

钓鱼邮件识别与防范指南

2025年12月29日信息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

元旦教工福利发放通知 ☆

 **xiyough** <xiyough@xupt.com>
To Mine <@qq.com>

福利发放、系统升级、文件分享、福利发放均需注意!

各位老师，学校将开始教职工福利发放工作。请相关教职工于规定时间内完成信息确认，以便福利顺利发放。本次将提供以下两种套餐供大家选择：

- 套餐A：一次性发放300元补助

- 套餐B：>油、大米、面粉

本次福利以线上方式统计，请您点击下方链接，登录并核对个人信息：

元旦福利信息 确认入口：<https://auto.xupt.edu.cn/home/index>

信息确认截止时间为 2025年 12月 30日 18:00，逾期未确认将影响福利发放进度，谢谢各位老师配合！
教职工元旦福利发放信息确认通知

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

元旦教工福利发放通知 ☆

 **xiyough** <xiyough@xupt.com>
To Mine <@qq.com>

官方域名为xupt.edu.cn或xiyou.edu.cn
所有类似edu.net / xupt.com / 短链接均为仿冒

各位老师，学校将开始教职工福利发放工作。请相关教职工于规定时间内完成信息确认，以便福利顺利发放。本次将提供以下两种套餐供大家选择：

- 套餐A：一次性发放300元补助

- 套餐B：>油、大米、面粉

本次福利以线上方式统计，请您点击下方链接，登录并核对个人信息：

元旦福利信息 确认入口：<https://auto.xupt.edu.cn/home/index>

信息确认截止时间为 2025年 12月 30日 18:00，逾期未确认将影响福利发放进度，谢谢各位老师配合！
教职工元旦福利发放信息确认通知

元旦教工福利发放通知 ☆



xiyough <xiyough@xupt.com>
To Mine <[redacted]@qq.com>

各位老师，学校将开始教职工福利发放工作。请相关教职工于规定时间内完成信息确认，以便福利顺利发放。本次将提供以下两种套餐供大家选择：

- 套餐A：一次性发放300元补助

- 套餐B：油、大米、面粉

本次福利以线上方式统计，请您点击下方链接，登录并核对个人信息：

元旦福利信息确认入口：<https://auto.xupt.edu.cn/home/index> **使用确认截止时间造成紧迫感**

信息确认截止时间为 **2025年12月30日18:00**，逾期未确认将影响福利发放进度，谢谢各位老师配合！
教职工元旦福利发放信息确认通知

222.24.61.195/info.html?uuid=da979d02-31d2-421d-8e81-9fa21bd51a16

注意邮箱内跳转提示，并查看真实网址，

教职工福利发放信息确认

各位老师，学校将开始教职工福利发放工作。请相关教职工于规定时间内完成信息确认，以便福利顺利发放。本次将提供以下两种套餐供大家选择：

- 套餐A：一次性发放300元补助
- 套餐B：油、大米、面粉

信息确认截止时间为 2025年12月30日18:00，逾期未确认将影响福利发放进度，谢谢各位老师配合！

姓名 *

手机号 *

工号 *

任何要求填写银行卡、短信验证码的页面 100%为钓鱼

银行卡号 *

福利套餐选择 *

套餐A：一次性发放300元补助 套餐B：油、大米、面粉

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。