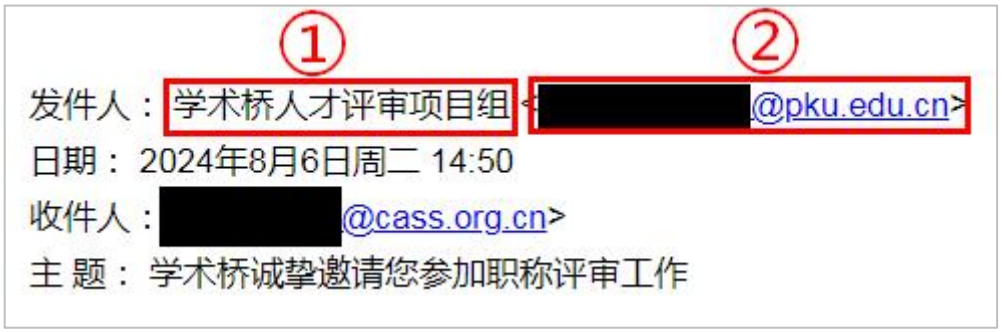
钓鱼邮件攻击防范指南

钓鱼邮件是指黑客伪装成同事、朋友、官方机构等用户信任的身份，通过发送电子邮件，诱使用户点击邮件正文中的恶意链接等方式窃取用户敏感数据等信息，从而实施进一步的网络攻击活动。

如何识别和防范钓鱼邮件攻击？可以参考以下几个步骤。

1、查看完整的发件人邮箱地址

邮件发件人地址一般包含发件人姓名或身份（如下图所示①处）、邮箱地址（如下图所示②处）两部分。



（1）发件人姓名和身份一般是发件人自己声明的，不能完全相信。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，则大概率是钓鱼邮件。

（2）学术桥发送邀请邮件的邮箱地址后缀为@mail.acabridge.edu.cn、@acabridge.edu.cn 或@acabridge.cn，请注意辨识。

2、查看正文中链接

邮件正文中链接地址如果是 IP 地址或不熟悉的域名，则大概率是钓鱼邮件。学术桥发送邀请邮件的链接地址均以

https://evaluation.acabridge.cn 开头，请注意辨识。

3、查看链接打开网站的域名

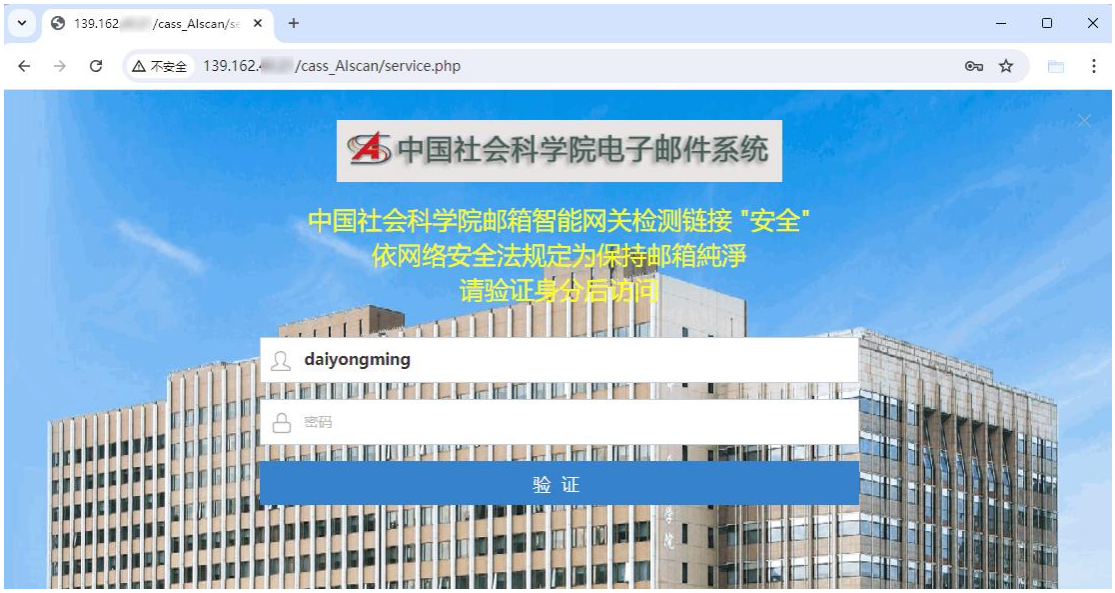
邮件正文中链接地址有可能看到的链接地址与实际打开的地址不一致，这种情况大概率是钓鱼邮件。

比如可能出现以下情况，邮件里看到的链接地址是以 https://evaluation.acabridge.cn 开头，但点击打开页面显示的 URL 地址却是 IP 地址或其他域名，这种情况即为钓鱼邮件。

4、查看是否要求输入邮箱密码

如果点击邮件中链接后，出现邮箱网关或其他验证页面，需要您输入邮箱密码的，大概率是钓鱼邮件。

如下图，钓鱼邮件可能通过伪造电子邮件系统网关检测界面，要求输入邮箱密码，用户输入密码后，邮箱账号密码会被不法分子窃取。



通过以上判断标准，可以大大降低被钓鱼邮件攻击的概率。如果您遇到不能确定是否为钓鱼邮件的情况，请联系我们或贵单位邮箱管理员咨询。