计算机应用中的网络安全防范对策

黄春梅

怀化市卫生健康事务中心，湖南 怀化 418000

摘要：在现代化背景下，互联网与计算机全面普及，促使人们生活以及工作模式发生了翻天覆地变化。而计算机在应用中将会储存大量信息，一旦信息被泄露，将会造成严重的影响。因此计算机应用中的网络安全防范工作至关重要，目前已经引起了人们的广泛重视。下面将从计算机应用中网络安全存在的问题出发，在这一基础上探究有效的策略与手段，为计算机网络安全提供全面保障。

关键词：计算机应用；网络安全；安全防范

DOI：10.63887/fns.2025.1.4.6

在科技迅猛发展背景下，人们生活水平显著提升，计算机成为了生活以及人与人之间突破时空界限的重要工具，促使整个工作以及交流效率显著提升。在虚拟的网络空间内，计算机应用直接将个人信息都储存了下来，呈现出开放性、无限性以及共享性，从而引发隐私泄露以及信息盗窃等问题。因此网络安全防范对策至关重要，为人们提供良好的应用建议。

1 计算机应用中网络安全问题以及隐患分析

根据目前计算机应用现状分析，网络安全问题引起了人们的广泛重视。如果网络安全得不到保障，将会直接影响到计算机的运用，并且埋下一系列的安全隐患，比如出现数据信息丢失或者损害的情况。通常情况下，计算机应用中常见的网络安全问题主要包括了以下几个方面：

1.1 网络安全管理制度有待完善

当前许多企业在计算机应用中对网络安全管理方面缺少明确规定，使不法分子钻了孔子。其中包括了网络钓鱼或者黑客。网络钓鱼主要是那些不法分子假冒国家机构或者银行向用户们发送一些诈骗短信或者邮件，在用户点进入后，不法分子将会趁机而入，获取用户的各种信息，从而可以根据实际情况制定对应的诈骗方案，使更多人上当受骗。由此可以看出网络中蕴藏着许多风险，并且具有不可察觉的特点，一旦自己的信息被盗取后，可能会面临严重的经济损失[1]。黑客则是威胁网络安全的常见方式，相关人员可以直接通过技术对用户的电脑进行攻击性的破坏，破坏用户数据，使用户无法正常使用计算机系统[1]。又或者通过非破坏性的攻击，在用户并不知道的情况下，实现信息的窃取。

1.2 软硬件管理有待提升

计算机主要是由硬件与软件两个方面组成的，其中硬件对网络安全影响比较大。常见的计算机硬件包括了路由器、服务器以及交换机等，而这也是进行信息流入以及输出的重要组成。在计算机硬件使用过程中，运行的效果可能达不到要求，无法实现有效的运行。一旦出现这些问题，计算机运行的速度将会受到严重的影响，导致后续的使用受到限制，出现不必要的损伤。计算机软件作为重要组成，在计算机应用与运行中起到了至关重要的作用。如果软件系统存在问题或者被人破坏，整个计算机将会发生故障[2]。与硬件问题相比，软件具有不可控制性，每一款软件可能都会携带一些安全风险。尤其是在计算机技术发展与更新的过中，软件系统在使用中将会出现许多漏洞或者问题，如果处理不及时，无法弥补目前软件系统存在的问题，导致病毒、木马程序进入到计算机内，从而信息安全得不到保障。并且，人们在运用计算机的过程中存在差异性，资源调配或者个性特征呈现出多元化特点，在信息资源管理中出现各种问题，一旦被攻击，数据将会丢失或者被篡改，造成不可弥补的损失。

1.3 病毒抵抗力较差

在一般情况下，病毒都是在文件复制、传送时侵入的。并且病毒能够针对计算机网络程序进行编程，从而破坏整个计算机的功能，导致系统瘫痪，由此可以看出病毒防范的难度比较大[2]。并且病毒具有复制性、感染性强的特点，尽管在目前科技与网络病毒案发展背景下出现了许多防病毒措施，但是依然无法保证计算机内部信息的安全。病毒将会在没有防备的情况下潜伏到计算机内，用户无法发现，从而系统的安全性得不到保障。

1.4 信息加密技术有待完善

影响网络安全性的主要因素为网络环境，缺少信息加密技术，导致计算机处于劣质的网络环境下，整个计算机网络的稳定性比较差，并且还会影响计算机的应用。通过目前网络体系分析，数据作为计算机应用关键，如果无法保护好核心数据，出现数据泄露，将会发生一系列的连锁反应，导致计算机的应用受到严重影响，无法正常的使用。

2 计算机应用中网络安全防范的有效策略

网络安全问题将会直接关系到计算机应用的效果，为了发挥出计算机的优势，应当探索科学有效的防范策略，降低安全事故发生的概率。因此在计算机应用中需要做好以下几个方面工作：

2.1 完善计算机网络安全管理制度

科学完善的计算机网络安全管理制度可以约束用户的使用，促使计算机应用安全性显著提升，实现持续稳定的运行。因此相关单位在应用与配备计算机的过程中，需要全面细致化管理。首先，应当做好内部使用人员网络安全防范工作、宣传与教育工作，使所有使用人员树立起良好的安全意识[3]。目前每个人都有属于自己的电子邮件或者网络银行账号，黑客可以灵活运用计算机用户浏览痕迹，或者通过一系列计算措施与手段，获取用户的账号信息与密码，转移用户的信息以及财产，使用户承受较大的财产损失。因此，用户在运用计算机网络的过程中，不能使用重复性的密码或者账号，也不能全部设置数字或者字母，可以采取数字、字母与标点符号以及大小写联合使用的方式，并且定期更换自己的密码，促使计算机网络安全使用。同时还应当注意不能随意打开来历不明的邮件或者附件；不能使用办公邮件注册第三方网络或者论坛，以免信息或者密码被泄露出去[4]。其次，相关部门还应当针对计算机使用制定一系列的规范化制度与体系，实现对工作人员的约束，有效降低事故发生的概率。最后，对于计算机操作与使用，应当根据实际的问题制定应急方案，在发生安全事故后，管理人员可以根据计算机的使用情况进行处理，降低网络安全造成的影响与威胁，促使计算机设备稳定的运行。

2.2 加强硬件与软件管理

在计算机应用中，为了促使网络安全防范工作取得良好成果，需要从硬件与软件两个方面出发做好管理，其作为计算机的两大系统，将会直接影响网络的安全稳定运行。在硬件管理中，需要做好硬件设备选型与采购，将计算机的安全性能放在第一位。比如尽可能选择一些具有硬件加密功能的硬盘，并且将其中储存的数据进行加密处理，以免硬盘丢失或者被盗数据被泄露出去[5]。目前许多企业硬盘都支持 AES 加密，保证自己的敏感以及隐私数据被保护起来。还需要将服务器放置在专门的机房中，机房应具备防火、防水、防潮、防雷击等安全设施，并安装门禁系统和监控摄像头，限制人员进出，确保硬件设备的安全。同时相关工作人员需要定期对计算机的硬件设置进行检查与维护，做好基础的防火、防尘以及防水工作。

对计算机软件工作，则需要在管理的过程中进行全方位的监督与把控，及时安装这些补丁是保障操作系统安全的重要措施。例如，微软会定期为 Windows 操作系统发布安全更新，用户应设置自动更新或定期手动检查并安装补丁，以防止黑客利用系统漏洞进行攻击。如果在发现了非法访问的情况后，应当采取有效的手段进行过滤与屏蔽，并且设置计算机安全涉密工作，宝着呢个密码设定具有一定的复杂性，明确访问权限，促使网络安全显著提升。

2.3 构建防火墙

目前计算机未来防范病毒或者黑客的入侵，基本上都会通过各种技术以及软件来控制计算机与网络，直接将一些垃圾邮件或者病毒阻隔在计算机外，为计

算机的使用以及各个软件的安全提供全面保障。在防火墙的作用下，可以有效避免用户在浏览网络或者下载文件的过程中代入病毒，保证计算机内信息的安全性。在这一基础上，防火墙还能够检验多个网络传输数据，实现对网络运行情况的全面监督与把控[6]。以金融行业为例，许多黑客都会选择这一领域的计算机为对象，主要是因为使用人员的安全防范意识比较低，为黑客提供了机会。因此为了保证金融领域内计算机系统的安全，在强化使用人员安全意识的同时，还应当设置独立的防火墙，以免黑客侵入。

在现代化背景下，衍生出许多计算机网络防火墙的类型，而每一种类型所对应的防范方向存在一定的区别。目前市面上应用比较广泛的包括了检测类防火墙、地址转换类防火墙、代理防火墙等。虽然有所不同，但是运行的原理一致，都是通过对网络中分包传输技术的运用以及数据包数据的精准判断，更好的了解信息安全。在计算机运行的过程中，各种人员可以时刻监督与把控，在发现潜在的危险时可以通过对防火墙阻隔危险数据包的运用，为计算机安全提供保障。除此之外，还可以在计算机内构建地址转换防火墙，将自己的 IP 转换成另外一种 IP，从而在浏览网页或者文件时可以隐藏自己的真实 IP，避免了被黑客侵袭，

2.4 应用信息加密技术

在计算机应用中，需要认识到信息加密技术的重要性，为数据信息安全提供全面保障。在进行计算机网络处理过程中，需要针对数据库特性，对各项信息进行加密处理，有效降低数据库内数据被盗用的情况。相关单位可以灵活运用前置代理、加密网关技术、也能够用层改造加密技术以及文件及加解密技术等等，满足目前数据安全保护工作的需求。在一般情况下，只需要采用一种加密技术，特殊情况下还可以运用两种或者两种以上的技术，保证数据不会被病毒或者黑客所侵袭，为数据安全提供全面保障。目前比较常见的信息加密技术如表 1。

表 1 信息加密技术分类

信息加密技术分类	特点	优点	常见算法
对称加密技术	加密与解密使用相同的秘钥	可以快速完成大量数据加密处理	AES（高级加密标准）：国际上广泛使用的对称加密算法，支持 128、192、256 位密钥长度，安全性高。DES（数据加密标准）：较早的对称加密算法，密钥长度为 56 位，现已逐渐被 AES 取代。3DES（三重 DES）：对 DES 的改进，通过三次加密提高安全性
非对称加密技术	加密和解密所使用不同的密钥	管理起来更加简单，适合大部分网络环境	RSA：最常用的非对称加密算法，广泛应用于安全通信和数字签名。ECC（椭圆曲线加密）：安全性高，计算效率优于 RSA，适用于资源受限的环境。

3 结束语

根据文章叙述，在现代化背景下，计算机已经得到了广泛的运用。然而目前在实际应用中出现了许多网络安全问题，导致最终的工作以及生活受到严重影响。因此在未来应用中，需要完善计算机网络安全管理制度，加强硬件与软件管理，构建防火墙，应用信息加密技术，促使广大用户树立良好安全意识，保证网络信息安全性。

参考文献

[1]关安青.基于网络信息安全技术管理的计算机应用研究[J].软件,2025,46(02):13-15.

[2]邓喆.大数据支撑下计算机应用技术教学的分析与研究[J].学周刊,2025,(05):4-6.

[3]徐洪敏.基于网络信息安全技术管理的计算机应用研究[J].张江科技评论,2024,(09):135-137.

[4]姚锦江,罗军.计算机应用基础课程思政探讨——以互联网应用之网络安全为例[J].电脑知识与技术,2023,19(14):155-157+173.

[5]刘城.大数据时代背景下计算机网络安全防范应用与运行[J].无线互联科技,2023,20(08):166-168.

[6]汤荻.基于应用视角的计算机网络安全技术创新与应用[J].网络安全技术与应用,2023,(03):15-17.

作者简介：黄春梅，1978 年 1 月 16 日，女，汉，湖南怀化，本科，中级（疾病控制），研究方向或从事工作：卫生健康管理