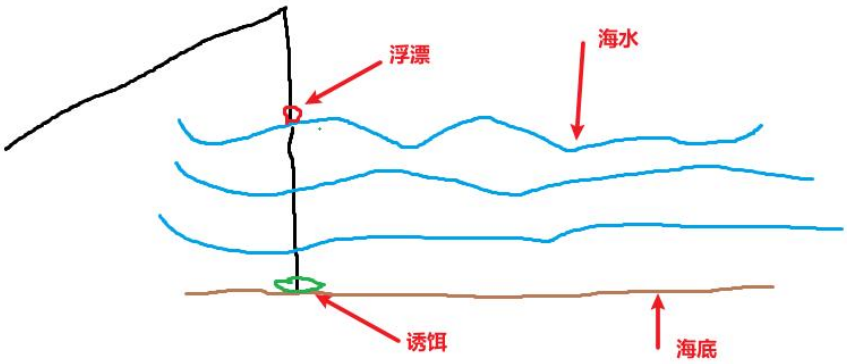
先开船到一个可能有鱼群的位置，然后把生蚝撬开，把鱼钩完全穿入生蚝的软体内藏好，不能露出钩尖，否则鱼不吃。

然后利用生蚝本身的重量让饵沉入海底。

这个钓法在福建，台湾海峡一代经常用，叫做沉底钓法。

杆子用的是手杆，不同于我们平常钓淡水鱼的杆子，是那种很复杂，很长的杆子，不存在，其实就是很简单的杆子，简化理解，就是根竹竿子，然后上面挂一个浮漂。

整个机制如下图所示：



在这个机制下，因为选的是浅海，水并不深，所以生蚝才能沉到底部，进而使得鱼线被完全绷直。

鱼咬住鱼钩，就会挣扎，进而拉动鱼线，进而拉动浮漂。

浮漂下沉，代表上钩，再根据经验选择拉杆时机，就能上鱼。

这是海钓的一种钓法。

钓其他鱼，又不一样。

比如钓鱿鱼，需要晚上钓，然后利用特制的灯打光（鱿鱼在夜晚会被光吸引），然后拉杆的手上下浮动，以模拟水中的活体，当鱿鱼慢慢的用触手包裹住诱饵（一个带倒钩的塑料鱼）的时候，需要慢慢的向上拉杆，让钩子死死的吃进鱿鱼的软体，最后快速拉杆，上鱼。

这些钓鱼手法，都是前人根据鱼的习性总结的钓鱼规律。

由于不同的鱼类喜好各异，因此要投其所好，它们才会上钩，否则就不会。

因此需要根据鱼的喜好来制定钓鱼策略，然后再根据制定的策略去研发针对性的工具（比如手杆），而不是先看看我们这边有什么牛逼的东西，看能不能去钓鱼，逻辑不能反，否则即便上鱼，效率也很低。

以上就是钓鱼玩法的基本逻辑。
那么迁移到网络中来，怎么去钓鱼呢？
本质就是利用人性。
这里分享几个文案的标题

这里先声明，笔者并没有用这些文案实战过，笔者只是听朋友说现在存在这样的文案。
可以看到，文案写的还是邪恶的，邪恶到一个文案发出来，马上就想去点击看一下。
为什么会这样呢？
原理就是人性的欲望。

人都是有欲望的，每个人都有喜好，也有自己埋在心里见不得人的东西，都很正常。
这些东西，稍加利用，就是钓人的饵。

人性，说起来复杂，其实很简单，无非就是自私而已。
什么是自私，就是希望别人坏，希望自己好。
这里先不讨论人性的主观好坏，这里就是客观的陈述事实。

因为人，首先是生物，其次才是人。
生物的本性，就是活着。
而生物为了活着，需要资源。
资源不是在原地等着就有的，而是需要通过残酷的竞争获得的。

自然界中，为了活下来，不是你死，就是我亡。
老虎捕食鹿，老虎成功，鹿死亡。
老虎不成功，老虎饿死。

人类莫名其妙获得了超越自然界其他生物的智力，于是和其他生物远远拉开了差距。
尤其在现代社会，大部分人不需要再为了食物你死我活，可以去做更高维度的竞争，但是优胜劣汰的丛林法则依旧不变。
想不参与竞争，也可以，但自然界优胜劣汰的法则会持续运转。
不积极竞争的人，慢慢的就会被归到社会底层去。
获得极低的物质供给。
几乎为零的精神供给。

这里讨论的，并不是人本性是好还是坏，那是主观层面的东西。

这里讨论的，是人本自私的客观存在性。

那么透过这个视角来理解上述文案，其实就能发现文案背后的吸引人的东西。

《x 总致我怀孕暴力威胁我打胎》

这个文案代表有两个人出事，一个 x 总，一个当事人女孩子，而且是一个公司的。

心理活动：

别人的坏事-->马上看笑话-->点击查看（对别人有害，可能对自己有利）

《涨薪计划&升迁名单》

心理活动：

快看看有没有我（和自身利弊强相干）-->妈的没老子，去死吧（对自己无利）

快看看有没有我（和自身利弊强相干）-->卧槽，还真有，马上给老婆打个电话今晚喝一杯（对自己有利）

《黑客入侵通告》

看看说了啥-->单纯猎奇（其实这个文案切入点一般，因为没有切中利弊要害，点击率没有其他文案高）

那么听我朋友介绍实战效果的时候，发现确实也是如此。

涨薪/裁员/公司老总出事之类的文案上钩率，要比黑客入侵，或者安全排查，或者疫苗等文案效果好，因为切中了人性趋利避害这条关键点。

和个人利弊强相关的，上钩率就高。

和个人利弊弱势相关，上钩率就低。

这样剖析下来，其实能够发现，钓鱼的本质也没什么神秘的，无非就是投其所好而已。

但知易行难，上面只是举了攻防演练中常用的一些文案，利用链条无非也就是

发送邮件-->鱼儿上钩-->钓鱼成功。

但在一些复杂环境下进行社工钓鱼，是非常考验技术的，需要大量的实战经验来做支撑。

eg：

x 单位邮箱不出网（所有协议），web 口暂无突破，项目需要打进内网。

目标：内网机器权限

成功方法：中间人攻击

信息搜集

- x 单位的运维部分是外包出去的，人员不稳定，更迭较为频繁。
- x 单位的 a 领导主管运维组，但是会委派 b 去执行具体工作，a 负责审批。
- b 在这周三周四请了两天假。
- 通过爆破获取了 c 的企业邮箱权限，但 c 不是运维组的人。
- 单位使用 horizon 云桌面办公，用户登录未绑定 mac

利用链：

- c 跟运维发邮件（利用运维不清楚人员身份，以为我是 b 的同事）：

x老师好：

根据集团最新通知，银监会将会在本月x月x日-x日对我司网络安全问题进行审查。

为应对银监会突发网络安全审查，目前需要马上对我司现有弱口令账户进行整改，根据组内初步排查，现已反馈一批弱口令，详见附件。

请立即发起账号密码修改申报流程，待我逐一核对人员新账密，和a老师同步流程之后，再反馈你进行修改操作。

该信件主送我一人即可，b本周三周四请假，暂时无需抄送。

然后获得一封发起密码修改的 re.流程信。

这里的关键点在于，第一次发出去的 excel 表中的数据是不包括我本人 c 的，并且附件中只有需要修改的账号。

然后邮件中的组内，指的是网络安全小组，是另一个组。

然后点击转发，我发送给运维的 req 和那条运维发过来的 re 会被当作信件往来粘在上面。

这里可以篡改附件来达到半真半假的效果，也是欺骗中惯用的手法。

删掉信件往来中我发送给运维的那部分（不删掉就露馅了），删掉 excel 表格附件中的其他人，只把我本人 c 写在里面，然后把这封流程信转发给 a，并附加以下内容：

a老师好:

运维日常巡检过程中发现我的账户属于弱口令，需要修改我的账号密码，特此报您审批。

a 确认改密，获得一封改密确认的 re.流程信件。

然后点击转发。

修改信件往来中确认部分的字样，然后换成原来的附件（除我之外的那一堆用户）。

然后删掉我发送给 a 的这部分（不删掉就露馅了），然后再把我最早发给运维的第一封信件加上（银监会审查改密码那一封）。

然后发送以下信件给运维：

x老师好:

需要修改的账号密码如附件所示，请按照表格中对应的数据进行修改。

另，为防止密码修改失败影响业务模块，请先将原账户账号密码数据按表格模板填写完毕后发我留档。

在进行具体修改操作之前，请再次与我确认，我需要与a老师同步，以确认修改时段不会影响业务。

望知悉。

最后得到一份有其他用户原密码的 xlsx 文件，且运维修改需要得到我的确认。

最后登录对应的 horizon，获取主机权限。

这套东西不是完全逻辑自洽的，因为我不知道哪些用户是弱口令，我只能猜测性的给一部分用户，但是也成功了，如果运维更加谨慎，就会发现有些账户并不是弱口令，这套方法就失效了。

更加优化的方法，直接编造让运维改密的话术也可以，改密码并不需要老密，这样运维发现的概率就更加小，我直接发一张 excel 表格让他按照表中密码改了就行。

不过这样虽然改密是方便了，但是恢复很难，因为不知道老密码，用户密码改了就会申诉，因为无法办公，然后很容易就被发现了。

总之各有优劣，具体环境具体分析，当时整套剧本推演下来，还是用了第一套方法，因为后续还需要打内网。

done