关于进一步加强防范“钓鱼邮件”的安全风险提示

各校园邮箱用户：

学校电子邮箱的钓鱼邮件攻击日趋严峻，部分用户因访问邮件中的钓鱼链接，导致个人信息泄露、邮箱被盗、电脑中毒，甚至发生个人经济受损等情况。现提醒各广大用户进一步提高钓鱼邮件防范意识，保护好学校和个人信息安全。

**“钓鱼邮件”**是指黑客伪装成单位、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、邮箱账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动。我校邮件系统已部署异常邮箱侦测功能和垃圾邮件过滤网关，根据邮件情况动态调整垃圾邮件过滤规则，不断提高钓鱼邮件过滤能力。但由于钓鱼邮件特征多变，单靠系统拦截无法杜绝，提高广大用户个人安全意识，看清钓鱼本质，才是对钓鱼邮件最有效的防御。

一、近期我校部分“钓鱼邮件”的特征

1.以“网络安全攻防演练自查”为由的钓鱼邮件

2．以“验证更新账户信息”为由的钓鱼邮件

3．仿冒上级部门的钓鱼邮件

4．以 “升级账户”为由的钓鱼邮件



5．以“安全警告”为由的诈骗钓鱼邮件

6．以“账户暂停”为由的钓鱼邮件

二、如何识别“钓鱼邮件”

1.不要轻信发件人地址中“显示名”（如下图），将鼠标放到显示名处，与**显示不一致**的一定是“钓鱼邮件”。发件人的显示名是可以随意编撰的，只有具体的发件邮件地址是真实的。

2.不要轻易点开陌生邮件中的链接，不随意下载和安装附件。

3.不要放松对“熟人”邮件的警惕。

4.不要使用公共场所的网络设备执行敏感操作。

5.不要将敏感信息发布到互联网上。

6.我校电子邮件通知均以学校官方域名：@wfmc.edu.cn或@stu.wfmc.edu.cn发出，非学校域名发出的通知都是骗子。

7.我校邮件系统不会以任何名义索要用户的邮箱名和密码或个人银行账户等信息。

**三、感染“钓鱼邮件”应急招数**

1.修改登录密码。邮箱的登录密码可能已经泄露，应在另外的机器上及时修改密码，防止攻击者获取邮箱中的邮件、联系人等敏感信息，遏制黑客进一步的攻击渗透。

2.及时报告。及时报给邮箱管理员，请专业的安全人员进一步处理和开展后续系统清理以及恢复工作。

3.全盘杀毒。钓鱼邮件中的链接或者附件等可能带有病毒、木马或勒索程序。发现异常应及时做全盘扫描杀毒，最好使用多个杀毒软件交叉杀毒。

4.隔离网络。切断受感染设备的网络连接（拔掉网线或者禁用网络），避免网络内其他设备被感染渗透，使安全事件范围得到控制，防止敏感文件被窃取，降低安全事件带来的损失。

校园网邮箱服务电话：8462296。

网络信息中心

2023年9月4日