河南省教育信息安全监测中心

关于电子邮箱安全使用建议

2020 年 3 月 10 日

关于电子邮箱安全使用建议

事件描述

电子邮件作为互联网行业的重要组成部分，是日常信息沟通、公文流转等办公活动和管理决策的信息传递载体，是高校信息化和电子政务的基础。然而电子邮件系统面临着越来越多的信息欺骗、机密泄露、病毒入侵等各种各样的安全风险。接教育部安全通知公告，近期发现我国大量党政机关电子邮箱遭渗透攻击，存在失泄密风险。针对该安全隐患省教育信息安全监测中心提供如下电子邮箱安全使用建议。

安全建议

一、使用复杂密码并定期修改

在设置密码时，要尽量避免使用个人信息，包括自己和家人的姓名、生日、手机号、身份证号等。因为这些个人信息常常会处于公开状态，非常容易被破译和猜测到。同时，也要避开过于简单的弱密码，比如 abc123、123456、iloveyou、admin 等等。另外建议，不要长期使用相同的密码，养成定期修改密码的习惯，安全更有保障。

二、定期检查电脑和邮箱环境

高校用户尽可能用个人或单位电脑登录高校邮箱，并定期对电脑查毒，防止木马植入。此外，还要检查邮箱设置，比如来信分类，自动转发，自助查询 IP 登录等日志记录，及时排除问题。

三、留意发信人是否真实

学术往来，商务交流等，要看清收发人，留意发信人是否真实，是否有代发标志，是否帐号相似，任何高校邮箱服务商以及学术论坛都不会以升级等名义让您点击链接进而获取老师信息。对于收到关于支付的邮件时，请与对方电话沟通确认后再进行支付。

四、使用邮件加密功能

建议老师在发送机密性较高的邮件时，使用邮件加密功能，收件人此时需要用密码才能查看邮件。另外，在收到邮件时，要留意发信人的信息是否完整，比如英文拼写是否流畅，高校后缀是否正确。如 edu.cn 可能会被伪造成 eud.cn 等。

五、来历不明的邮箱附件点击要谨慎

很多木马都藏在来历不明的附件中，当您出于匆忙点击附件时，您的电脑就可能中

上木马病毒，黑客就会窃取您的电脑资料和邮件来往等信息，进而冒充您给外界发送邮件，给您造成不必要的损失。

六、其他安全措施

- 建议开启手机验证服务；
- 建议安装正版杀毒软件、反木马软件，不要随便在网站上留下您的邮箱帐号和密码；
- 建议清除浏览器的 cookie，切勿选择自动记住密码（包括浏览器和客户端）；
- 建议在邮箱设置中开启客户端授权码进行使用，可有效防止其他人使用客户端登录您的邮箱；
- 建议管理员或个人至少每月对邮箱进行安全体检；
- 建议开启邮箱的登录二次验证功能，包括采用手机二次验证、备用安全码等；
- 建议各高校应建立涉公邮箱的安全管理制度，明确邮箱的安全责任。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052