

网络安全意识 | 网络钓鱼

钓鱼，指**运用欺诈心理结合电脑科技的新犯罪手法**，也可以粗略地理解为一种使用特殊手段引诱你上钩以获取好处的骗局。

在现代生活中，人与人之间交流接触的渠道越来越多，接触面越来越广，交流频率也越来越高。相应地，钓鱼也得益于此，在日渐频繁的交际中变得愈加强大。

一、常见的钓鱼手段

比较常见的钓鱼手段不外乎是邮件钓鱼，短信钓鱼，电话钓鱼，U盘钓鱼这几种。而如果就网络安全意识来讲，钓鱼的目的，说到底就是要拿到你的各种账户密码或是你的钱。甚至可以说，无论是从什么渠道下手，最后都要回归于此。那么凡是有网页，电话，邮件，短信涉及于此，还烦请提高警惕！

邮件，短信，电话，U盘等等只是一个初级接触的媒介，在这之后，钓鱼者一般会**引诱用户访问某个恶意网站并输入敏感信息，引诱用户下载安装某种恶意软件，引诱用户下载打开恶意文档**等等。

二、钓鱼的人用什么做鱼饵？

前文提到，钓鱼是指一种**运用欺诈心理结合电脑科技的新犯罪手法**，那么，钓鱼者究竟是运用了怎样的欺诈心理，来引诱受害者上钩上当呢？

1.贪婪。人的贪心历来好用，骗子也常常在它身上大做文章。在专注于此的钓鱼局中，最经典也最直白的一种就是“尼日利亚419骗局”，“我是秦始皇，给我2000我复活兵马俑封你做丞相”就属于此种骗局。随着大家安全意识的逐渐增强，这样简单直白的骗局出现频率已经越来越少，但无论将来还会出现怎样精巧的骗局，其根本永远是在利用人的贪心。请记住一句话，**天上不会掉馅饼，不会有那么多平白无故的便宜可以占。**

2.信息差。现代钓鱼手段繁多，有很多奇技淫巧是大家难以想到的。短信，电话，邮件，甚至word文档，什么钓鱼手段都有可能，只有想不到，没有做不到。

3.轻信。不要轻信别人，不要轻信别人给你的东西，经常质疑经常怀疑，你就是相对安全的。

4.利用紧张焦虑情绪。比如发邮件说你的账户将要被封号，你的银行卡将要被冻结一类。紧张慌乱之下，大家可能会丢掉一部分判断能力。

5.利用权威。人是社会性动物，会对各种形式的权威有反应。比如“某某某大师都选择了这款产品”一类。

6.好奇。人类对未知永远都有好奇心，但有的时候好奇会害死猫的。

7.觉得自己永远不会被骗的人，往往就是钓鱼者的下一个目标。

三、一些钓鱼的例子

1.图中即是一封通过群邮件功能发送的钓鱼邮件。



该邮件标题和内容如此起名，目的就在勾起收件人的好奇心，然后引诱受害者点击已经准备好的链接中。图上这种奇奇怪怪的链接名为“短链接”，可以和正常的链接相互转换。钓鱼链接转换为短链接后会隐藏原本网址的特征，使受害者不警觉。下图为点击上图钓鱼链接后页面。




观察图中左上角网址即可发现，该网页并非真正的QQ邮箱登录网址。但有一点值得注意，在QQ中直接点开时，是看不见网址的，只能看见网页标题“登录”。也就是说，在类似这种环境下，它会更难察觉。如下：

×

登录

+



QQ号码/手机/邮箱

请输入您的QQ密码

登 录

忘记密码?

注册新帐号

不要以为这非常容易察觉，实际上，在日常生活中，不是每个人都有十分的精力去防范钓鱼欺骗的。仅以该邮件为例，笔者身边就已经有至少5人中招而不自知，仅仅是笔者邮箱中就收到了两封其他好友中招后转发而来的。（下图另一封邮件中包含的链接也是典型的短链接）

邀请函 ... - 元旦晚会邀请函。 以加密，点击查看：<http://mrw.so/...> 昨天 19:38

邀请函通知： - 元旦晚会邀请函 以加密，点击查看：<http://t.cn/Ai...> 昨天 14:15

2. 零时安全团队在为某交易所做授权测试时，也向该交易所的客服发送了含有钓鱼链接的邮件。

上一个例子中的链接和QQ毫无关联，有心者可以发觉。但以下笔者发送的链接中，实际上使用了该交易所自身使用的网站组件漏洞，以构成链接。故该链接属于交易所自身域名下，客服人员并没有发觉，最后点击了该链接。随后我方获取了客服人员的登录凭证，登进管理后台。

i have some issues. 收件箱



零时

10月 日

收件人:



Hello there! I am logged in on the platform but the website is always wrong, this can be accessed, I don't know if it is our website, I hope to give a statement.

[/lib/charting_library/charting_library/static/tv-chart.82ee311dc10bb182c736.html#disabledFeatures=\[\]&enabledFeatures=\[\]&indicatorsFile](#)



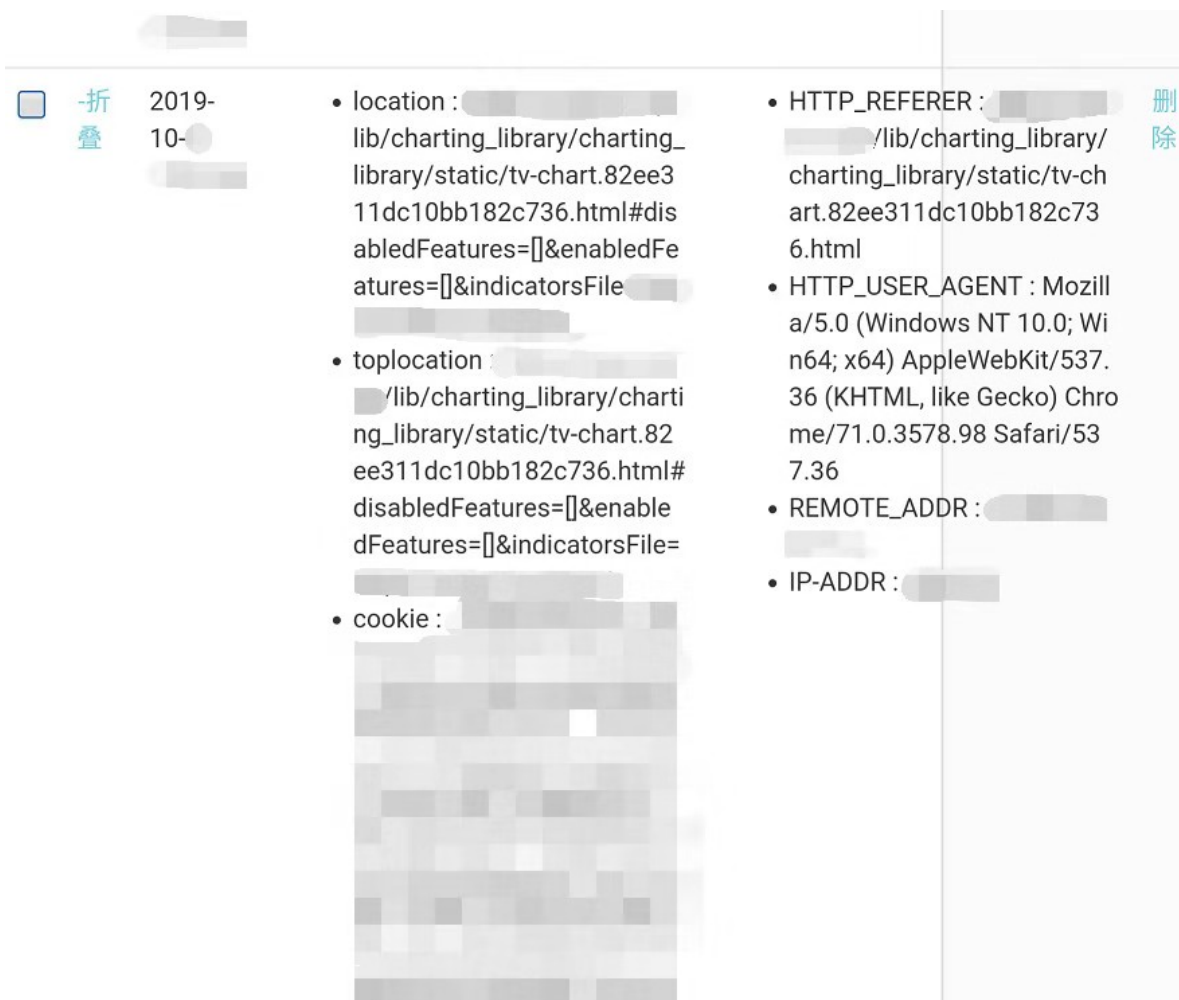
客服

10月 日

收件人: 我

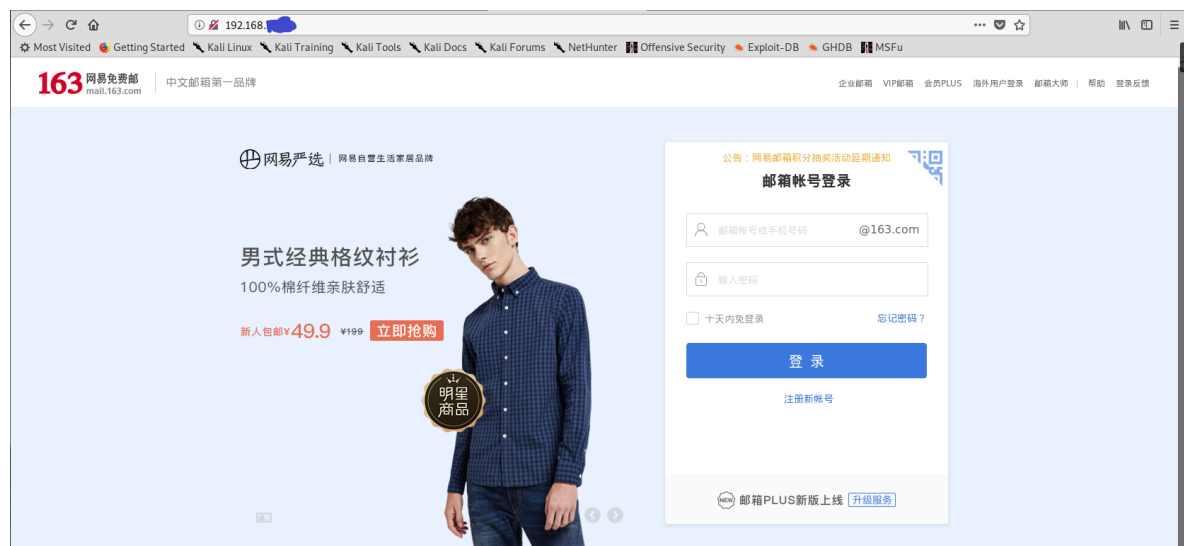


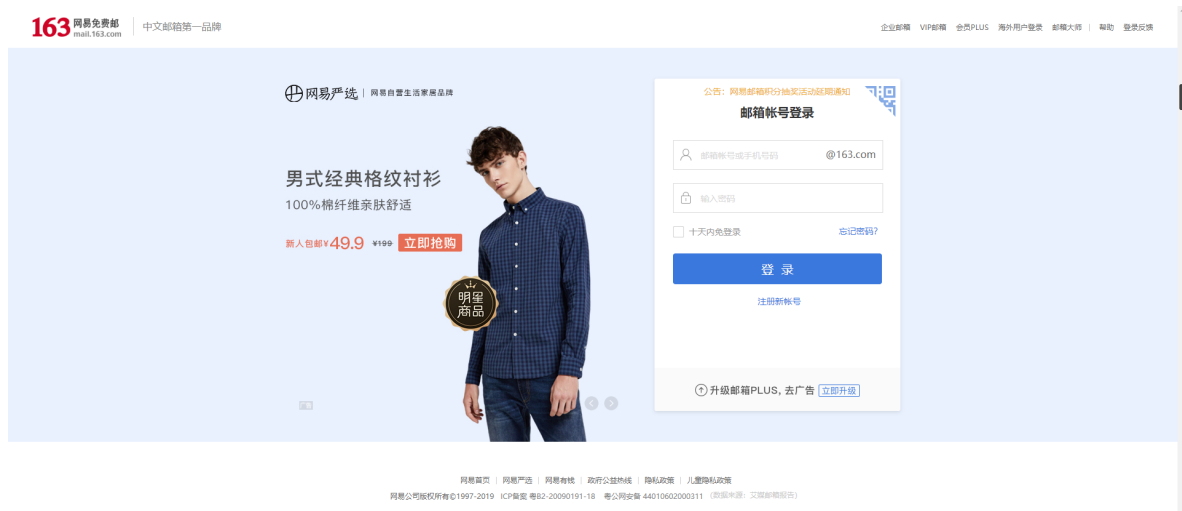
our webside is h



3.真假网站之间的差异不是那么好分辨的，甚至可能就是一模一样。网页克隆工具会克隆出和主体完全一样的网页，让你难以分辨，当你输入了账户密码选择登录后，它也只是跳转到真正的网页上。对于常规用户来说，可能只是奇怪为什么又要输入一遍密码然后顺便骂骂网站。当你忙起来的时候，可能真的不会想太多。

图1为克隆网站，图2为真实网站。





4.钓鱼网站可能会使用不正规的词汇或奇怪的字符。



四、关于鉴别和防范钓鱼的小建议

- 1.一般来说,官方发出的邮件,信息不会有语法,称呼上的问题,但钓鱼邮件可能会在这方面出差错;
- 2.当有邮件或短信等诱导你点击链接时,请仔细观察链接,ip和ip+端口,这种形式的链接不要点击(45.127.78.93和58.24.84.116:8080类似的,XX.XX.XX.XX是ip,后面的冒号和数字是端口号);
- 3.当有邮件或短信等诱导你点击链接时,请仔细观察,是否是看不明白其归属或功能的短链接,如:

http://diaoyu.com/diaoyu1



生成的短网址: <http://cn.hk.uy/g3>

请按Ctrl+C复制

请输入长网址:

http://diaoyu.com/diaoyu1



生成的短网址: <http://j.mp/2Q9nswb>

请按Ctrl+C复制

4.当有邮件或短信等诱导你点击链接时，请仔细观察域名（网址），是否有下图例子中的类似情况，如果不放心，可以输入自己牢记的网址或从官方渠道进入；

rn = m (r+n连写，与m混淆)

l = l = 1 (左面是大写的l，中间是小写的L，右面是数字1，三者易相互混淆)

0 = O = o (左面是数字0，中间是大写字母O，右面是小写字母o，易相互混淆)

www.taobao.com (相似域名，多一个或少一个字母之类)

等等

5.一般来说，正规机构在需要用户付出代价之前，都会有提醒预告，但钓鱼邮件会直接使用紧迫的语气（你的账户24小时就会被封禁）；

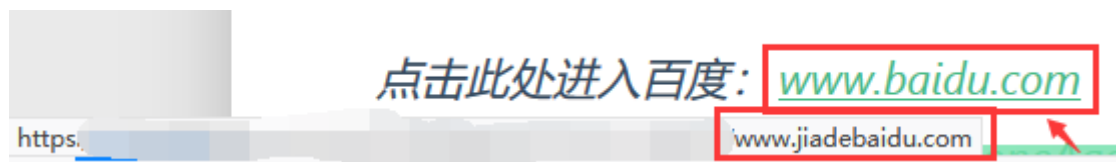
6.一般来说，单单一封邮件无法对你实施攻击，一定要以邮件为基础，在此之上产生别的交互才可以，比如说**点击链接后输入内容，运行/打开文件**，当需要以上动作时，请警惕小心；

7.一些使用工具复制出的网站，点击登录后会跳转到真正的网站上，在用户看来，就是**输入密码，登录后又让登录了一次**。如果出现类似这样的异常情况，请**立刻更改密码**；

8.当你怀疑一个网站，想要鉴别时，**尝试输入错误的账号密码**，看看网页的反应；

9.当你收到一个可疑的邮件时，可以**询问客服**或是多渠道询问发件人，客服会帮你鉴别它是否属于常规业务，发件人会告诉你那是不是他发的邮件；

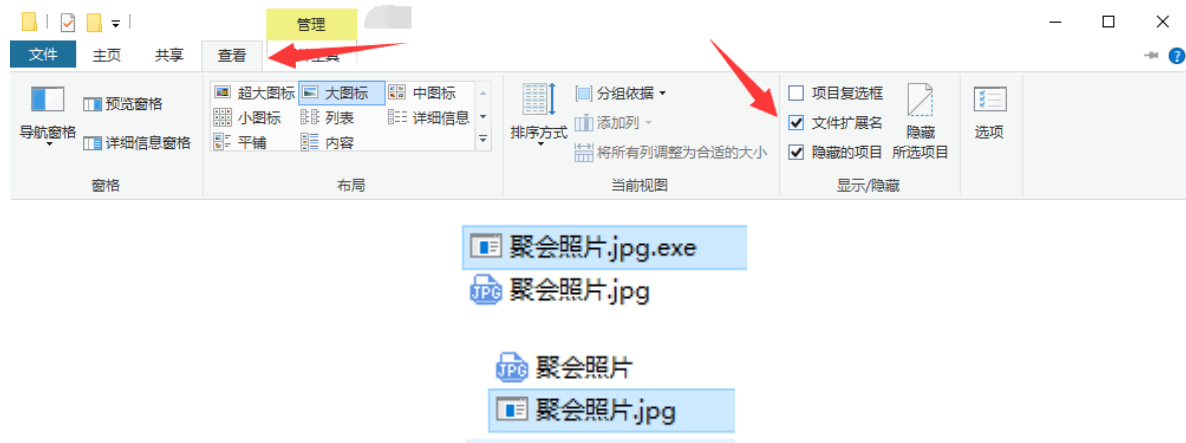
10.当你的邮件中包含一个链接时，可以将**鼠标悬停在该链接上，查看它真正的指向**，是否与表面上相同，当你点击进“百度”时，是否真的跳转到了百度（鼠标悬停在红箭头所指的链接上）；



11.在别人的公司地盘里扔一个含有u盘病毒的u盘也是常见的钓鱼手段，如果捡到了不明来源的u盘，**不要好奇地插到自己的电脑上**；

12.不要随意安装未知来源的软件，在正常功能之外添加恶意远程控制代码且不被发现，是很容易做到的；

13.打开电脑上的文件后缀显示（win10用户可在打开任意文件夹后按下图操作），这样你就会发现，有一种恶意程序，它的名字叫“聚会照片.jpg.exe”；



14.禁用word中的宏，word文档远不如看起来无害。宏病毒可能在你打开那个文档时就已经暗暗发作了。

