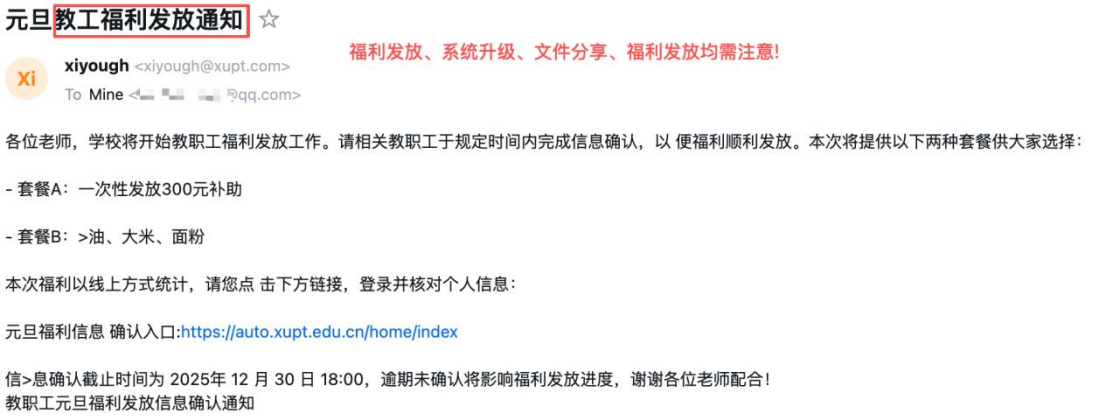
钓鱼邮件识别与防范指南

2025 年 12 月 29 日信息网络中心团队向全体教职工发送了模拟钓鱼邮件“元旦福利发放通知”。本次演练是“金蝉”黑产团伙近期对我校多次钓鱼攻击后的专项防范行动，现告知防范要点：

一、校园场景常见钓鱼类型



金钱陷阱： 高温津贴、绩效奖金、退税补贴。诱导输入银行卡号、身份证号，直接造成资金损失 。

系统升级 ：“邮箱即将停用，立即验证”。套取统一身份认证账号密码，成为继续群发钓鱼的跳板 。

文件分享 ：“请查阅/审批这份合同”。附件含木马，打开后电脑被远程控制 。

发票订单 ：“您有一笔电子发票待下载”。诱导下载带毒文件，植入勒索或窃密木马 。

二、一眼识别钓鱼邮件 5 招

看域名：所有官方通知必用 ***@xupt.edu.cn 或 ***@xiyou.edu.cn；出现 edu.net / xupt.com / 短链接均为仿冒。

看时限：使用“12 小时内未验证将停用”“今日 17:00 前务必完成”制造紧迫感。

看链接：鼠标悬停可显示真实网址；任何要求填写银行卡、短信验证码的页面

100% 钓鱼。

看附件：*.exe / *.zip / *.iso / *.js 等扩展名，或大于 10 MB 的“发票.zip”，一律先杀毒再打开。

三、误操作紧急处置 3 步

1. 立即断网：拔掉网线/关闭 Wi-Fi，防止木马回传。

2. 全盘杀毒：推荐使用火绒、Defender 进行全面扫描。

3. 即刻改密：在另一台干净设备上修改校园统一身份认证、邮箱、网银密码；如已输入银行卡号，请立即冻结卡片并联系银行。

四、报告与求助

发现可疑邮件，请立即转发至或拨打信息网络中心 029-88166125（工作日 8:30-17:30）。我们将统一进行威胁情报分析和域名阻断。