钓鱼邮件防范详细指南

随着互联网的快速发展，新的网络攻击形式“网络钓鱼”呈现逐年上升的趋势，利用网络钓鱼进行欺骗的行为越来越猖獗，对互联网的安全威胁越来越大。网络钓鱼最常见的欺骗方式就是设计钓鱼网站，引诱网络用户进入以假乱真的网站而导致自身的用户名、密码等重要数据的泄露，进而遭受重大损失。钓鱼网站的欺骗性很强，用户不细心、不谨慎就很容易上当受骗，而引诱用户进入钓鱼网站的主要手段就是采用钓鱼邮件进行诱导。那么，什么是钓鱼邮件?如何识别钓鱼邮件?中招了怎么办?

一、“钓鱼邮件”的基本概念

钓鱼邮件是指黑客伪装成同事、合作伙伴、朋友、家人等用户信任的人，通过发送电子邮件的方式，诱使用户回复邮件，点击嵌入邮件正文的恶意链接或者打开邮件附件以植入木马或间谍程序，进而窃取用户敏感数据、个人银行账户、邮箱账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动。

二、钓鱼邮件的危害

钓鱼邮件通过隐含的恶意链接，窃取用户重要个人信息，可能造成直接或间接经济损失，甚至政治危害。

1.直接经济危害

钓鱼邮件的主要目的是要劫财。钓鱼邮件往往暗藏着两重侵害方式：一是用户没有发现邮件中链接的假网银、假网站，输入了个人账户和密码等信息，

导致信息泄露造成经济损失；二是用户即便识破了假网银、假网站，没有输入自己的网银账号和密码，虽然本次的直接损失可以避免，但还是可能被攻击者的后招所伤，因为通常这些假网站中都暗藏了事先植入的木马程序或间谍程序。若用户的电脑防御能力较弱，只要点开了虚假网站的界面，电脑就会被植入木马或间谍程序。以后，用户只要在该机上使用此网银就会被这些恶意程序监控到，并以数据包的形式传到不法分子预先设定的邮箱里，从而给网络用户造成重大经济损失。

2.间接经济危害

钓鱼邮件除了可能导致上述直接经济危害外，还可能导致用户邮箱被黑客侵入从而造成很多其他间接经济危害

（1）损坏邮箱中联系人的资料。入侵者会收集所有邮件中的用户资料，更严重的是修改邮箱的密码，用户将永远失去这个邮箱的使用权。若是商业用户邮箱被盗窃，则可能造成更大经济损失。

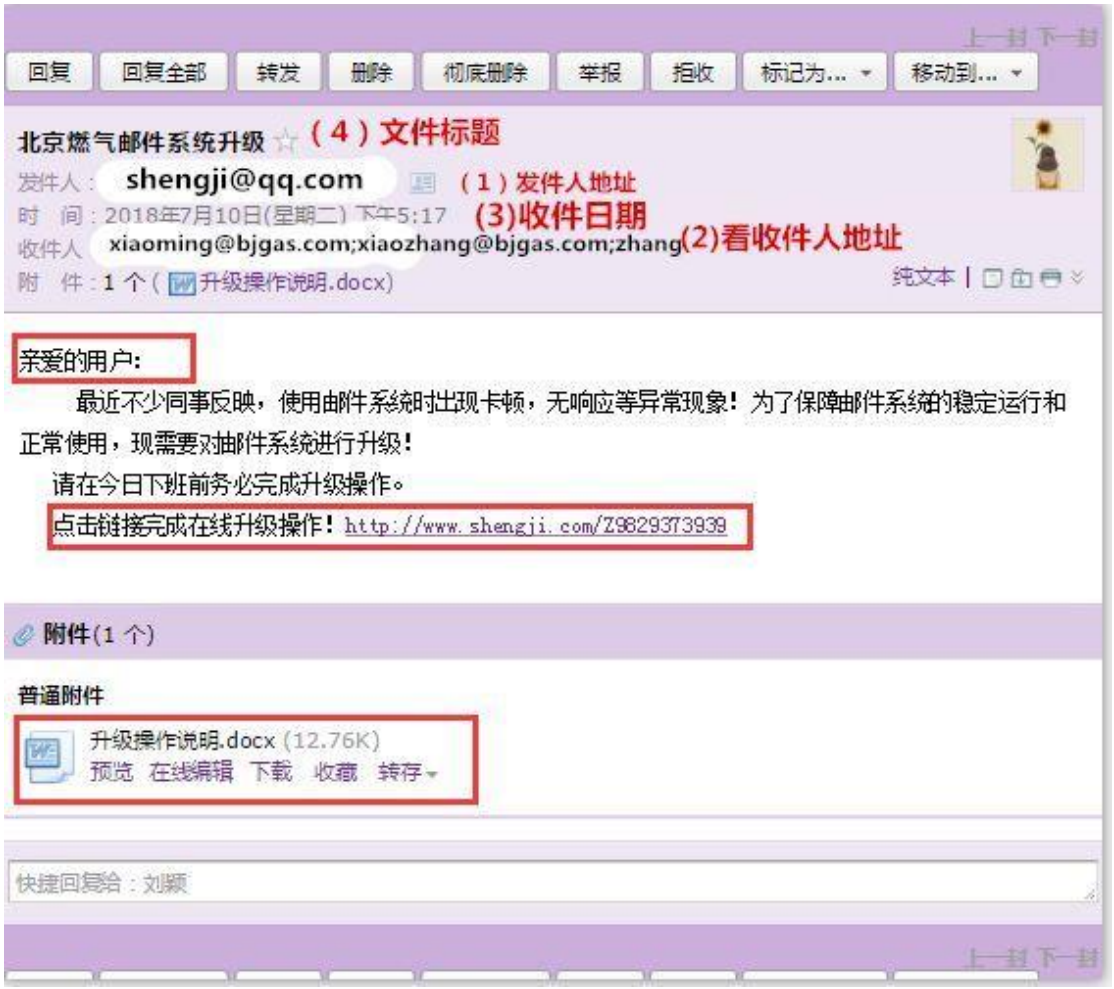
（2）入侵者掌握用户邮箱后，可以根据需要申请一个与用户类似的名字和一个类似的邮件地址。如果恰好遇到有用户要打款，入侵者就可以把自己的帐户发给用户的客户，或者在成功拦截发往该邮箱的邮件后，把用户帐户替换为入侵者的账户，这样客户的相应款项就会打入到入侵者的帐户。

（3）入侵者还可利用买家贪图便宜的人性弱点，通过被盗用户的名义与用户的客户进行联系来诈骗。例如，入侵者可以把相关产品价格报得适当的低，引诱买家支付一定的预付款，通过这种方式可以在短时间内给很多客户造成重大损失，也给邮箱用户带来更重大的信誉损失。

3.政治危害

钓鱼邮件的诈骗方法不会仅拘泥于一种，除了会造成上述经济损失外，也可能造成严重政治危机。 一个典型的案例就是美国的“邮件门”事件。2016 年 7 月 22 日，就在美国司法部宣布不指控希拉里的两周之后，阿桑奇领导下的“维基解密”公布了希拉里方民主党委员会内部约 2 万封的绝密邮件，所有邮件中主要讨论的是如何把希拉里推上总统宝座。这些邮件的公布，让美国民众意识到民主党内部的协作阴谋，从而引起公众更大的质疑：被希拉里团队删掉的另外 3 万封，不能给外人看的邮件可能含有更多可怕的内幕。在此关键时刻，希拉里竞选团队中最重要的成员，竞选经理 John Podesta 点开了一封黑客发给他的钓鱼邮件，从而泄露了他个人邮箱密码，导致其邮箱被黑客翻遍，黑客把获得的邮件交给了“维基解密”。从 2016 年 10 月开始，“维基解密”逐渐公布 Podesta 的这些邮件，由此导致美国大选的风云突变，最终特朗普以微弱优势获得选举胜利。可以说钓鱼邮件在改变 2016 年美国大选结果中起到了至关重要的作用。

四、如何识别钓鱼邮件



1.看发件人地址。如果是公务邮件，发件人多数会使用工作邮箱，如果发现对方使用的是个人邮箱帐号或者邮箱账号拼写很奇怪，那么就需要提高警惕。钓鱼邮件的发件人地址经常会进行伪造，比如伪装成本单位域名的邮箱账号或者系统管理员账号。

2.看收件人地址。如果发现所接收的邮件被群发给公司内大量人员，而这些人员并不是工作常用联系人或同一工作组织内人员，那么就需要警惕，有可能是钓鱼邮件。

3.看发件的日期。公务邮件通常接收邮件的时间在工作时间内，如果收到邮件是非工作时间，需要提高警惕。比如，凌晨 3 点钟。

4.看邮件标题。大量钓鱼邮件主题关键字涉及“系统管理员”、“通知”、“订单”、“采购单”、“发票”、“会议日程”、“参会名单”、“历届会议回顾”等，收到此类关键词的邮件，需提高警惕。

5.看正文措辞。对使用“亲爱的用户”、“亲爱的同事”等一些泛化问候的邮件应保持警惕。同时也要对任何制造紧急气氛的邮件提高警惕，如要求“请务必今日下班前完成”，这是让人慌忙中犯错的手段之一。

6.看正文目的。当心对方索要登录密码，一般正规的发件人所发送的邮件是不会索要收件人的邮箱登录账号和密码的，所以在收到邮件后要留意此类要求避免上当。

7.看正文内容。当心邮件内容中需要点击的链接地址，若包含“&redirect”字段，很可能就是钓鱼链接；当心垃圾邮件的“退订”功能，有些垃圾邮件正文中的“退订”按钮可能是虚假的，点击之后可能会收到更多的垃圾邮件，或者被植入恶意代码，可以直接将发件人拉进黑名单，拒收后续邮件。

8.看附件内容。当心邮件中的附件信息，不要随便点击下载。诸如 word、pdf、excel、PPT、rar 等文件都可能植入木马或间谍程序，尤其是附件中直接带有后缀为.exe、.bat 的可执行文件，千万不要点击。

五、钓鱼邮件防范五要、五不要

1.“五要”

（1）杀毒软件要安装。安装杀毒软件并定期更新病毒库，开启杀毒软件对邮件附件的扫描功能。同时定期下载安装系统和软件的更新；

（2）登录口令要保密。要做到不向任何人主动或轻易地泄露邮箱的密码信息。不要将登录口令贴在办公桌或者易于被发现的记事本上。办公邮箱的密码要定期更换。

（3）邮箱账号要绑定手机。将邮箱帐号与个人手机号码绑定，不光可以找回密码，也可以接收“异地登录提醒”信息。

（4）公私邮箱要分离。不用工作邮箱注册公共网站的服务，也不要用工作邮箱发送私人邮件。

（5）重要文件要做好防护。及时清空收件箱、发件箱和垃圾箱内不再使用的重要邮件；备份重要文件，防止被攻击后文件丢失；重要邮件或附件应加密发送，且正文中不能附带解密密码。

2.“五不要”

（1）不要轻信发件人地址中显示的“显示名”。因为显示名实际上是可以随便设置的，要注意阅读发件邮箱全称。

（2）不要轻易点开陌生邮件中的链接。正文中如果有链接地址，切忌直接打开，大量的钓鱼邮件使用短链接（例如 http://t.cn/zWU7f71）或带链接的文字来迷惑用户。如果接到的邮件是邮箱升级、邮箱停用等办公信息通知类邮件，在点开链接时，还应认真比对链接中的网址是否为单位网址，如果不是，则可能为钓鱼邮件。

（3）不要放松对“熟人”邮件的警惕。攻击者常常会利用攻陷的组织内成员邮箱发送钓鱼邮件，如果收到了来自信任的朋友或者同事的邮件，你对邮件内容表示怀疑，可直接拨打电话向其核实。

（4）不要使用公共场所的网络设备执行敏感操作。不要使用公共场所的电脑登入电子信箱、使用即时通讯软件、网上银行或进行其它涉及敏感资料的操作。在无法确定其安全性的前提下，请不要在连接 WiFi 后进行登录和收发邮件，慎防免费无线网络因疏于管理被别有用心人士使用数据截留监侦手段获取用户信息。

（5）不要将敏感信息发布到互联网上。用户发布到互联网上的信息和数据会被攻击者收集。攻击者可以通过分析这些信息和数据，有针对性的向用户发送钓鱼邮件。

六、感染钓鱼邮件莫要慌，应急招数来帮忙

当点开钓鱼邮件，造成感染后，不要惊慌，可以开展以下几种应急工作，减小钓鱼攻击产生的危害。

1.及时报告。及时报给邮箱管理员，请专业的安全人员进一步处理和开展后续系统清理以及恢复工作。

2.修改登录密码。邮箱的登录密码可能已经泄露，应在另外的机器上及时修改密码，防止攻击者获取邮箱中的邮件、联系人等敏感信息，遏制黑客进一步的攻击渗透。

3.全盘杀毒。钓鱼邮件中的链接或者附件等可能带有病毒、木马或勒索程序。发现异常应及时做全盘扫描杀毒，最好使用多个杀毒软件交叉杀毒。

4.隔离网络。切断受感染设备的网络连接（拔掉网线或者禁用网络），避免网络内其他设备被感染渗透，使安全事件范围得到控制，防止敏感文件被窃取，降低安全事件带来的损失。