钓鱼邮件防范注意事项

对于来源不明的可疑邮件一定要做到**不信！不点！不下载！**

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、家人等信任的人，欺骗收件人将个人信息（如姓名、联系方式、口令等）回复给指定的接收者；或引导收件人连接到特制的网页，这些网页通常会伪装成和真实网站一样，令登录者信以为真，诱导输入个人信息从而实施盗取；或在邮件中夹带恶意程序（木马、蠕虫、病毒等）作为附件，诱导下载运行，从而令收件人计算机中毒。

二、 如何识别及防范“钓鱼邮件”？

1. 垃圾箱中的邮件尽量不要打开，即使打开也请不要点击或下载附件。如果不小心点击了附件请联系信息化处（如果是携带了恶意程序的附件，仅删除附件无法组织恶意程序），按照网络安全管理员的要求将邮件转发给安全团队，对邮件进行排查。如果觉得是邮箱系统误报，一定要采取电话、微信、官网查询等可信途径确认邮件的真实性。
2. 看发件人地址，钓鱼邮件和诈骗短信一样，发件人会伪装成某个官方机构发件人。
3. 看邮件标题，警惕诈骗字眼。典型的钓鱼邮件标题常包含(但不限于）**“福利、账单、邮件投递失败、包裹投递、执法、扫描文档”**等，重大灾害、疫情、疾病等热点事件常被用于借机传播。
4. 看正文目的，保持镇定从容。当心索要个人信息、登录密码、转账汇款等请求，通过内部电话等其它可信渠道进行核实。**对通过“紧急、失效、重要”等词语制造紧急气氛的邮件谨慎辨别，不要忙中犯错**。

5. 看链接网址，注意鼠标**悬停**。鼠标悬停在邮件所含链接的上方，观看邮件阅读程序下方显示的地址与声称的地址是否一致。
6. 看内嵌附件，当心木马易容。恶意电子邮件会采取通过超长文件名隐藏附件真实类型，起迷惑性附件名称诱使用户下载带毒邮件。**在下载邮件附件之前，应仔细检查附件文件名和格式，不要因好奇而下载可疑附件**。打开前用杀毒软件进行扫描。常见的带毒邮件附件为：.zip，.rar 等压缩文件格式。.doc，.pdf 等文档中也可带有恶意代码。