网络安全与人身安全培训

本次培训旨在提高大家对网络安全和人身安全的认知和意识。我们将深入探讨网络安全风险的预防和处置，并介绍日常生活中人身安全的注意事项。通过这个培训，希望大家能够更好地保护自己，维护组织的信息安全。

老a

老师 魏

网络安全与人身安全培训

网络安全和人身安全是当今社会两大重要领域,对我们每个人都至关重要。本次培训将系统地为您介绍网络安全知识和人身安全技能,帮助您全面提高自我保护意识和技能,有效应对各种安全隐患。

培训目标

了解网络安全威胁

让参训人员了解常见的网络攻击类型，如病毒、木马、钓鱼、勒索软件等，掌握相应的防范措施。

提高网络安全意识

培养参训人员的网络安全意识，增强对个人隐私、重要信息的保护意识和技能。

掌握人身安全技能

帮助参训人员识别危险情况，学习自我防卫和应急逃生的基本方法，提高自我保护能力。

应对紧急情况

让参训人员了解应急救援知识，培养在网络攻击或人身安全事故发生时的应对能力。

培训对象

公司员工

本培训针对公司各部门的所有员工，旨在提高大家的网络和人身安全意识。

远程办公人员

对于大量采取远程办公模式的员工而言，网络和个人安全防护尤为重要。

高管人员

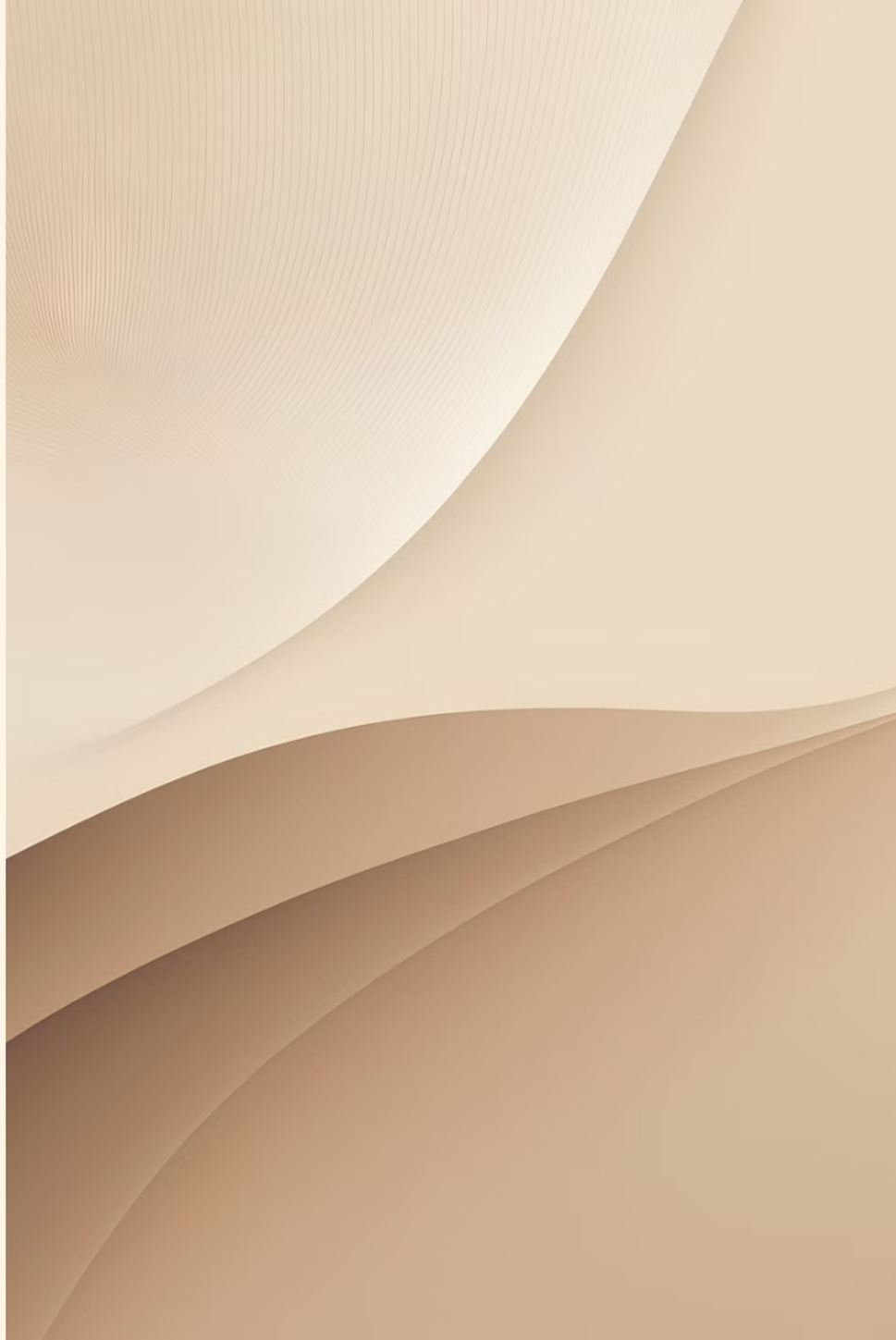
公司高层人员不仅要关注个人安全，还需了解网络安全风险，以更好地制定相关政策。

IT 负责人

IT 部门人员应掌握专业的网络安全知识和应急处理技能，为其他员工提供指导。

培训内容

本次培训将全面涵盖网络安全和人身安全两大方面的知识和技能。从基础概念到实践应用，为参训人员提供系统性和针对性的培训，帮助他们掌握必要的防范和自救知识，提升安全意识和自我保护能力。



网络安全基础知识

网络基础

了解网络的基本工作原理及组成部分，为后续的网络安全知识奠定基础。

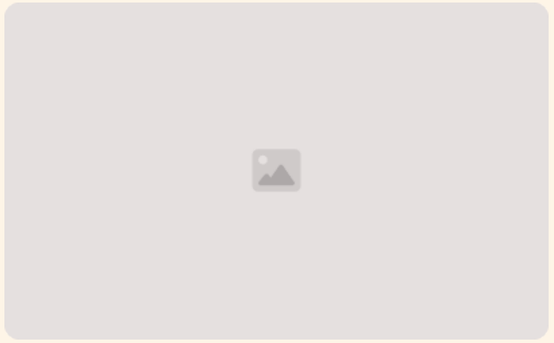
安全隐患

知晓网络中可能存在的常见安全隐患，如病毒、木马、黑客攻击等。

防护措施

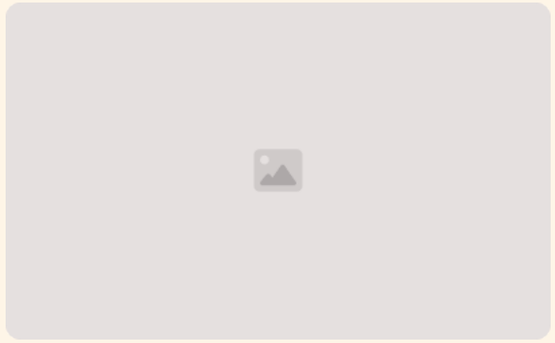
学习基本的网络安全防护知识，如防火墙、病毒防护软件的使用。

网络攻击类型及防范措施



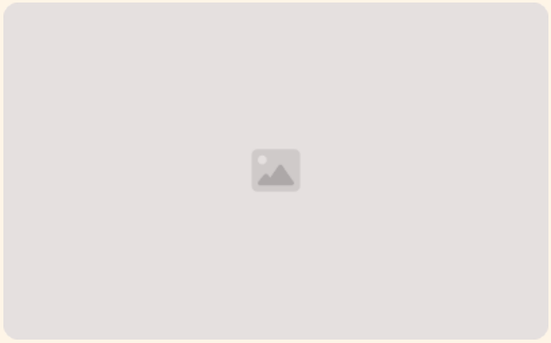
勒索软件攻击

勒索软件能够恶意加密文件并索要赎金,对个人和企业造成严重损失。定期备份数据、使用可靠的反病毒软件是关键防御措施。



非法入侵攻击

黑客可通过各种手段窃取账号密码、植入后门进入系统。加强身份认证、及时更新软件、限制访问权限是有效预防方法。



分布式拒绝服务攻击

大规模的请求流量能瘫痪网站和服务器。采用CDN、流量清洗等技术可有效阻挡此类攻击。

个人信息保护

1 信息泄露风险

个人隐私和机密信息被不当使用和披露，可能造成财产损失、声誉受损以及其他严重后果。

2 合法合规要求

个人信息保护涉及法律和道德层面的责任，要遵守相关隐私保护法规。

3 信息收集及存储

收集个人信息时需经过授权同意，并采取安全措施进行妥善保管。

4 信息使用及披露

只能在获得授权的前提下，按照约定目的使用和共享个人信息。

密码管理

设置强密码

使用包含大小写字母、数字和特殊字符的复杂密码可以大幅提高安全性。定期更换密码并避免重复使用是很重要的。

使用密码管理器

密码管理器可以安全地存储和管理您的所有密码，避免记忆或手动输入。这样可以减少泄露风险并提高使用便利性。

启用双因素认证

在重要账户上启用双因素认证，除了密码还需要另一种验证方式，如短信或应用程序代码，可以大大提升安全性。

网络欺诈识别

识别诈骗信息

学会识别可疑链接、虚假网站以及不合理的要求，提高警惕避免上当受骗。注意查看发件人、域名和内容是否合理。

风险评估和报告

及时评估网络欺诈风险，并将可疑情况及时报告相关部门。这有助于降低损失并协助调查打击犯罪分子。

保护个人信息

切勿轻易透露个人隐私信息，尤其是银行卡号、密码等关键数据。遇到可疑情况要及时采取防范措施。

提高警惕意识

提高对网络欺诈的警惕和认知，保持谨慎态度，不轻易相信来历不明的信息和要求。

网络隐私保护

1 保护个人隐私数据

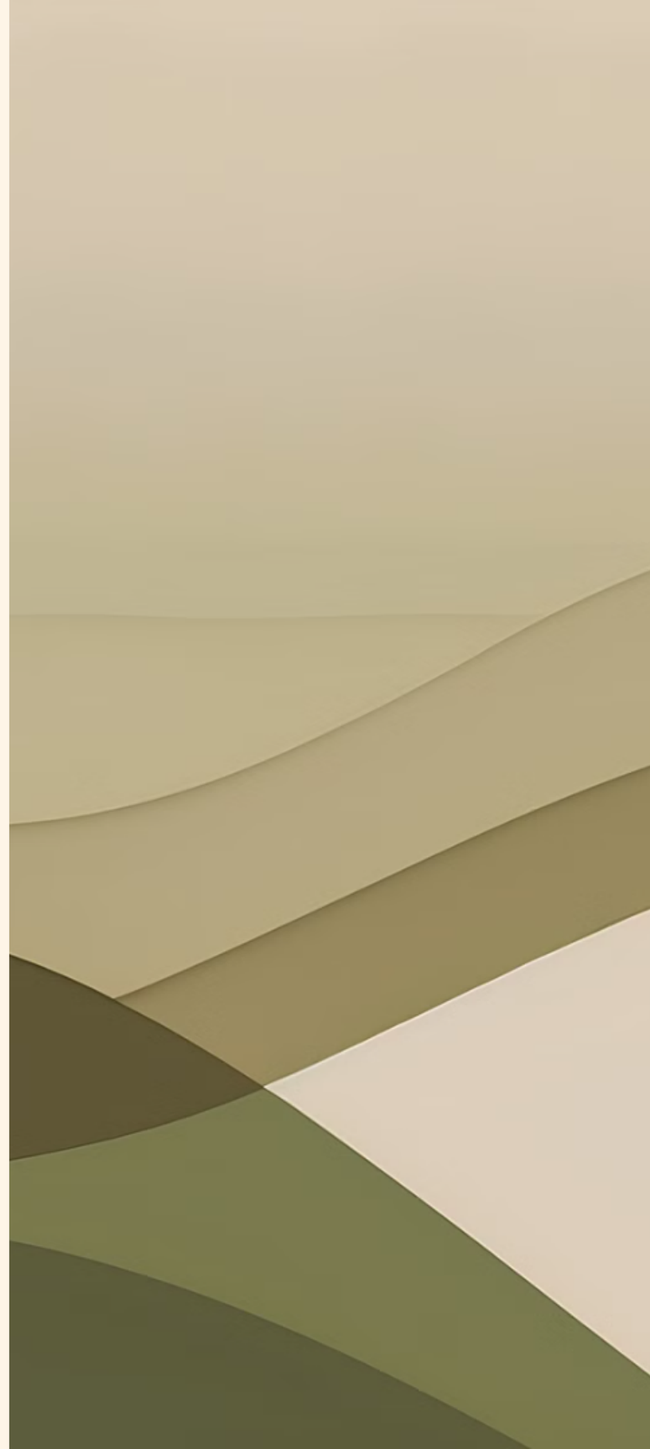
谨慎管理个人信息和敏感数据,避免被泄露或被他人获取。定期检查网络账号隐私设置,限制他人对您信息的访问权限。

2 避免在公共场合泄露隐私

在公共Wi-Fi环境或公共场合谨慎使用手机和电脑,避免输入密码、谈论敏感信息等,防止隐私被他人窃取。

3 善用隐私保护工具

使用可靠的反病毒软件、VPN、加密工具等,保护自己免受网络窃取、监视和跟踪,有效隔离隐私泄露。



社交媒体安全使用

账号密码安全

设置复杂强度高的密码, 定期更新, 并开启双重身份验证。避免使用简单密码或重复利用。

个人信息保护

谨慎发布个人隐私信息, 限制公开范围。了解并设置社交媒体的隐私权限和安全选项。

预防病毒传播

识别并避免传播虚假信息和链接, 谨慎打开来路不明的附件。定期更新手机和电脑的软件。

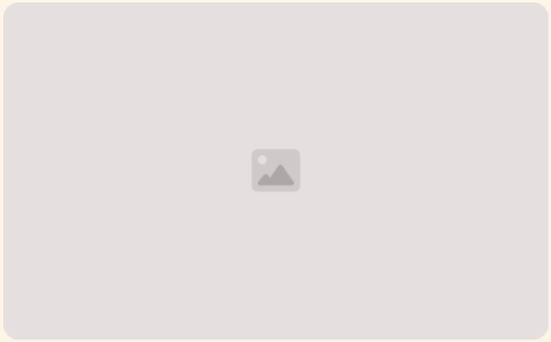
公共场所网络安全

注意公共 WIFI 安全

在公共场所使用免费 WIFI 时要格外小心,黑客可能会窃取您的账号密码和敏感信息,尽量避免在公共 WIFI 上进行重要交易。

保护个人隐私

在公共场所使用电子设备时,要注意遮挡屏幕,防止他人窥探敏感信息。谨慎处理涉及个人隐私的内容。



注意公共监控

公共场所可能设有监控摄像头,请注意自己的行为举止,保护好个人隐私和安全。如有疑虑,可向管理人员咨询。

移动设备安全

1 设备加密

确保移动设备使用强加密技术,如指纹或人脸识别,保护数据免遭未授权访问。

2 APP审慎选择

仅从可靠的应用商店下载应用程序,并仔细检查应用程序权限,避免隐私信息泄露。

3 远程定位与清除

启用远程定位和设备清除功能,一旦设备丢失可远程锁定或清除数据以防止信息泄露。

4 公共WiFi谨慎

避免在公共WiFi环境下进行敏感操作,如登录银行账户,以免遭受窃取或中间人攻击。

远程办公安全

网络连接安全

确保远程工作时使用安全的网络连接,如虚拟专用网络(VPN)或公司提供的专用网络。避免使用公共WiFi或不受信任的互联网连接。

设备保护

确保远程设备如笔记本电脑、手机等已安装最新的安全补丁和防病毒软件。启用加密和屏幕锁定功能,防止他人未经授权访问。

数据安全

远程工作时,谨慎处理机密文件和敏感数据。使用公司提供的安全云存储或协作工具,避免在个人设备上存储重要数据。

网络隐私

保护个人隐私和公司信息,避免在公共场合讨论工作内容。注意网络会议的信息安全,不要泄露敏感信息。