“钓鱼邮件”警示信息

全体师生:

网络安全人人有责。随着网络技术的发展，电子邮件已经成为我们日常工作学习中不可或缺的沟通工具。但不安全的邮件附件已成为网络攻击者入侵您电脑系统的渠道之一。恶意软件或病毒可能会通过电子邮件附件传播，一旦稍有不慎下载并打开了这些附件,可能会导致个人信息泄露、电脑系统受损甚至被控制。

请切记:无论任何情况下，学校都不会以邮件的形式要求您提供密码或账户信息!

钓鱼邮件是一种常见的网络攻击方式，旨在通过伪装成合法的电子邮件诱骗收件人提供敏感信息，如用户名、密码、银行账户详情等。这种邮件通常会包含看似合法的链接或附件，但实际上这些链接会引导用户访问假冒的网站，或下载含有恶意软件的附件。

为了帮助大家更好地识别和防范钓鱼邮件，以下是几个关键的警示信息和识别技巧：

1.确认发件人邮箱地址：真正的发件人邮箱地址通常是官方的，而后缀名则可以用来确认是否是官方邮箱。不要被显示的发件人名称迷惑，学校邮件系统域名为@jxufe.edu.cn。即使是用学校邮件系统域名发送的邮件，也要保持一定的警惕性，存在钓鱼邮件的发件人地址可能会被伪造可能性。

2. 多思考邮件内容：黑客可能盗用真实邮箱发送钓鱼邮件。如果邮件来自非业务部门官方邮箱地址、无落款、有错别字、有错误的部门名称、带有威胁的语气等，都可能是钓鱼邮件的迹象。

3. 找相关部门核实：在点击不明链接、下载不明附件、扫描二维码前，请三思。如果无法确定邮件的真实性，可以联系相关业务部门或智慧校园管理中心确认。

4. 谨慎对待附件和链接：尽量避免直接点击邮件中的链接，对待邮件中的网络链接，需再三确认发件人邮箱地址是否正确，确认链接的网站地址是否官方，确认链接点击是否必要。不要在其他网站输入自己的账号密码。

5. 不放松对“熟人”邮件的警惕：攻击者常利用组织内成员发送钓鱼邮件。如果收到了来自信任朋友或部门的邮件，对邮件内容怀疑需要主动联系进行核实，更不要急于下载相关附件，警惕关键字眼。

6. 看收件人地址：如果发现所接收的邮件被群发给校内大量人员，而这些人员并不是工作常用联系人或相关单位人员，那么就需要警惕，有可能是钓鱼邮件。

7. 看邮件标题：大量钓鱼邮件主题关键字涉及“系统管理员”、“告警通知”、“账户冻结”、“密码到期”、“邮件账号报备”、“邮件异常登录”等，收到此类关键词的邮件，需提高警惕。

8. 看正文措辞：对使用“亲爱的用户”、“亲爱的同事”等一些泛化问候或同事间不常用称呼的邮件应保持警惕。同时也要对任何制造紧急气氛的邮件提高警惕，如要求“账号已到期”，“邮箱容量达到上限”等。

9.看正文内容：邮件中有要求使用者点击邮件中的链接完成某项操作(如激活账号，确认密码)，一定不要随便点击链接，必要时可以先联系相关部门确认邮件内容，避免上当。

10.看附件内容：邮件中的附件信息，不要随便点击下载。诸如 word、pdf、excel、PPT、rar 等文件都可能植入木马或间谍程序，尤其是附件中直接带有后缀为.exe、.bat 的可执行文件，千万不要点击。

11.看发件的日期：公务邮件通常接收邮件的时间在工作时间内，如果收到邮件是非工作时间(如凌晨时段)，很有可能是钓鱼邮件。

希望大家提高警惕，谨防钓鱼邮件的侵害，保护好自己的个人信息和账户安全。

智慧校园管理中心

2024 年 9 月 27 日