**邮件系统使用安全常识**

电子邮件的广泛使用，催生了各种邮件欺诈。例如通过攻陷邮箱系统来获取企业、政府敏感信息，以及敏感文件，特别是邮箱跨站、挂马、欺骗等已经成为邮箱攻击的最常使用的手段。

一、常见邮件仿冒手段及邮件攻击诈骗

1.仿冒发件人别名

2.仿冒发件人

3.相似域名仿冒

4.仿冒回复人

5.仿冒企业邮件

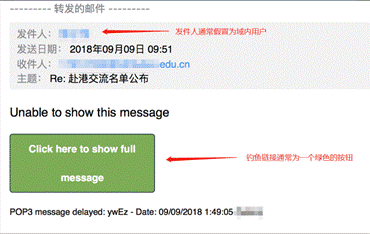
6.勒索软件攻击

7.商业邮件诈骗

二、钓鱼邮件

以企业的名义对外发送钓鱼邮件，特别是仿冒电子商务企业（淘宝、京东、亚马逊等）、公共事业（公检法，12306等）发送钓鱼邮件时危害极大。

2018年9月7日，Coremail CAC安全中心发现有一种新型的钓鱼邮件正在呈现扩散趋势，由于该钓鱼邮件的伪装程度较高，部分用户容易轻信误点击钓鱼链接。此类邮件通常会伪装成企业内部的用户，向其他内部用户发送钓鱼邮件。链接通常是一个绿色的按钮，误点击链接的用户会被窃取历史收发邮件的主题信息，进一步向企业内部其他人发送钓鱼邮件。利用历史收发邮件的主题信息，进一步迷惑其他用户，造成钓鱼邮件进一步扩散。



该钓鱼邮件中的链接会将用户引导至恶意网页。恶意网页可能会有多种情况，但在每种情况下都是恶意的：

情况1：恶意页面会提示用户目前系统存在危险，需要点击下载安全防御工具，该工具实际上是一个木马程序，下载安装后会窃取用户信息。

情况2：恶意页面会提示一个类似中奖的页面，通过点击“OK”的按钮迷惑用户，让用户在不知情在情况下点击该按钮，然后下载木马程序，窃取用户信息。

情况3：恶意页面会伪装成可信页面在样子，提示用户输入自己的账号，窃取用户登录信息。

普通邮箱用户日常使用邮箱时请注意此类邮件，如果发现类似或者可疑的邮件，不要轻易点击链接，并及时通知管理员。

用户如果误点击了相关链接，请给自己的机器进行杀毒，同时更换自己的邮箱密码，并密切关注是否有异常IP登陆自己的邮箱。

三、邮件安全使用

1.安全的使用环境很重要

（1）邮箱专人专用，不要多人使用，如有人员变动，请及时更改密码；

（2）尽量不要在公共计算机上使用邮箱，若使用记得及时退出邮箱；

（3）在确保网络安全的情况使用企业邮箱；

（4）客户端电脑安全；

（5）电脑要及时更新补丁修复漏洞、做好病毒和木马排查工作；

（6）不浏览不安全的网站，不从一些可疑的钓鱼网站登录邮箱；

（7）不要轻易打开陌生人发来的网址链接和可疑的附件。

（8）阅读邮件时留意相关发件人账号信息，如果是陌生账号邮件保持警惕，且不轻易点击邮件中的链接。

2.邮箱密码，至关重要

目前邮箱密码以“数字+字母+特殊符号”组合的形式设置，尽量避免使用规律性比较强的密码。黑客想要破解这样强度的密码难道也相对更大。

3.加强域内账号监管

要经常查看邮箱是否设置了自动转发，如果不是自己添加的自动转发，请立即更改密码。

4.多重密保，绑定微信启用安全登陆

目前我校使用的腾讯企业邮箱，在绑定微信启用微信安全登陆，每次登陆使用微信二次验证码，可以更好保障账号安全。具体操作详细见“贵州理工学院邮件系统用户操作手册”。

5．微信异地登陆提醒，自助修改密码

目前企业邮箱在绑定微信以后，如被异地登录，微信会收到异地登录提醒。如遇可以异地登录，需要及时登陆mail.git.edu.cn，通过“忘记密码”修改密码，并且开启微信安全登陆。



如有必要可以及时联系管理员。