钓鱼邮件防范指南

信息化办公室

易敬

2024年11月11日

一、什么是钓鱼邮件

- “**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。

二、钓鱼邮件分类

链接钓鱼

这类邮件的风险在于邮件中的网页链接，此链接往往是攻击者伪造的邮箱登录页面，诱导用户输入邮箱账号密码以盗用用户的邮箱，要求用户输入姓名、身份证号、银行卡号、银行卡密码等信息，从而盗取用户的银行账号；另一种链接指向网页暗藏木马程序，点开即中招。

二维码钓鱼

通过内含的二维码，引导用户扫描进入钓鱼网站，用户扫描二维码打开的网站往往会要求用户输入邮箱密码或银行卡密码以获取用户敏感信息。二维码也可能指向植入了病毒的App或者附件,并要求用户下载。

附件钓鱼

这类邮件的风险在于邮件附件，附件类型主要是shtml、html网页、带有木马病毒的可执行文件、压缩包，也可能是Office文件、PDF等。用户双击附件文件时，附件文件中的脚本、宏或者客户端软件CVE漏洞会自动执行，从而打开钓鱼网站或者给用户的电脑注入木马或病毒。

欺诈邮件

通过虚构的邮件内容欺诈用户，诱导用户给指定账号转账。常见的情况有：（1）邮件发送者声称自己是黑客，要求用户使用比特币转账，否则将对用户电脑和隐私进行侵害；（2）冒充政府部门，要求用户加QQ群或微信群，以进一步进行欺诈；（3）声称用户可参加培训或会议，要求用户汇款培训费、会议费。

APT攻击

伪造身份通过多次邮件来往获取信任后实施进一步欺骗。常见的情况有：通过某些手段获取用户与合作伙伴的历史邮件后，伪造带有历史邮件内容的回信，冒充合作伙伴与用户进行邮件对话，并在邮件中要求转账，从而实施诈骗。

三、钓鱼邮件识别方法

3.1 查看完整的发件人邮箱地址

电子邮箱收件人的信息由**邮件显示名**和**邮件地址**两部分组成，而邮件地址又是由**邮箱帐号**和**邮箱域名**组成。

邮件的发件人地址中往往包含发件人的姓名或身份，此处的姓名和身份一般是发件人自己声明的，**不能完全相信**。对于可疑邮件（含网页链接、二维码、附件，涉及财务的）需查看完整的发件人邮箱地址。如果发件人邮箱地址是陌生的，或者邮箱地址与发件人声明的身份不一致，则是钓鱼邮件。**对于这种邮件，如果不能分辨，需本人进行核实。**

三、钓鱼邮件识别方法

3.2 查看完整的链接URL地址

如果邮件中的链接URL地址**不常见**，比如过长、无含义的随机字符串、大量的数字、不常见的域名（.top\.cool\.website）、带有收件人的邮件地址等，则很可能是钓鱼邮件。

现在的主要攻击手段是**伪装URL地址和域名**，非常难以分辨，所以一定要判断发件人的身份，确认邮件内容的真实性

3.3 查看完整的文件名，尤其注意文件的后缀

对于附件文件不仅要看文件名，还要注意文件后缀。如有的钓鱼邮件，地址部分声明的身份是“荆楚理工学院”，但邮箱地址却是http://qq.com，http://qq.com是腾讯面向个人邮件服务，一般情况下，学校不会用个人邮箱来发信。此外，文中链接是一个压缩包，而压缩包里是.exe文件，后缀名为“exe”的文件为可执行文件，很可能是木马或病毒。

三、钓鱼邮件识别方法

3.4 异常情况

- **发件人邮箱地址和声明的身份不一致**

发件人中的姓名字段声明是管理员或同事等，但实际邮件地址为外部地址，一般都是钓鱼邮件。

- **发件人邮箱地址域名和链接地址域名不一致**

对于带有链接的邮件，发件人邮箱地址的域名和链接URL地址的域名不一致的，一般都是钓鱼邮件。尤其是打开链接页面后要求输入邮箱密码的，更应格外警惕。

- **号称是政府部门的邮件，但邮箱地址为国外个人邮箱**

政府部门发来的正式邮件不会使用outlook等个人邮箱，而且一般不会通过QQ群的方式来向企业传达比较重要事情，更不会只通过邮件来下最后通牒（“逾期视为送达”）。

- **号称是政府部门的邮件，但邮箱地址为随机编造**
- **邮箱地址为中国.cn域名，邮件文字为外文**
- **主题或正文中繁体字和简体字混合**

三、钓鱼邮件识别方法

3.4 异常情况

- **.top\.xyz \.cool\.website \.one等不常见域名**

钓鱼邮件的发件地址往往是来自.top、.xyz、.one等不常见域名。如果是不常见域的陌生地址发来的邮件一般是垃圾邮件或钓鱼邮件。

- **主题、正文措辞泛化或生硬**

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”，这是令人慌忙中犯错的手段之一。

- **打开附件后要求输入邮箱密码**
- **发件人地址的姓名字段不是发件人的身份**

企业内部发出的邮件，发件人地址中的姓名字段一般会是真实的人名，少数情况是部门名称，不会将“通知”、“警告”等表示邮件主题的词放到姓名字段。管理员不会以用户无法确定的邮箱地址给用户发送重要通知邮件。

四、如何防范钓鱼邮件

安装杀毒软件	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。
登录口令要保密	确保不向任何人主动或轻易泄露邮箱的密码信息，不将登录口令贴在办公桌或者易于被发现的记事本上。办公邮箱的密码要足够复杂，并定期更换。
邮箱账号要绑定手机	将邮箱帐号与个人手机号码绑定，不仅可以找回密码，也可接收“异地登录提醒”信息。
登录邮箱尽量使用多因素认证	多因素认证是防范邮箱账号被盗用的最有效技术手段，攻击者即使通过猜测、暴力破解等手段获取了用户的邮箱密码，没有其他的身份认证信息，仍然无法盗用用户邮箱。
不要对陌生人的邮件进行响应	陌生人发来的邮件，不要进行回复，不要点击邮件中的链接（包括“退订”等），不要加QQ群，也不要拨打邮件中的电话或手机号码，这些操作会告诉发件人当前邮箱地址是有效的，容易遭到发件人进一步的攻击。很多垃圾邮件正文中的“退订”按钮都是虚假的，点击后只会收到更多的垃圾邮件。
重要邮件及时归档	及时清空邮箱内不再使用的重要邮件；归档备份重要邮件，防止被攻击后邮件丢失。

四、如何防范钓鱼邮件

凡是 **凡是**要求点击链接或者扫描二维码的，都需要警惕。

凡是 **凡是**点击链接或者扫码后，打开的网页要求输入密码的基本都是钓鱼邮件。

凡是 **凡是**陌生人要求转账的一律不转。

凡是 **凡是**陌生人发来的邮件中带有附件的，不要双击打开邮件附件，如需打开附件要先杀毒。

凡是 **凡是**打开附件后，自动弹出页面的都是钓鱼邮件，不要输入密码。

确定 熟人要求转账汇款或者是与银行联系等必须填写个人信息时，一定要通过其他消息途径联系对方**确认**。

谢谢

信息化办公室

2024年11月11日