中国地质大学（武汉）

关于开展2024年钓鱼邮件演练的通知

各位老师同学：

随着信息技术的飞速发展，网络安全问题日益凸显，尤其是网络钓鱼攻击，已成为威胁个人信息与数据安全的重要因素之一。为提高师生网络安全意识，提升师生对钓鱼邮件的识别防范能力，信息化工作办公室将于近期在全校范围内开展校内邮箱钓鱼邮件演练。现将有关事项通知如下：

一、演练目的

1、提高警惕性：通过模拟真实的钓鱼邮件场景，使师生能够识别并警惕各类钓鱼邮件，避免点击恶意链接或下载附件。

2、增强防范技能：引导师生如何正确处理可疑邮件，包括如何验证邮件真实性、报告可疑邮件等。

3、完善应急机制：检验学校网络安全应急响应流程的效率和效果，确保在遭遇真实钓鱼攻击时能够迅速有效地应对。

注：本次演练活动未获取和记录广大师生任何隐私信息（除邮箱地址以外），未涉及任何非法和恶意软件。

二、演练安排

演练时间：2024年11月

演练范围：全校所有师生，包括但不限于教职工邮箱用户、学生邮箱用户。

演练方式：校内钓鱼邮件演练将通过“不提前告知”“不定期发送”的方式，面向所有校内电子邮箱发送钓鱼邮件，演练结果会在一定范围内通报。

三、钓鱼邮件防范提示

1、提高邮箱安全防范意识，邮箱密码应使用符合复杂度要求的组合密码，并定期修改密码。

2、对于要求提供个人信息的邮件，请谨慎对待并再三确认内容的真实性，不要随意输入账号、密码等个人信息。

3、避免直接点击不明邮件中的链接。

4、对带有附件的任何邮件，务必不盲目点开、下载甚至安装。

5、登录邮箱的终端设备应安装正版杀毒软件，并及时更新。

6、我校邮件域名为“xxx@cug.edu.cn”。如收到以学校名义发出的邮件请核查域名是否完全一致。遇到存在特殊邮件后缀时，请大家务必格外仔细核对，有条件的建议增加电话回访确认相关信息。

钓鱼邮件攻击防范知识可参考国家互联网应急中心发布的钓鱼邮件攻击防范指南：

https://www.cert.org.cn/publish/main/9/2018/20180605080248533599764/20180605080248533599764_.html

如有任何疑问或发现真实的网络安全威胁，请立即联系信息化工作办公室，联系电话：67885015

信息化工作办公室

2024年11月6日