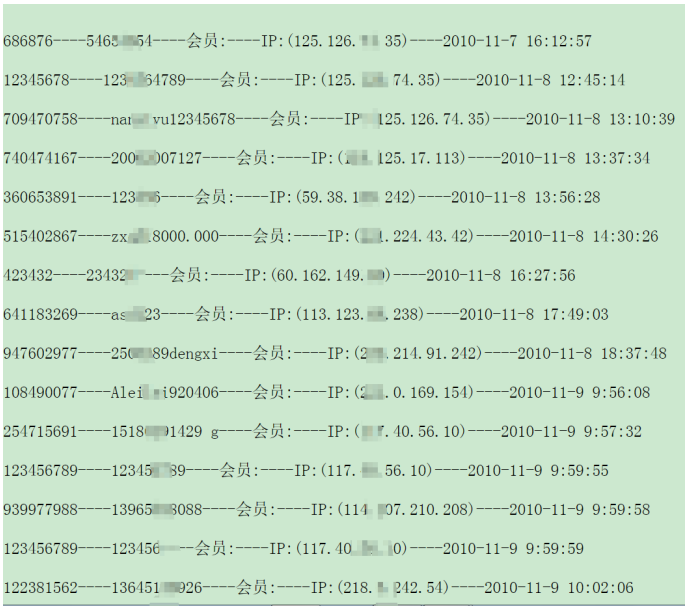
网上冲浪安全指南

by Henry

前言

之所以写这篇总结，一是在以前乡镇中学支教的过程中，发现学生们在 QQ 群里转发类似“转发领 100 QQ 币”的这种钓鱼链接（严格的说，是指向盗号链接的结构化消息），点进去一看，好家伙——根本不存在的抽奖活动，花花绿绿逼真的“获奖人信息”，点击领取需要输入 QQ 的账号密码。其实一输入之后，盗号者的后台是能够得到账号密码的，盗号的人再用这些被感染的号去大量转发盗号链接，一传十，十传百，大规模的盗号事件由此发生。



第二，最近对信息安全特别感兴趣，也正好在了解渗透方面的内容，写点东西，也算自己有个学习上的专题小结。

总之，本文档的写作目的，是为了让更多的人能明白盗号是怎么一回事，如何识别木马链接，中间为了授渔，也会从其它的角度提出鉴别方法。

想把这篇文档写得滴水不漏，可惜我的思维它信马由缰，因此谬误在所难免，欢迎各位向我的邮箱 root@zuoxueba.org 提交反馈，感谢！

网上冲浪安全指南

目录

常见骗术总结

兼职刷单诈骗

兼职刷单诈骗案件量占整体通讯网络案件量的27.77%，是2017第一大案件类型。

兼职、刷单类型的诈骗

请看新闻便是：

- 上海一大学生“兼职刷单”被骗 8.7 万元：收到第一笔 4000 元报酬后深信不疑

摘要：这类诈骗主要针对在校大学生和家庭主妇，以简单操作、高薪回报为诱饵，布下先给“甜头”后坑钱的骗局。

- 大学生兼职“刷单”被骗 8.7 万元 警方:存在三种“套路”（来源：东方网）

通过作案要素的分析，警方公布了三类手法：

第一、被害人手机收到有关“兼职广告”的短信和链接，主动添加犯罪嫌疑人在短信或网络中预留的社交软件，填写个人简历和各

种申请表，并拍下犯罪嫌疑人在电商平台指定的商品付款刷单，很快就会收到少量的刷单返现，在赢取被害人的信任以后，要求被害人在不同的电商平台内拍下指定商品刷单，然后以“系统故障”、“刷单延时”等理由要求被害人反复多次刷单，后被害人申请退款没有回应方知被骗。

第二、 被害人在网络中搜索“兼职”等关键字，在社交软件、网络论坛上寻找主动添加了犯罪嫌疑人在网络中预留的社交软件后并向其咨询刷单的规则，购买虚拟或实物商品，扫描犯罪嫌疑人发送的二维码直接付款或者直接多次转账到犯罪嫌疑人的账户中。

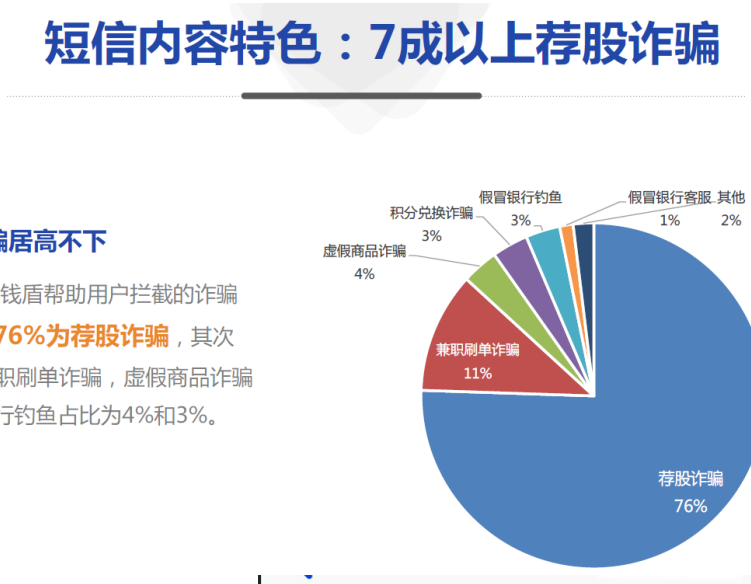
第三、 被害人收到“网店购买记录良好”“刷好评返现”的短信，短信内容以高额的回报来诱惑被害人，被害人添加了犯罪嫌疑人的社交软件后，犯罪嫌疑人要求被害人登陆正规的电商平台，要求被害人选中商品至“购物车”但不要付费，诱骗被害人通过第三方软件扫码或点击链接支付，并用“需要完成不同任务才能退还本金”为由诱骗其不停支付。

总结

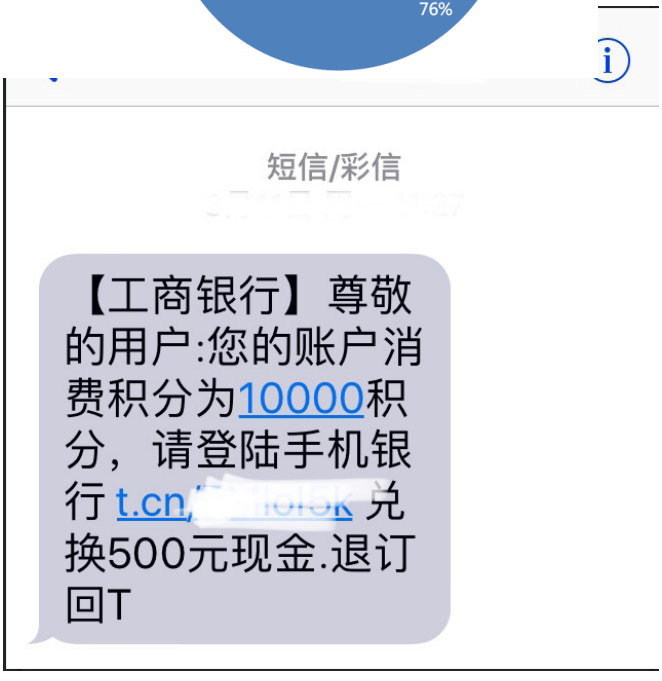
1. 刷单是违法的。详见反不正当竞争法大修 网店“刷单”或重罚200 万；

2. 青年朋友们可以在网上做哪些兼职，可部分参考知乎-有哪些兼职赚钱的方法？中的高赞答案；不过还是那句话，兼职是一件**有成本也有风险**的事情，选择时要理性。

短信诈骗



原理



右边图里的这个链接 t.cn/xxx，是个假的工商银行的链接，你所输入的所有个人信息，都不会用于登录真实的工行，而是被会不法分子获取到。

其实，形如 t.cn/xxx 的链接，是新浪微博提供的短链接服务生成的，具体后面是什么网站，只有访问进去看浏览器的链接才清楚，有一定的隐蔽性，所以经常被不法分子用来做钓鱼网站的前置 url，是盗号链接的重灾区.

此外，关于发信息的号码是 106919 开头，难道不比私人的号码发来的短信更“可信”？——很可惜，并不会更可信，这是；还有，你别看短信最前面是【工商银行】就信了，这种 106919 打头的短信号码，是工信部（政府机构）给各大民营短信平台的号段中的，原则上是只对公司等机构开放，但你应当知道，只要肯花钱，不法分子在某些短信平台上，也完全可以发送类似【xx 银行】的信息。

对策

下面主要从两个维度来分析这种诈骗手法，让大家学会避免上当受骗：

① **陈述是否属实。***不属实，本人压根没工行的卡，何来的 10000 积分？而且就算在用工行的卡，为什么我的积分正好是 10000（壹万整呢）——蹊跷，很是蹊跷！*

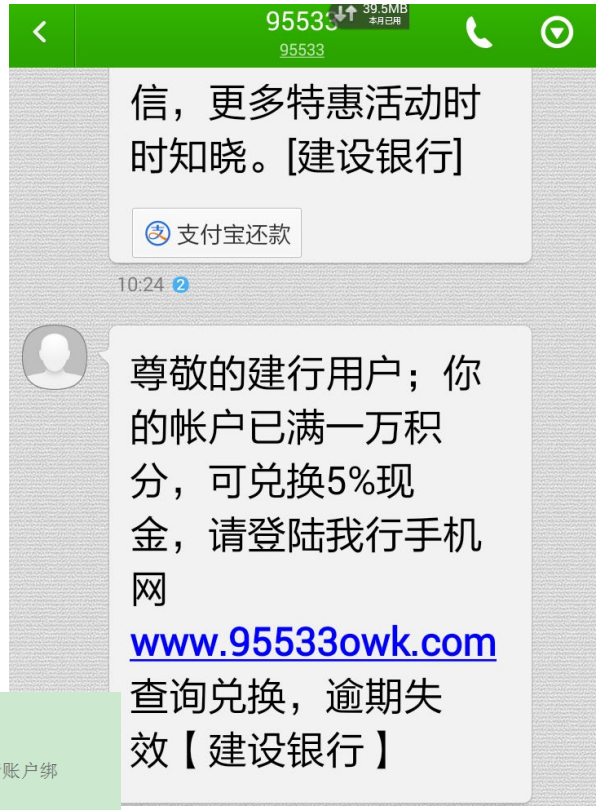
② **安全常识；**

a) 几乎**所有的银行都不会在给客户群发的短信里发链接；**

b) 没有【xx 银行】这类字样的短信，**一定不是**银行官方发的，但有这类字样的短信也**不一定是**官方发的，伪基站也可以发成这样；

c) 使用形似 T.cn/xxx 的短链接，几乎可以肯定是盗号链接了；

举一反三



假如有一天，建行的官方号码 95533 给你发了一条短信，说你可以登录某某网址领钱，你应不应该相信?

绝对不应该。刚刚我们谈到，银行几乎不会在短信中放链接（因为太容易被仿冒了），并且它给的网址一看就有问题(owk 是什么鬼…)，让我们来看看官方网站的网址是怎样的。

而且，还要告诉你，这是伪基站给你发送的短信。伪基站是什么？就是不法分子（违法地）买了一些设备，搭建了假的基站，因为绝大部分手机都没有甄别功能（伪基站一般比真的基站离你更近，信号更好，手机会自动连接的），这时候，不管是给你发短信还是打电话，不法分子想用什么号码就用什么号码。关于短信诈骗的介绍，基本就说到这里了，各位可以去网上搜索“伪基站”、“短信诈骗”、“精准诈骗”来更加全面地了解一下这方面的常见骗术，进而更好地保护自己和家人。

我觉得你不太可能会去看呢。下面就介绍一下电信诈骗，尤其是近年来日益猖獗的精准诈骗。

电信诈骗

且看案例：8·19 徐玉玉电信诈骗案，这属于公安部近年严厉打击的精准诈骗的一例，源头在于个人信息泄露。

这个防范起来倒也不难，相信能看到这篇文档的各位都是有能力鉴别的。从什么*“妈妈我 xx 被抓了，那边要见钱才放人，给我打钱”*，到*“爸爸，我手机掉了，用的朋友电话，现在”*，从住院、到被抓、再到出国留学紧急用钱，也是无所不用其极。希望青年朋友们，离家之前都跟父母们说好，遇到这类情况时自己会怎么办，避免让骗子有机可乘。

QQ 盗号

游戏代充

低价代充究竟有没有，朋友们可以先到心理学及常识补充一节理解成本的概念，再理性做出判断。

100 元充 5,000 点券，这种能是真的吗？还有，游戏代充很多时候店家是会让你提供账号密码的，很多人的密码是通用的！你能确定店家上号之后不会到处看看？充值完后的你留给店家的账号密码，店家以后会怎么处理？你确定自己的个人隐私能得到保障吗？

所以，我建议不要选择代充，如果实在要用代充，也建议改成简单的密码（例如 QWE123456）再发给店家，充完必须立刻更改密码，否则 gg!

“免费领会员”

明确一个原则：天上不会掉馅饼；结合我在常识补充中的成本来理解，其实**绝大多数**都是盗号的网站。

另外，为了让大家理解，附上一张经典的钓鱼网站后台的照片，非常恐怖！

请各位务必提高警惕，严防盗号。建议可以打开 QQ 登录的设备锁，这样就算别人拿到密码也无可奈何，登不上去的。

常识补充

成本

首先，我想以移动话费充值卡为例，介绍一下***成本***的概念。

移动充值卡，在前几年移动建议支付还未发展起来的时候，曾是大多数玩家充值 Q 币、游戏点券的主要充值渠道，当然这几年移动支付发展如日中天，话费充值卡逐渐没落了。

使用话费充值卡给支付宝充值余额的时候，会出现一件有意思的事，且看下面这张截图。

“您已成功充值 30.00 元面值，充值金额 28.50，服务费 1.50 元”，我们在营业厅买 30 块的充值卡就得花 30 元啊，为什么在这里充值还要收服务费呢?

好，为了解释这个服务费，结合上面的截图，我问个问题：

- 30 元面值的充值卡，营业厅卖给咱们 30 元，营业厅赚不赚得到钱?

我的观点是，营业厅是要赚钱的（基于做生意的原则嘛）。那么，既然营业厅赚得到钱，充值卡的进货成本必定低于 30 元，所以， 30 元充

值卡实际的价值是比 30 元略低的；再结合上面 5%的手续费分析，设充值卡的成本是x, 那么可以基本得出 $28.5 \leq x < 30$，也就是说，充值卡的发行方为了防止“永动机”的发生（比如 30 元的充值卡，营业厅 29 元就能进到，充到支付宝里得 30 元，那相当于你充个值，直接用 29 元得到了 30 元，净赚 1 元——马云爸爸能让这样薅羊毛的事情发生吗？不能，所以，不到 30 块进的充值卡，充到支付宝里也不能给你 30 块。

- **但还有一个问题，那用充值卡去充话费，为什么是 30 元面额的就能到账 30 话费呢？**

我的解释是，因为手机话费和支付宝余额的*价值*不同。支付宝余额里有 30 元，你就能购买到 30 元的东西，交水电费、交学费、交话费都可以，它的通用性是很强的；换句话说，支付宝余额的购买力比手机话费强；其实这个购买力的理论也适用于学校食堂的饭卡、公交卡等，相信你一定理解了我这个成本-价值的理论了。

万变不离其宗，骗子就是让你以为你捡了便宜（低成本换高收益），其实骗子骗你才是低成本换高收益。

如何防止个人信息泄露

为了更好地理解这部分内容，科普几个概念和几个注意事项（为了醒目，我用的措辞都是禁止）：

照片也能泄露你的隐私？——EXIF 信息

Exif 的全称是（Exchangeable image file format），它是可交换图像文件格式。是专门为数码相机的照片设定的，可以记录数码照片的属性信息和拍摄数据。

通俗来说，Exif 可以在图片上附加一些额外的信息，例如拍摄地点，拍摄方向，拍摄的设备信息，拍摄图片的时间等等。这些信息并没有什么坏处，例如最常用拍摄照片的方向信息，所有的图片软件都依赖它的值来确定图片在你设备上显示的方向，这就是你无论手机是倒着拍摄还是横着拍摄，最终呈现在手机上都是正的的原因。

Exif 信息里有一些例如 GPS 定位数据、拍摄时间等等信息，基本上任何智能手机或者相机，在拍摄照片的时候，都会自动写入到图片中。

微信中“发送原图”功能，会暴露你拍照片的位置。

如果比较注重个人信息的话，可以在手机的设置中，关闭定位服务等隐私相关功能。

参考：泄露你位置隐私的远不止“微信发原图”.

禁止不打码在朋友圈晒火车票

有了火车票照片，坏人就得到了除出生月日以外的部分，穷举空间只有 366 种可能，加之网上有开源的身份证有效性判断的算法，只剩下区区几十种可能性；


```
root@LEESEC_PC:/tmp# node 12306valid.js
420117198801081638
420117198801161638
420117198801241638
420117198802041638
420117198802121638
420117198802201638
420117198803191638
420117198803271638
420117198804071638
420117198804151638
420117198804231638
420117198804311638
420117198805031638
420117198805111638
420117198806181638
420117198806261638
```

最后，再使用大杀器——12306 网站核验，将这几十种可能性一一输入系统中，最后核验通过的，就是准确的身份证号码了！

怎么样，现在你明白了随意分享火车票的危害了吧。参考自：破解火车票上的身份证号码

禁止晒自己的身份证

“苍蝇不叮无缝蛋”，身份证、驾驶证、网银截图、手持身份证的照片等，都是一个道理，这个就不多说了，稍不注意将后患无穷。

安全上网的正确姿势

通过 VPN 上网

VPN 是一款全局代理的功能，可以让你的数据全部经由 VPN 服务器，在公司里用得多，建议大家下载阿里开发的“钱盾”App[1]，里面提供了上网安全保护的 VPN 连接，从技术角度上来说，可以防止网络的嗅探[2]和中间人攻击[3]。我自己一般连接陌生 WiFi 的时候会打开这个功能再上网；当然，最好是不要使用陌生 WiFi 进行敏感操作，如网购、转账等。

[1] 阿里钱盾 App 下载地址，https://qd.alibaba.com/
[2] 嗅探 （窃听网络上流经的数据包），https://baike.baidu.com/item/%E5%97%85%E6%8E%A2/5114370
[3] 中间人攻击，https://baike.baidu.com/item/%E4%B8%AD%E9%97%B4%E4%BA%BA%E6%94%BB%E5%87%BB

附录

腾讯 网站安全检测诊断工具	https://guanjia.qq.com/online_server/webindex.html
阿里钱盾 app	https://qd.alibaba.com/v/wannacry.htm?spm=a3702.7769011.7932614.3.670d363aWckNe1
国家互联网应急中心	http://www.cert.org.cn
«2018 年 我国互联网络安全态势综述» *较为专业、详实*	http://www.cert.org.cn/publish/main/upload/File/2018situation.pdf

许可声明