通信计算机信息安全问题及解决对策

张　伟
天津赢大科技有限公司　天津　300384

摘　要：随着社会经济与科学技术的发展，我国通信领域取得了显著进步，通信计算机已逐渐融入人们的日常生活，为人们带来了诸多便利。但在享受这些便利的同时，我们也必须警惕其中潜在的风险，这些风险在一定程度上制约了通信计算机的持续发展。目前，计算机使用过程中的网络安全问题亟待解决，这主要是由于相关保护机制不完善。因此，我们必须不断加强用户的信息安全意识，从加强信息安全防护做起。同时通过技术升级和改进来提升计算机使用过程中的安全性能。

关键词：通信；计算机信息；安全问题；解决对策

引言：信息化时代，计算机技术在推动社会发展的同时，也带来了严重的网络安全问题。本文阐述了通信计算机信息安全的重要性及其所面临的数据泄露、网络攻击、恶意软件等安全问题。并提出了一系列针对性的解决对策，包括加强防病毒措施、强化密码保护、完善数据备份与恢复机制、提升网络安全防护、实施安全审计和监控以及加强用户教育与培训。这些对策共同构成了一个全面的信息安全保护体系，旨在确保通信计算机信息的安全性和完整性。

1 通信计算机信息安全的重要性

通信计算机信息安全的重要性无可置疑，它深刻影响着我们的生活、工作和国家安全。在现代社会，通信计算机技术已渗透到我们生活的方方面面，无论是日常交流、购物消费，还是企业运营、政府管理，都离不开它。然而，随着技术的广泛应用，信息安全问题也日益凸显。通信计算机信息安全直接关系到个人隐私的保护。我们的身份信息、银行账户、社交动态等个人数据，都存储在各类通信设备和计算机系统中。如果这些信息被非法获取或滥用，我们的隐私权将受到严重侵犯，甚至可能因此遭受经济损失和精神困扰[1]。对于企业来说，信息安全更是生死攸关。企业的核心数据、商业机密和客户资料等，都是其赖以生存和发展的宝贵资产。一旦这些信息被泄露或被竞争对手利用，企业将面临巨大的商业风险，甚至可能因此遭受灭顶之灾。此外，通信计算机信息安全还关乎国家的安全和稳定。政府机构的重要文件、军事机密以及关键基础设施的控制指令等，都通过通信计算机系统进行传输和存储。如果这些信息被敌对势力窃取或破坏，将对国家的政治、经济和社会安全造成难以估量的影响。

2 通信计算机信息的安全问题

2.1 数据泄露

数据泄露是当今通信计算机信息安全领域面临的一个重大问题。在大数据和云计算技术的推动下，我们的个人信息、财务信息以及企业的商业数据等敏感信息都被高度集中地存储在互联网的数据中心。这种集中存储虽然带来了数据处理的便利，但同时也增加了数据泄露的风险。一旦这些信息被未经授权地访问或泄露，后果可能是灾难性的。个人隐私的曝光可能导致身份盗窃、诈骗等犯罪行为的发生。对于企业而言，商业机密的泄露可能会损害其竞争优势，甚至导致重大的经济损失。更为严重的是，当泄露的数据涉及国家安全时，其后果更是不堪设想。近年来，数据泄露事件层出不穷，且呈上升趋势。这既反映了信息安全挑战的严峻性，也凸显了当前安全防护措施的不足。

2.2 网络攻击

在通信计算机信息领域，网络攻击日渐成为严重的安全问题，其深层原因主要有以下几点。（1）网络技术的迅猛发展使得通信系统和计算机网络日益复杂，为攻击者提供了更多的入侵机会；随着云计算、大数据、物联网等技术的普及，数据交换和信息共享变得日益频繁，这也增加了信息泄露和被攻击的风险。（2）水利水电工程等关键基础设施的信息化、智能化水平不断提高，越来越多的控制系统和设备连接到网络上，这使得这些系统更容易受到网络攻击。（3）网络安全意识的缺失也是导致网络攻击频发的一个重要原因。许多组织和个人对网络安全的重要性认识不足，缺乏有效的安全防护措施，容易被攻击者利用漏洞进行入侵。（4）网络犯罪的动机也是多种多样的，包括经济利益、破坏目的、政治或恐怖主义等；这些动机驱使着攻击者不断寻找新

的攻击目标和手段，对通信系统和计算机网络构成持续威胁。

2.3 恶意软件

恶意软件，这一通信计算机信息安全的大敌，常常在用户毫无察觉的情况下侵入系统。这些软件，如病毒、木马、蠕虫等，都极具隐蔽性和破坏性，当用户在浏览网页或下载软件时，稍有不慎就可能为恶意软件提供可乘之机。病毒是恶意软件中最常见的一种，它们会复制自身并感染计算机中的其他文件，从而破坏数据、干扰系统运行，甚至导致系统崩溃。病毒的传播速度快，破坏力大，是信息安全领域的一大难题，木马则是另一种常见的恶意软件；与病毒不同，木马通常伪装成合法软件，诱骗用户主动下载并执行[2]。一旦用户中招，木马就会窃取个人信息、破坏系统文件，甚至为黑客打开远程控制的“后门”，蠕虫也是一种不容忽视的恶意软件。它们通过网络进行自我复制和传播，大量消耗网络资源，很可能导致网络拥堵甚至崩溃，蠕虫的传播速度和破坏力都非常惊人，一旦爆发，往往会给网络带来灾难性的影响。

3 通信计算机信息的解决对策

3.1 加强防病毒措施

随着数字化时代的快速发展，计算机病毒成为了网络安全的一大隐患，这些恶意的计算机程序不仅可能损坏数据，还可能窃取个人信息，甚至使整个系统陷入瘫痪。因此，加强防病毒措施成为了保障信息安全的首要任务，选择一款可信赖的防病毒软件是至关重要的，这样的软件应具备实时监控功能，能够在病毒试图侵入系统的第一时间进行检测和隔离。同样，软件的病毒库需要不断更新，以便及时识别和防御新出现的病毒变种，用户应养成定期更新病毒库的习惯，确保防病毒软件的防护能力始终与时俱进。除了依赖防病毒软件，用户自身的警惕性也至关重要，在日常使用计算机和网络时，应避免打开来自不明来源的邮件、链接或下载附件。这些不明链接或附件往往隐藏着病毒，一旦点击或下载，就可能导致系统被病毒感染；因此，用户需要保持高度的警觉性，对任何可疑的信息都要进行谨慎判断。此外，定期对计算机系统进行全面扫描也是必不可少的，这种扫描可以深入检测系统的每一个角落，发现并清除那些可能已经潜入系统但尚未被激活的病毒。

3.2 强化密码保护

密码，作为我们数字生活的第一道防线，其重要性不言而喻；然而，随着网络技术的发展，简单的密码已经无法满足当今的安全需求。为了确保个人信息和资产的安全，我们必须强化密码保护，一个强大的密码是防止黑客入侵的关键；那么，什么样的密码才算强大呢？它应该是一个包含大小写字母、数字和特殊符号的复杂组合。这种密码在面对各种破解手段时都能展现出强大的抵抗力，但记忆这样的密码对很多人来说是个挑战，这时，密码管理工具就派上了用场。密码管理工具如同我们的私人助理，帮助我们安全地存储、整理和记忆各种复杂密码，使用这些工具，我们无需再为忘记密码而烦恼，也能避免在不同账户间混淆密码。但仅仅依赖密码还不足以保护我们的高度敏感账户，对于这些账户，双重认证提供了额外的安全保障。双重认证意味着，在输入密码后，我们还需要提供第二种验证方式。这就像是给我们的数字生活加上了双重锁，即使密码被破解，攻击者也难以通过第二重验证，在这个数字化快速发展的时代，强化密码保护已经成为我们每个人的必修课。通过创建复杂密码、利用密码管理工具以及启用双重认证，我们可以更好地守护自己的数字身份和信息安全。

3.3 完善数据备份与恢复机制

在高度数字化的当今时代，数据已经成为我们生活和工作中不可或缺的一部分。数据的丢失或损坏可能带来深远的影响，从个人层面的记忆丧失到企业层面的业务中断，都强调了数据完整性和可用性的重要性。因此，一个健全的数据备份与恢复机制对于保护我们的数字资产至关重要。数据备份是这一机制的核心组成部分。用户应当定期，根据数据的更新频率和重要性，将所有关键数据进行备份。备份的方式可以多样化，既可以使用物理的外部存储设备，如USB闪存盘、移动硬盘，也可以选择云存储服务[3]。特别是对于那些经常变动的数据，如工作文档、照片或视频等，建议设置更加频繁的备份周期，以减少数据丢失的风险。然而，仅仅进行数据备份并不足够。一个完备的数据恢复计划同样重要，它确保了在数据意外丢失或损坏时能够快速有效地进行恢复。这样的计划应包括清晰的步骤和指导，说明在发生数据危机时应如何操作，哪些数据是业务连续性的关键，以及如何在最短时间内重新获取或恢复这些数据。此外，对备份数据的验证也是不可或缺的一环。用户需要定期检查备份文件的完整性和可读性，以确保在紧急情况下可以依赖这些备份。

3.4 提升网络安全防护

在数字时代，随着信息技术的迅猛发展，网络安全问题愈发凸显其重要性。为了保护通信计算机信息不受外部威胁和攻击，构建一个坚实的网络安全防护体系显得尤为重要。这一体系融合了先进的技术手段、严格的

管理策略以及规范的用户行为等多个层面。（1）网络防火墙作为网络安全的基础设施，起着至关重要的作用。它如同一个守门人，时刻监控着进出网络的流量。任何未经授权的访问或潜在的攻击行为，都难以逃脱防火墙的锐利目光。通过精心配置防火墙规则，我们可以限制对敏感资源的访问，从而大大降低数据泄露的风险。（2）定期更新操作系统和软件也是维护网络安全不可或缺的一环。这些更新往往包含了对已知安全漏洞的修复，及时应用这些最新的安全补丁，能够有效防止黑客利用这些漏洞进行攻击。因此，用户必须保持对系统和软件的持续关注，确保及时获取并应用最新的更新。（3）通过实施严格的网络访问权限管理，我们可以进一步提升网络安全。为不同用户或用户组分配明确的访问权限，能够确保敏感数据只被授权人员访问。

3.5 实施安全审计和监控

实施安全审计和实时监控是网络安全领域中至关重要的环节，安全审计就像是对系统的一次全面健康检查，它深入挖掘并评估网络架构的稳固性、系统配置的合理性、应用软件的可靠性以及数据加密标准是否严谨。在这个过程中，专业的安全团队会运用各种先进的技术手段和精密的工具，不放过每一个可能影响系统安全的细节。除了技术层面的审查，管理和操作层面也是安全审计的重点。用户权限的分配是否合理、安全策略是否得到严格执行等都在审计的范畴之内。这种全方位的审查，确保了系统的安全性得到全面的提升。审计中发现的每一个问题，都会得到详细的记录和分析，并配以切实可行的改善措施和建议。这些建议并非空谈，而是会迅速转化为实际行动，加强系统的安全防护。与此同时，实时监控则是保障系统安全的另一道坚实屏障。它要求安全团队利用高效的安全信息和事件管理系统，对网络流量、系统日志、用户行为等进行24小时不间断的监测。这种监测就像是一双警惕的眼睛，时刻注视着网络上的一举一动。一旦出现任何异常，如网络流量的异常波动、不合常规的访问行为或是潜在的恶意攻击，都会立即触发警报系统，确保安全团队能够在第一时间作出反应，有效遏制安全事件的发生。

3.6 加强用户教育与培训

在保护通信计算机信息安全的众多策略中，加强用户教育与培训占据着举足轻重的地位。人为因素往往是信息安全链条中最薄弱的一环，而提升用户的信息安全意识则能有效减少因操作不当或缺乏警觉而引起的安全问题。用户教育与培训的首要目标是帮助用户识别并防范网络钓鱼、诈骗等网络安全风险[4]。这些培训课程中，用户将学习如何辨别可疑的电子邮件、链接或网站，从而避免陷入网络犯罪的陷阱。例如，通过案例分析，用户可以了解到常见的网络诈骗手法，并学会在面对类似情况时保持警惕，不轻易泄露个人信息，不随意点击来源不明的链接。除了提高警觉性，用户还需要掌握正确使用安全工具和软件的方法。培训课程会指导用户如何配置和使用防病毒软件、防火墙等安全工具，确保这些工具能够发挥最大的防护作用。此外，用户还会学习到如何定期更新操作系统和软件，以修补已知的安全漏洞，防止恶意软件的入侵。为了防止数据丢失，用户还需要养成良好的数据备份习惯。培训课程会强调定期备份重要数据的重要性，并提供数据备份和恢复的实操指导。

结语：综上所述，通信计算机信息安全至关重要，它涉及个人隐私、企业资产和国家安全的保护。为确保信息安全，需采取多种措施，如加强防病毒、密码保护、数据备份恢复等，还要关注网络安全、安全审计及用户教育。这些努力共同构筑了信息安全的坚固防线。在数字化时代，我们每个人都应提高信息安全意识，通过实践不断完善防御措施。只有这样，我们的信息才能更安全、更可靠，个人隐私、企业资产及国家安全才能得到切实保障。

参考文献

[1]何应发.通信计算机信息安全问题及解决对策分析[J].信息记录材料,2020,21(01):48-49.

[2]杨旭.通信计算机信息安全相关问题及措施[J].中国新通信,2019,21(11):166.

[3]王林军,魏敏敏.新形势下计算机通信网络安全防护策略[J].时代经贸,2019(36):95-96.

[4]杨旭.通信计算机信息安全相关问题及措施[J].中国新通信,2019,21(11):166.