**关于钓鱼邮件的识别与防范**

为进一步保护电子邮件信息安全，请广大师生用户提高警惕，谨慎防范钓鱼邮件。

**一、钓鱼邮件的主要特征**

钓鱼邮件是常见的网络攻击方式，通常以通知的方式，提醒用户“邮箱异常”“升级配置”“安全警告”“欺诈恐吓”或“利益诱惑”来诱骗用户点击邮件中的链接，下载带毒文件或访问伪装网站，进而窃取用户银行账户、用户密码、身份证号和手机号码等敏感信息，或者在设备上执行勒索病毒等恶意代码实施进一步的网络攻击活动。所以，对此类带有需要点击链接、要求填写敏感信息或需要下载不明附件的电子邮件，需谨慎处理。

**二、钓鱼邮件的识别**

1、看发件人地址：

登录网页版邮件系统，点击收到邮件的发件人，可以看到邮件发件人的实际发件地址；发件人的名字是可以随意编撰的，只有具体的发件邮件地址是真实的。

2、看邮件正文：

钓鱼邮件一般会有以下特征：

（1）泛化的称呼：由于钓鱼邮件是一次发送给大量用户，所以对于直呼“你好”，或直接使用邮件账号名称后加“你好”的邮件，需提高警惕。

（2）制造恐慌气氛：对任何制造紧急氛围的邮件，需提高警惕。如要求“请在2023年5月31日前务必完成升级操作”，这是让人在慌忙之中犯错的惯用手段。

（3）不明链接：邮件可能会包含指向其他网站的链接。将鼠标放在链接处,会显示真实网址。如果显示的真实网址与邮件中所列出的链接网址不同，就很可能是一次钓鱼攻击。

（4）附件：对于邮件中的附件，一定要保持警惕，在未确定邮件可信前，请不要轻易下载。

3、其他方式核实：

如果你收到了来自朋友或者同事的邮件，但对邮件内容表示怀疑，可直接使用其他方式向其核实。

**三、钓鱼邮件的防范**

1、提高网络信息安全意识，谨慎核对邮件的发件人和收件人地址，不要被发件人名称误导。

2、不要轻信各种以管理员身份发送的学校通知、中奖信息、系统升级等通知。如需填写个人信息的，一定要再三核对网站的真实性。

3、不要随意打开不明来源的邮件附件和点击邮件正文中的可疑网址链接，不要随意打开内容可疑的邮件附件（Word/PDF/zip/rar等）。

4、设置复杂的邮箱密码，推荐设置英文（大小写）、数字、符号混合密码，建议定期更换密码。

5、安装杀毒软件，定期更新病毒库并进行全盘扫描，对于发现的漏洞或者病毒进行及时封堵及清理。对于下载的邮件附件需进行扫描，确认没有病毒后方可打开。

6、经甄别或核实系钓鱼邮件后，可以选择直接删除，不予理会，更不要回复。

7、如已点击钓鱼邮件，或者输入了账号密码等信息，应第一时间进行断网并与其他终端进行网络隔离，并对账号密码进行修改，包括邮箱的账号密码及链接中输入的账号密码。

8、钓鱼邮件中的附件或链接可能包含病毒、木马、蠕虫等恶意程序。如已点击了钓鱼邮件中的附件或链接，应立即对全盘进行病毒查杀。如有必要需要进行系统重装。