钓鱼邮件攻击防范指南

转自：国家互联网应急中心
https://www.cert.org.cn/publish/main/9/2018/20180605080248533599764/20180605080248533599764_.html

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。

一、钓鱼邮件要当心，几招助你来识别

图钓鱼邮件示例

主要的识别钓鱼邮件方法如下：

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，比如伪造成本单位域名的邮箱账号或者系统管理员账号。

2.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。

3.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。

4.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。

5.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。

二、钓鱼邮件防范五要、五不要

防范钓鱼邮件要做到以下“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。同时定期下载和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。（1）及时清空收件箱、发件箱和垃圾箱内不再使用的重要邮件；（2）备份重要文件，防止被攻击后文件丢失；（3）重要邮件或附件应加密发送，且正文中不能附带解密密码。

防范钓鱼邮件要做到以下“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 Wi-Fi 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。

三、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。