反诈之“钓鱼邮件”教你几招

轻松识破！

信息网络工程研究中心（信息化办公室）
Information and Network Engineering and Research Center (Office of Information Technology)

典型案例

2022年5月18日，大量搜狐员工收到一封来自“搜狐财务部”名为《5月份员工工资补助通知》的邮件，不少员工按照附件要求扫码，并填写了银行账号等信息。然而不但没有等到所谓的补助，工资卡内的余额也被划走了，经调查总共被骗4万余元。搜狐集团回应，**实为某员工使用邮件时被意外钓鱼导致密码泄露，进而被冒充财务部盗发邮件。**

我校师生也经常反馈收到了钓鱼邮件，有的师生**点击钓鱼链接**，**输入账号密码**，导致**账号被盗**，有的**甚至造成财产损失**！

典型案例

近日很多老师反馈收到了这封邮件，为黑客盗用华工邮箱，给本校用户发送的**钓鱼邮件**！

关于：华南理工大学教工邮件系统《已告知三次未验证通过邮箱》即将进行暂停服务删除用户处理！！！

发给

2022-06-27 13:50 隐藏信息

发件人: @scut.edu.cn>

收件人: @scut.edu.cn>

时间: 2022年6月27日 (周一) 13:50

大小: 7 KB

发件人地址为华工后缀，但根据内容判断，为用户邮箱账号被盗！
若无法判断，请联系对方核实

请至以下备案地址验证你的邮件账户。邮箱系统安全防护！

《请严格遵照以下操作指南完成备案》未备案邮箱则视为无人使用将暂停服务！
1，提交申请
2，初步审核
3，等待通知
4，备案完成

华南理工大学
South China University of Technology

邮箱内容有华工LOGO，伪造度高

邮箱系统安全防护已通知多次；

提醒：未验证通过邮箱，根据国家安全联网备案中心通告将进行停号删除用户处理。

请您立即点击登记：华南理工大学邮件系统webmail.scut.edu.cn联网备案登录

请各单位高度重视，传达通知精神至每一位用户，切实提高广大

中国互联网信息中心

2022年6月27日

该链接实际上是外域链接，为钓鱼链接，
请勿点击！
若不慎点击，请勿输入账号密码！

典型案例

冒充领导

在吗?

张

发件人: 张 <ebonyrose19723@gmail.

时间: 2022年6月1日 (周三) 10:42

大小: 6 KB

在办公室吗?

冒充管理员

@scut.edu.cn【未知登录异常提醒】

【管理员】

发给 2022-06-07 23:54 隐藏

发件人: 【管理员】<market@jinglun.com.cn>

收件人: @scut.edu.cn>

时间: 2022年6月7日 (周二) 23:54

大小: 7 KB

@scut.edu.cn

检测到多次异常地址与未知设备尝试登录，这个登录已被阻止，为保护你的账
安全，现需备案验证为本人使用。（如非本人操作请立即备案，是本人操作确
本人操作即可）

请遵照以下操作指南完成备案实名，以免给个人和公司造成损失!

-

请大家在6月12日前在以下官网备案完成，否则会影响到邮箱
使用!

点击确认为本人登录

冒充管理员

关于邮件系统升级通知!

IT

发给 @scut.edu.cn

发件人: IT<zy-yuan@zgcmc.com>

收件人: @scut.edu.cn< @scut.edu.cn>

时间: 2022年5月13日 (周五) 05:00

大小: 9 KB

您好:

为提升系统服务能力，邮件系统拟定于2022年6
除长期未登陆(使用)的邮箱操作，逾时未备案将会认为
次维护不会对用户留存在系统中的邮件产生任何影响。

点击此处进行备案: : http://192.168.22.23/in

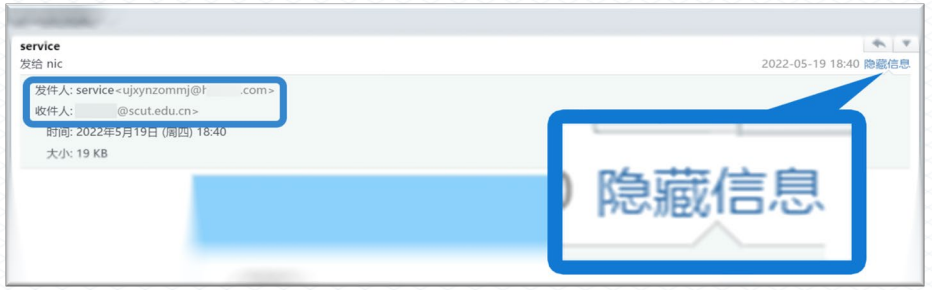
(为了您的安全，请使用IE以外的浏览器进行操作)

你能一眼识破钓鱼邮件吗?

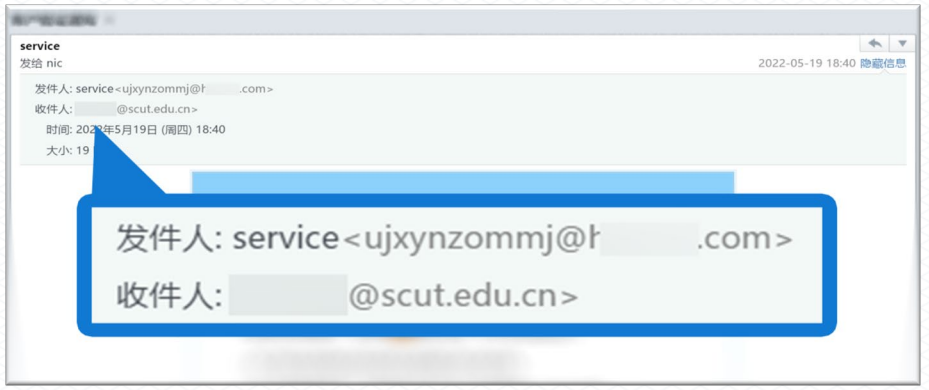
如何识破钓鱼邮件?

1、看发件地址

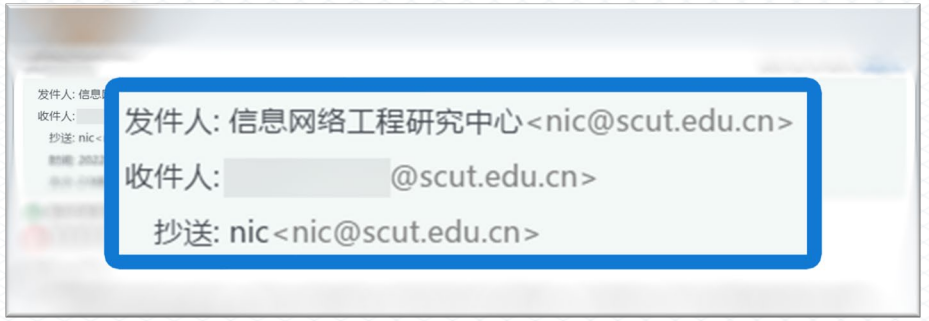
1 点击“详细信息”
查看完整的发件地址



2 不是**@scut.edu.cn（教工邮箱）**
或**@mail.scut.edu.cn（学生邮箱）**
的后缀均不是华工邮箱发出的邮件!



3 即使是**公务邮箱**发出的邮件
也要根据内容注意甄别!



如何识破钓鱼邮件?

此外，很多钓鱼邮件发件人喜欢用“@gmail.com”、“@hotmail.com”等国内少见的邮箱，此类邮件极有可能是钓鱼邮件。如近期较多调研邮件发件人姓名使用校领导的名字，实际邮箱地址并非我校教工邮箱地址的钓鱼邮件。

如何识破钓鱼邮件?

2、看邮件标题

常见钓鱼邮件标题

冒充管理员

《您的账号登录异常》
《您的邮箱需要升级》
《您的邮箱容量已满》
《您的密码已过期》
……

冒充领导、同事

《在吗？》
《最近过得好吗？》
……

冒充部门或机构

《工资补助发放通知》
《个人所得税缴纳通知》
《培训通知》
《满意度评价》
……

跟进热点，诱导点击

《最新疫情通报》
《热点新闻》
……

如何识破钓鱼邮件?

3、看正文内容

钓鱼邮件的最终目的是通过精心伪造的内容，取得收件人的信任，骗取收件人的账号和密码等敏感信息、诱惑收件人点击邮件中的木马链接网页、骗取收件人的财物等。

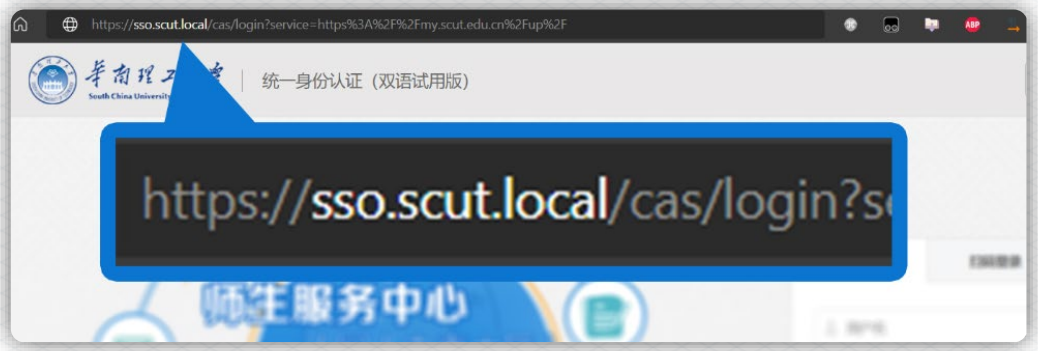
对使用“亲爱的用户”、“亲爱的同事”等一些泛化问候的邮件应保持警惕。同时也要对任何制造紧急气氛的邮件提高警惕，如要求“请务必今日下班前完成”等。

当心垃圾邮件的“退订”功能，有些垃圾邮件正文中的“退订”按钮可能是虚假的。**点击之后可能会收到更多的垃圾邮件，或者被植入恶意代码。**

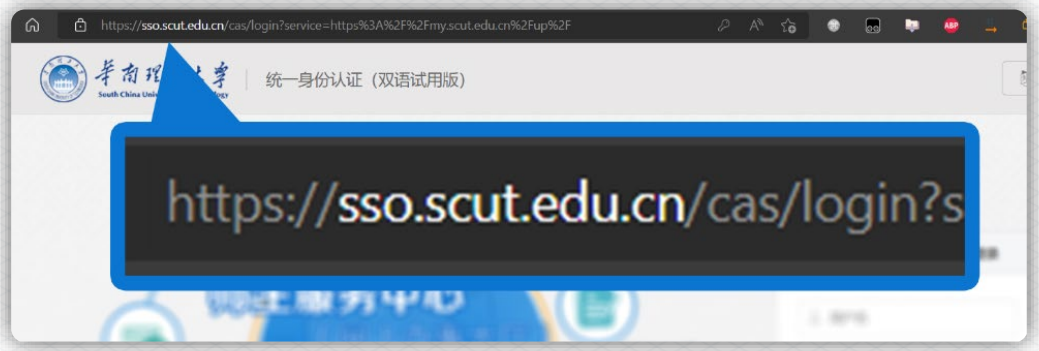
如何识破钓鱼邮件?

4、看跳转的链接

请勿点击钓鱼邮件中的链接，如确认不是钓鱼邮件，点击链接后也请注意在地址栏（不是正文显示的链接）看跳转后的链接，例如点击邮件链接后跳转的华工统一认证页面：



不是*.scut.edu.cn的域名均不是华工网站，可能为伪造网站，请谨慎输入用户名和密码！



正确的华工网站域名：

*.scut.edu.cn

如何举报钓鱼邮件

当您遇到钓鱼邮件，可**直接加入黑名单**，拒收后续邮件，**并将钓鱼邮件举报给网络中心。**网页端可点击“更多”-“举报”，或将邮件转发到“spamreport@scut.edu.cn”，以便我们更新垃圾邮件的过滤规则。

但是钓鱼邮件发件人经常更换邮箱名以及内容，很难做到完全过滤，还请您注意甄别。

如何防范钓鱼邮件?

请牢记以下几点

1. 我校域名为**scut.edu.cn**，如果邮箱或链接域名不是**scut.edu.cn（教工邮箱）或mail.scut.edu.cn（学生邮箱）**，却自称自己为学校相关部门和机构等，绝对有问题！
2. **个人的账号、登录密码不要泄露**，定期修改密码，设置高强度密码
3. **公私邮箱要分离**，不用工作邮箱注册公共网站的服务，也不要用工作邮箱发送私人邮件
4. **不要轻信发件人地址的“姓名”**，实际上姓名是可以随便设置的
5. 对熟人或华工邮箱发出的邮件，**如有疑问，请直接打电话向其核实**
6. **不要随意打开邮件的链接或附件**，有些钓鱼邮件的链接或附件可能带有病毒、木马或勒索程序
7. **安装杀毒软件**。如Windows系统自带的Windows 安全中心、火绒安全软件、360安全卫士等，**保持开启状态，设置自动更新病毒库**

如何防范钓鱼邮件?

发觉自己被上钩，如何自救?

当您不小心点击链接、输入密码，或打开了可疑的附件，请：

1. **立即删除可疑邮件的附件**
2. **使用杀毒软件进行全盘扫描**
3. **立即前往所输入账号的官方网站重置您的账户密码**，例如华工统一认证的账号密码

   重置地址为https://sso.scut.edu.cn/cas/pwd

最后

我校邮箱系统已经为各位教工过滤大量的垃圾邮件，过滤率已经达到80%以上，包括具备高度垃圾特征的钓鱼邮件，但是**由于部分钓鱼邮件的特征跟正常邮件相似，无法有效过滤，如有这些漏网之鱼，请广大师生收到后根据以上指引识别和处理！**