ISSN:2661-3719(Print);2661-3727(Online)

浅析计算机网络安全技术的影响因素与防范措施

李久勇
山东黄河河务局黄河河口管理局　山东东营　257091

摘　要：随着科学技术的发展，计算机应用技术被广泛应用到各个领域，为生产经营及人们生活质量都带来了积极影响。但是网络安全问题却一直层出不穷，时常出现个人隐私泄露、大额财产被转移等严重损失，其中的原因引人深思，因此，当前计算机发展的最主要问题就是要切实提升网络安全技术，明确其主要的影响因素，并积极探寻有效的防护措施，保障计算机网络安全。
关键词：计算机；网络安全技术；影响因素；防范措施

Analysis of computer network security technology influencing factors and preventive measures

Jiuyong Li
Shandong Yellow River Administration Bureau, Yellow River Estuary Administration Bureau, Dongying City, Shandong Province, 257091

Abstract: With the development of science and technology, computer application technology is widely used in various fields for production and management and people's quality of life has brought a positive impact. But network security problems have been emerging in an endless stream, often appear personal privacy disclosure, large amounts of the property transferred and other serious losses, the reasons for which are thought-provoking. Therefore, the current computer development of the most important problem is to effectively improve the network security technology, clear its main influencing factors, and actively explore effective protective measures to protect the computer network security.
Key words: computer; network security technology; influencing factors; preventive measures

当代人们过于依赖信息网络，所有的重要信息都暴露在互联网上，然而当前网络安全难以维持的状况极大增加了个人隐私泄露的风险，为人们的信息安全带来隐患，如果不及时采取行之有效的措施，那么将会后患无穷，不仅会对经济造成损失，严重还会威胁到人身安危，因此要加强对计算机网络安全技术的研究，从根本上解决网络安全问题，维护用户的信息与人身安全[1]。网络安全技术的研究不是一蹴而就的，需要经过不断的分析和探索去实现能够解决当前网络问题的方法，及时查找到阻碍网络安全运营的影响因素，并加大研究投入，提出切实可行的防范措施，维护网络安全环境。

一、计算机网络安全技术的影响因素

1.1 用户的安全意识较为薄弱

影响计算机网络安全的主观因素就是用户的自身问题，在如今社会发展中，不论男女老少都在互联网的影响下开展娱乐、学习、工作，但是却并不关注网络安全问题，网络意识较为薄弱，不具备任何防范准备，尤其是一些幼龄儿童或者上了年纪的老人，更容易成为网络威胁的直接目标[2]。再加上当前越来越多的网络开发者，更重视网络运营效应，而忽略了安全方面的创设，投入的维护措施与管理实施的力度都与实际生活中网络的安全需求有较大的的差距。而且当前网民普遍认为网络危险存在一定的偶然性，并在上网时抱有侥幸心理，处理安全问题的态度不够积极，无法从根本上检测网络危险因素，没有具体的防护手段，应对方式更加原始，因此网络安全运行影响难以保障。

1.2 运行管理机制存在缺陷

在网络安全运行过程中，一方面网络信息安全管理工作人员不足，因为在互联网中交流与沟通的成本不高，不同的用户呈现方式为分布式而且网络服务器的配置也有所不同，再加上用户的需求也在随着科技的进步以及实践的推移而发生变化，因此相关的技术发展与运行管理的方式也存在一定程度的变化，因此在管理岗位的相关工作人员中，真正掌握网络安全管理技能方面的人才还是占少数，所以管理不到位[3]；另一方面，互联网安全防范体系还不够完善，当前互联网的发展具备综合性特征，这也直接导致互联网发展具有危险性，在目前网络使用中，很多用户急于操作，没有在充分了解软件的主要内容之后再去进行相关操作，最终用户隐私泄露，网络安全系统崩盘，为人们带来很多不必要的威胁。除

此之外，系统的落伍、电脑配置不够、内部网络出现问题等，这些因素都直接给危险分子可乘之机，因为在当前电脑中没有一套较为完善的运行管理机制，系统危险防范体系无法正常工作，对出现的漏洞不能做到及时的查漏补缺，导致网络运行难以维持在安全范围之内。

1.3 系统本身存在一定的问题

在计算机网络安全维护中，系统的自身存在问题是最容易使病毒入侵的，非常不利于计算机的正常运行。对于部分传播病毒的软硬盘和部分网站来说，一旦病毒入侵，就会搭建出快速传播的桥梁，具有非常大的破坏影响力，威胁整个计算机系统的安全，很容易导致整个硬件或软件系统出现崩溃，甚至会使系统瘫痪，无法运转[4]。

1.4 计算机网络监管力度不够

在计算机的正常运行中，需要有较为完备的监管机制实现高效的网络监管，且具有一定的法律限制。但是由于计算机相关的法治范围过大，监管执行难度加大，又因为网络是一个相对来说比较开放的虚拟世界，在网上冲浪的用户真实身份很容易被隐藏，就导致一些违法犯罪分子在网络上冒用身份信息实施诈骗，尽管如此，但是在网络上由于监管难度巨大，无法行使切实有效的监管机制，因此无法及时将罪犯绳之以法，尽管目前我国已经在严厉监管网络安全，坚决打击网络犯罪分子，维护网络正常安全运行，但是目前的法律体系却并没有实现较为完备的改善，网络监管力度还需加大发展，提升重视程度。

二、计算机网络安全技术的防范措施

2.1 有效培养计算机用户和管理人员的安全防范意识

一方面，要想切实维护网络安全，最直接的措施就是互联网使用用户能够提升自身的安全防范意识，增强网络安全常识。首先，可以通过社区宣传、学校宣传、单位宣传等社会宣传方式来提升用户的网络危险防范意识，将科学上网，维护自身信息安全的知识渗透到家家户户，包括尝试使用网络的老年人，或奶年龄尚小的孩童，都要具备危险意识[5]；其次，针对一些具有隐私性的信息，网络运行可以提醒用户设置安全密钥，通过密码或口令解锁隐私信息的访问权限，并合理对计算机应用数据进行规范操作，阻止一切没有访问权限的用户随意访问或盗取网络信息，有效提升网络安全；最后，用户要注意使用 WiFi 网络时，尽量避免在公共场合使用陌生网络，陌生网络很有可能是钓鱼网络，在连接成功之后成功盗取用户的所有隐私信息。因此用户要多加防范，从根本上杜绝网络安全威胁。

另一方面，计算机网络管理人员是直接接触网络安全威胁的群体，因此，网络安全维护企业要培养一支精英管理队伍，从而保障队伍内部网络管理人员具备较强的专业素养，对网络运行状况实行全面的监控。首先，网络维护方要对网络管理人员实行全面的技术培训，加强对相关人员的网络安全处理以及监督意识，增强管理能力，培养能够精确判断危险因素的能力，严格打击非法攻击的情况。其次，安全维护企业要能够切实培养管理人员创新管理模式，学习更加先进的管理技术，取得网络维护监管优势，促进当前网络实现安全信息化技术转型，不等网络威胁攻击而采用抵御模式，而是主动出击，预防威胁安全因素滋生，争取到网络维护的主动权；最后，在计算机网络信息优化进行中，最重要的一步就是要通过计算机中相关数据以及信息采集实现网络安全维护系统的创建和架构，不断分析和研究出更多的解决策略，切实维护网络信息安全，确保我国计算机安全网络系统得以高效发展。

2.2 加强网络监控评估、积极更新软件系统

一方面，采用更加先进的网络安全技术手段是切实提升网络安全管理的有效措施，在组建一支较为完备的管理人员队伍之后，还需要加强网络监控评估，培养技能优异的评估专员，树立更高水准的技术团队，注重系统维护与监控。在平时的工作中，注重维护网络安全设备，做好所有系统的检测工作，确保没有出现任何漏洞是病毒有机可乘，并使用最新技术软件探测技术对计算机的端口进行全面的检查，查看是否有异样，如果出现一些较小的问题，要及时使用病毒扫描软件进行全方位的病毒查杀，根除小问题的滋生，若检测评估人员发现较大的病毒问题后，要立即隔离网络端口，实行较强力度的技术干预，保障病毒被妥善解决。因此在网络安全监控过程中，一定要增强对网络设备的安全筛查，通过较为合理的方式加强网络防御能力，保护计算机网络信息数据安全，为用户带来更好的网络体验。

另一方面，用户及时进行软件系统的更新可以无形之中增强计算机系统的保护力度，不那么容易被网络不法分子盗取个人信息，而出现不必要的经济财产损失，使用户的上网安全得到一定程度的保障。这其中的原因主要是在更新计算机软件后，能够使其原本的抵御病毒的能力也随之增强，病毒在滋生的同时系统内部的防护也进一步加强，是病毒难以轻易介入，保护用户的数据安全。因此用户要多多进行软件更新，让计算机一直处在新的操作系统中，为网络信息安全盖上一层坚固的防护罩。

2.3 加强防病毒入侵技术

在整个计算机安全维护系统运行过程中，网络安全管理是重要的环节之一，如何能够保障运行网络又快又好发展是当前整个互联网应用推广所面临的最大的问题，要想解决当前的燃眉之急，保障网络环境安全运营，就需要加强计算机安全防护的技术创新，当前防止计算机遭遇网络威胁的主要防护方式包括：防火墙、网络监察、数据加密、病毒查杀、入侵检测五方面，这些是最被用户所接受且经常使用的安全防护技术，在此基础上，

技术团队还要加强创新，研究出更万无一失的防护措施，帮助人们解决当前网络安全漏洞威胁。

抵御计算机遭遇不法分子进攻的技术方式多种多样，但是其中最根本的还是应该加强防病毒入侵的技术，从源头上保护用户的网络使用安全。加强对网络访问的控制，严格控制非法用户擅自更改用户信息及密码，进入网络系统需要身份验证，不免出现不法侵入的问题。实行信息加密技术就是在传播信息的过程中保障数据安全不受到威胁，这样的技术研究能够确保网络中的文件、数据等信息在传输过程中的安全，加强保护屏障。

三、结束语

计算机网络安全技术对整个互联网的使用和发展运行来说是至关重要的，是实现用户上网安全，保障自身信息的基础。但是在目前的网络使用中，还是存在着诸多的病毒问题以及个人信息暴露问题，非法用户擅自制造网络病毒行不法之事，威胁人民群众的网络安全。基于此，本文主要分析了当前计算机网络安全技术问题开展的影响因素，又从以上三方面措施展开研究切实解决当前问题的有效办法，实现网络安全运行管理，净化计算机网络环境，从根本上杜绝网络安全威胁。

参考文献：

[1] 王书漫 . 计算机网络信息安全中数据加密技术分析 [J]. 电子测试 ,2022(7):86-88.

[2] 张皓钧 . 计算机网络安全技术的应用策略 [J]. 电声技术 ,2022,46(2):59-61.

[3] 李健 , 李小虎 , 武彦明 . 计算机网络信息安全技术及发展 [J]. 中国新通信 ,2022,24(1):131-132.

[4] 王萍芳 . 中职院校计算机网络安全技术应用与实践研究——评《计算机网络信息安全及管理技术研究》[J]. 中国安全生产科学技术 ,2020,16(6):189.

[5] 李君 . 数据加密技术在计算机网络信息安全中的应用 [J]. 南方农机 ,2020,51(15):196-197.