信息技术发展与网络安全防范措施

朱雁平
中电信量子信息科技集团有限公司　安徽　合肥　233000

摘　要：信息技术经历了从语言文字、印刷术、电子通信到计算机网络及人工智能的飞跃发展，极大促进了社会进步。然而，随着信息技术的广泛应用，网络安全面临严峻挑战，包括技术创新带来的新威胁、攻击手段多样化与复杂化，以及用户安全意识不足。为应对这些挑战，需加强密码管理、个人信息保护、安装更新安全软件、实施网络访问控制、确保数据备份与恢复，并培养广泛的网络安全意识。通过这些综合措施，构建坚实的网络安全防线，保障信息技术的健康发展和社会安全稳定。

关键词：信息技术发展；网络安全；防范措施

引言：随着信息技术的迅猛发展，人类社会迎来了前所未有的变革与便利。从语言文字的萌芽到互联网的普及，再到人工智能的兴起，信息技术的每一次飞跃都深刻影响着人们的生活方式和工作模式。然而，技术进步的同时，网络安全问题也日益凸显，成为制约信息技术健康发展的关键因素。本文旨在探讨信息技术的发展历程及其带来的网络安全挑战，并提出相应的防范措施，以期为保障信息技术安全、促进社会稳定发展提供参考。

1 信息技术发展概述

1.1 信息技术的发展阶段

（1）语言与文字阶段：作为信息传递的起点，语言与文字的出现标志着人类进入了文明社会。语言使得人们能够即时交流思想、情感和经验，而文字的出现则使得这些宝贵的信息能够跨越时间的长河被记录下来，为后世所学习和传承。这一阶段的成就，奠定了后续信息技术发展的基础。（2）印刷术阶段：如果说语言与文字是知识传播的种子，那么印刷术就是使其生根发芽的春雨。印刷术的发明极大地降低了书籍制作的成本，加速了知识的复制和传播速度，使得知识不再局限于少数人的掌握之中，而是能够普及到更广泛的民众之中。这一阶段的革命性变化，推动了人类文明的飞速发展。（3）电子通信阶段：随着电力的广泛应用和电磁理论的建立，电子通信技术逐渐兴起。电报、电话等电子通信设备的出现，实现了信息的远程即时传输，打破了地理和时间的限制。这一阶段的飞跃，使得信息传递的速度和效率得到了极大的提升。（4）计算机网络阶段：20世纪末至21世纪初，随着计算机技术和通信技术的融合，计算机网络技术得到了迅猛发展。互联网的诞生和普及，将全球各地的人们紧密地联系在一起，形成了一个庞大的数字世界。在这个世界中，信息的传递和共享变得更加便捷和高效，为人们的生产生活带来了极大的便利。（5）人工智能时代：当前，我们正处于人工智能时代的初期。人工智能技术的快速发展，使得机器能够模拟人类的智能行为，完成更加复杂和高级的任务。同时，多媒体技术的广泛应用也为信息的呈现和传播提供了更加丰富多样的形式。未来，随着人工智能技术的不断成熟和应用场景的不断拓展，我们有望迎来一个更加智能化和多媒体化的社会。

1.2 当前信息技术的主要特点

（1）高速发展与广泛应用：当前的信息技术正处于高速发展的阶段，新技术、新产品层出不穷。同时，这些技术也已经被广泛应用于社会各个领域，从教育、医疗到金融、交通等，无一不体现着信息技术的力量。（2）数据爆炸与信息共享：随着互联网的普及和物联网等新兴技术的发展，数据量呈现出爆炸性增长的态势。同时，信息共享的便捷性和高效性也得到了极大的提升。人们可以轻松地获取各种信息资源，进行跨地域、跨领域的合作与交流。（3）智能化与自动化趋势：人工智能技术的快速发展使得智能化和自动化成为当前信息技术发展的重要趋势。通过引入人工智能技术，可以实现各种复杂任务的自动化处理和分析决策，提高工作效率和准确性。（4）新兴技术的不断涌现：除了人工智能技术外，物联网、云计算、区块链等新兴技术也在不断发展壮大。这些新技术将为信息技术的发展注入新的活力和动力，推动社会各个领域的进一步变革与发展[1]。

2 网络安全面临的挑战

2.1 技术创新带来的新挑战

技术创新是推动社会进步的重要力量，但同时也带来了新的安全挑战。物联网设备的广泛应用，虽然极大

地方便了生活和工作，但由于设备种类繁多、安全标准不一，导致安全漏洞频发。黑客可以通过这些漏洞入侵设备，窃取敏感信息或进行恶意控制，对个人隐私和公共安全构成严重威胁。此外，云计算作为数据存储和处理的核心平台，其数据安全与隐私保护问题同样不容忽视。如何确保云端数据不被非法访问、篡改或泄露，是云计算服务商和用户共同面临的挑战。人工智能技术的快速发展，在提升安全防护能力的同时，也为黑客提供了更强大的攻击工具。AI技术能够自动化地分析网络流量、识别安全威胁，但同时也可能被用于构建更加智能和隐蔽的攻击手段。因此，人工智能技术在攻防两端的双重作用，使得网络安全防护工作更加复杂和艰巨。

2.2 网络攻击手段的多样化与复杂化

网络攻击手段的不断演变和复杂化，是当前网络安全面临的另一大挑战。黑客攻击与网络钓鱼等传统手段依然猖獗，且手法不断翻新，难以防范。同时，高级持续性威胁（APT）等新型攻击方式的出现，更是让企业和组织防不胜防。APT攻击通常具有高度的隐蔽性和长期性，能够绕过传统的安全防护措施，对特定目标进行深度渗透和破坏。此外，勒索软件和数据泄露等攻击手段也频繁发生，给企业和个人带来了巨大的经济损失和声誉损害。基于AI的网络攻击更是让防护难度大增，黑客可以利用AI技术自动化地寻找系统漏洞、制定攻击策略，使得网络安全防护工作面临前所未有的挑战。

2.3 用户安全意识与行为的不足

用户作为网络安全的最终防线，其安全意识与行为的不足也是导致网络安全问题频发的重要原因之一。许多用户在使用网络时缺乏足够的安全意识，常常使用弱密码、密码重复使用等行为增加了被破解的风险。同时，在社交网络中随意分享个人信息也容易导致隐私泄露。此外，许多用户还常常忽视安全提示和警告信息，使得原本可以预防的安全事件最终发生。因此，提升用户的安全意识和行为是加强网络安全防护工作的重要环节。

3 网络安全防范措施

3.1 密码管理

（1）使用强密码并定期更换：强密码应包含大小写字母、数字和特殊字符的混合，长度至少为8位或以上，避免使用容易猜测的词汇、生日、电话号码等个人信息作为密码。同时，应定期更换密码，建议至少每三个月更换一次，特别是在密码可能已泄露的情况下。（2）避免在多个账户上使用相同密码：许多人在不同平台和服务上使用相同的密码，这种做法一旦其中一个账户密码被破解，其他账户也将面临风险。因此，每个账户都应使用唯一的密码，并通过密码管理工具来管理和记忆[2]。（3）启用双重认证或多因素认证：双重认证或多因素认证为账户安全提供了额外的保障。除了密码外，用户还需要提供其他形式的身份验证信息，如手机验证码、指纹识别或动态令牌等。这样即使密码被窃取，未经授权的访问也能被有效阻止。

3.2 个人信息保护

（1）避免在公共网络上进行敏感操作：公共Wi-Fi网络往往安全性较低，容易受到黑客攻击和监听。因此，在进行网银交易、查看邮件或登录敏感账户时，应尽量避免使用公共网络。如果必须使用，可以考虑使用VPN加密网络连接。（2）警惕社交工程攻击：社交工程攻击是一种利用人的心理弱点来诱骗用户泄露敏感信息的攻击方式。用户应保持警惕，不轻易点击来源不明的链接或下载附件，特别是那些要求提供个人信息或执行敏感操作的链接。同时，要警惕来自陌生人的电话、短信或邮件，避免泄露个人信息。（3）谨慎在社交媒体上发布个人信息：社交媒体已成为人们分享生活点滴的重要平台，但同时也为黑客提供了收集个人信息的渠道。用户应谨慎在社交媒体上发布个人信息，特别是家庭住址、电话号码、生日等敏感信息。同时，要定期检查和清理社交媒体上的隐私设置，确保个人信息的安全。

3.3 安全软件与更新

（1）安装并定期更新杀毒软件和防火墙：杀毒软件和防火墙是计算机安全的重要组成部分，它们能够检测和阻止恶意软件的入侵。因此，用户应安装可靠的杀毒软件和防火墙，并定期更新以获取最新的病毒定义和防护规则。（2）及时更新操作系统和软件以修复安全漏洞：操作系统和软件中的安全漏洞是黑客攻击的常见入口。因此，用户应及时关注并安装官方发布的更新补丁，以修复已知的安全漏洞。这不仅可以减少潜在的安全风险，还可以提高系统的稳定性和性能[3]。（3）使用安全的浏览器并定期清理插件与缓存：浏览器是用户访问网络的主要工具，其安全性直接影响用户的上网体验和数据安全。因此，用户应选择经过认证的安全浏览器，并定期清理浏览器插件、缓存和cookies等敏感信息，以防止被恶意利用。

3.4 网络访问控制

（1）使用VPN加密网络连接：VPN（虚拟私人网络）通过加密技术为用户的网络连接提供了一层额外的保护。在使用公共Wi-Fi或其他不安全的网络环境时，VPN能够确保用户的数据传输过程是加密的，有效防止黑客监听、窃取或篡改数据。用户应确保选择可信赖的

VPN服务提供商，并正确配置VPN连接，以保障网络访问的安全性。（2）禁用不必要的网络端口和服务：许多计算机和网络设备默认开启了多个网络端口和服务，这些端口和服务往往是黑客攻击的目标。通过禁用不必要的网络端口和服务，可以减少潜在的攻击面，降低被黑客利用的风险。用户应定期检查并关闭不必要的服务，如文件共享、远程桌面等，除非确实需要并且已经采取了适当的安全措施。（3）部署防火墙和入侵检测系统（IDS/IPS）：防火墙是网络安全的第一道防线，能够监控和控制进出网络的数据包，阻止未经授权的访问和恶意流量。入侵检测系统（IDS/IPS）则能够实时监测网络流量中的异常行为，发现潜在的安全威胁并发出警报或自动采取措施进行防御。企业应部署强大的防火墙和入侵检测系统，确保网络免受外部攻击和内部威胁[4]。

3.5 数据备份与恢复

（1）定期备份重要数据到云端或外部硬盘：定期备份数据是防止数据丢失或损坏的关键步骤。企业应制定详细的数据备份计划，将重要数据定期备份到云端或外部硬盘等安全存储介质上。同时，备份数据应存放在与主数据中心地理位置分开的地点，以防止自然灾害等突发事件造成的数据丢失。（2）选择可靠的数据恢复服务并制定恢复计划：在数据丢失或损坏的情况下，能够快速恢复数据至关重要。因此，企业应选择可靠的数据恢复服务提供商，并与之建立合作关系。同时，企业应制定详细的数据恢复计划，明确数据恢复的目标、流程和责任人，以便在发生紧急情况时能够迅速响应并恢复数据。（3）了解备份策略的细节以便快速恢复数据：备份策略的制定需要考虑多种因素，包括备份数据的类型、频率、存储位置以及恢复时间等。了解这些细节对于在需要时快速恢复数据至关重要。企业应定期对备份策略进行审查和更新，确保其适应当前的业务需求和安全威胁。同时，员工应接受培训以了解备份策略的具体内容，以便在需要时能够迅速执行恢复操作。

3.6 培养网络安全意识

（1）提高员工对网络安全的认知与培训：企业应定期举办网络安全培训活动，提高员工对网络威胁的认识和防范能力。培训内容应涵盖最新的网络攻击手段、防范措施、安全政策和规范等方面。通过实际案例分析和模拟演练等方式，帮助员工掌握应对网络安全威胁的技能和知识。（2）建立严格的网络安全政策与规范：企业应制定明确的网络安全政策和规范，明确员工在网络使用过程中的行为准则和责任义务。这些政策和规范应涵盖密码管理、个人信息保护、安全软件安装与更新等多个方面。同时，建立相应的奖惩机制以督促员工遵守网络安全政策和规范。（3）定期演练应急响应流程以应对突发事件：通过模拟真实的网络安全事件进行应急响应演练，可以检验企业应对突发事件的能力和水平，并发现潜在的问题和不足之处。在演练过程中，应重点关注应急响应流程的顺畅性、团队协作的效率以及信息通报的及时性等方面。通过不断的演练和改进，提高企业应对网络安全威胁的应急响应能力。

结束语

综上所述，信息技术的发展为人类社会带来了前所未有的变革与机遇，但同时也伴随着严峻的网络安全挑战。面对这些挑战，我们需要持续加强技术创新，完善网络安全体系，提升全民网络安全意识。只有这样，我们才能在享受信息技术带来的便利的同时，确保信息安全与隐私保护，推动信息技术向更加健康、安全、可持续的方向发展。未来，让我们携手共进，共同构建一个更加安全、可靠的信息技术环境。

参考文献

[1]朱超杰.计算机网络安全漏洞及防范措施[J].数码设计,2019,(1):362-363.

[2]王伟丽.计算机网络信息安全及其防范对策的探讨[J].数码设计,2019,(1):18-19.

[3]曲峰.计算机网络信息技术安全及防范对策分析[J].数字技术与应用,2019,37(12):197-198.

[4]彭世春.计算机信息化管理的发展与网络安全的有效防范措施探索[J].现代销(经营版2020(07):102-103.