山西省教育科学研究院

山西省教育科学研究院
关于开展钓鱼邮件专项学习的通知

根据教育厅下发的《关于开展钓鱼邮件专项演练的通知》，为提高我院教职工的安全意识和反钓鱼能力，山西省教育科学研究院开展钓鱼邮件专项学习，了解学习相关案例和资料。

一、相关案例

案例一：

一名教师在收到一封看似来自学生的钓鱼邮件后，点击了邮件中的链接，并在该链接中输入了自己的登录信息。该教师在不知情的情况下，将自己的登录信息传递给了攻击者。攻击者随后成功登录了教师的电子邮件账户，并从中获取了一些敏感信息。

案例二：

一名政府官员收到了一封钓鱼邮件，邮件中要求其提供其所有的安全认证凭证。该官员认为邮件来自正规机构，便点击了邮件中的链接，并在该链接中输入了其所有的安全认证凭证。攻击者获取了该官员的安全认证凭证，从而成功登录了其账户，并窃取了该官员的敏感信息。

二、面对钓鱼邮件注意事项

教育行业的钓鱼邮件主要针对学生、教师和家长等群体，攻击者会利用伪装成官方机构或者熟悉的个人名义，诱导用户点击

邮件中的链接或者附件，从而窃取个人信息或者实施其他攻击。以下是面对教育行业的钓鱼邮件的注意事项:

警惕邮件的来源。用户在收到可疑邮件时，要先查看邮件的发件人地址，确保是否为正规机构或者个人名义。同时，用户也要注意邮件的主题、内容和语气等是否与正规邮件一致。

注意邮件中的链接和附件。攻击者会在邮件中嵌入恶意链接或者附件，用户在点击链接或者下载附件之前，要先确认链接和附件的来源和内容是否可信。同时，也要注意不要随意下载未知来源的文件，以免被病毒或者恶意软件感染。

及时更新防病毒软件。用户在收到可疑邮件时，应该立即更新防病毒软件，并开启实时保护和邮件过滤功能，以及及时升级防病毒软件的病毒库，以便能够更好地识别和拦截恶意邮件。

注意个人信息的保护。用户在使用电子邮件时，应该注意保护个人信息，如账户密码、银行卡号、身份证号等，避免将这些敏感信息泄露给不明来源的人或者机构。

定期清理邮箱。用户在使用电子邮件时，应该定期清理邮箱，删除无用的邮件和附件，以免被攻击者利用。同时，也要清理浏览器自动保存的账户和密码，防止邮箱直接被登录，被攻击者利用。

山西省教育科学研究院

2023 年 11 月 30 日