

计算机网络通信中的安全问题与防范策略分析

杨 萍

(阿克苏职业技术学院 新疆阿克苏 843000)

【摘要】随着信息技术迅速发展,计算机逐渐成为人们娱乐、办公等过程中必不可少的工具,丰富了人们的生活,提升了各行各业的生产效率。但是在利用计算机进行上网等过程中,可能出现网络诈骗、网络病毒等网络通信安全问题,使人们面临财产被骗、信息被盗等威胁,会对个人或企业带来巨大的经济或名誉损失,因此要采取系统、有效的防范措施。基于此,本文在分析计算机网络通信特点及加强其安全防防范的意义的基础上,结合目前普遍存在的安全问题,针对性的探索相关的防范策略,以期助力计算机网络通信向更安全的方向发展。

【关键词】计算机网络;通信安全;安全防范

DOI: 10.18686/jyfyzy.v3i4.40611

计算机及其网络通信技术的发展和普及,使世界产生了翻天覆地的变化,其在生产及日常生活中发挥着越来越重要的作用,QQ、微信、电子邮件、钉钉及各式浏览器等已成为国人日常生活、工作中必要的信息通讯工具。而人们在利用这些计算机软件进行网络信息通信时,可能因自身操作、网络陷阱、软件漏洞、网络病毒等多元因素,泄露了自身大量信息,包含私密照片、重要文件及各类账号密码等重要信息,这些信息的泄露可能进一步使其遭遇诈骗、账号及财产被盗等风险,对于公司而言,重要运营、管理信息被盗可能导致巨大的管理危机,极不利于其今后的发展。可见,加强计算机网络通信安全的防护势在必行。

1 计算机网络通信安全的特点与防范意义分析

1.1 特点

计算机网络通信安全主要具有完整性、保密性两个特点。完整性特点指利用计算机网络传输信息过程中,一般不会因外界因素出现数据丢失等问题,因此具有通信的完整性。保密性则是计算机通信安全中应具备的重要能力,主要表现在网络信息的传输及数据存储等过程中,相应的安全系统应能够保护用户计算机内部信息及通过网络保存、传递的个人私密信息,如通过信息加密等手段,限制不同用户对计算机信息的访问权限,只有具有相应授权的账号才能访问对应权限的信息。完整性与保密性特点,使计算机网络通信具备了安全保障。

1.2 意义

计算机网络通信的安全指在相关安全技术及系统的保障下,对计算机系统、硬件、软件、操作系统等内容进行全面的维护,全面、有效的网络通信安全系统,可有效的避免计算机网络信息传输过程中面临的数据被干扰、破坏、窃取等问题,从而达到保障网络通信安全的目的。而不同情况下,对计算机的网络通信安全的要求及具体保障内容是不同的,要想全面的保障计算机的通信安全,就需要计算机根据系统运行的情况做出具体的安全防护变化,例如,用户通过电脑QQ进行网络聊天或发送文件时,需要计算机安全系统会对聊天内容、文件内容进行加密处理,保障信息准确、安全的传递给相应的用户,如在互联网上进行商业运作、专业管理等工作,需要计算机的网络安全系统高效、全面地拦截各类尝试访问的不安全

信息,如未获取认证的网页、下载信息等,从而阻挡垃圾、病毒等隐秘的安全隐患进入计算机,又如通过计算机网络开展金融业务时,需要有相应的专业密钥,保障每一笔交易的安全,避免相关的金融账号、密码被盗取。具体而言,保障计算机网络通信安全有两方面的意义。

1.2.1 有助于人们更好的生活、工作

当前人们对计算机的使用频率十分高,特别是对于各类公司而言,无论是经营还是管理等层面,都购买了大量计算机,构建了相应的信息工作体系,以便更高效的开展各类工作,以财务工作为例,通过计算机能更快速、编辑的保存、传输和处理各种财务信息,大幅提升财务核算等工作的效率,但若因通信安全问题导致财务数据失真或被窃取,将直接影响企业的利益,还可能产生管理危机和不良的社会效益。因此做好计算机通信安全防范,能助力人们更好的生活、工作。

1.2.2 更好的维护人们的利益

信息时代,各类信息与人们的利益息息相关,计算机网络通信中可能涉及非常广泛的信息,无论是个人私密信息,还是企业生产信息,都可以通过电子邮件、QQ等实现信息传输,若这些信息因账号被盗而被盗取,可能直接骗取财产,利用信息欺骗转账或诱导人们进行网络非法赌博等行为,直接危害了人们的利益。而合理的加强计算机网络通信的安全防范工作,能够针对性的降低相关问题发生的概率,维护用户利益。

2 计算机网络通信中常见的安全问题及原因探析

2.1 问题

2.1.1 病毒入侵

木马、蠕虫等类型的病毒是造成计算机网络通信存在安全隐患的重要因素,且可能对计算机造成致命影响,如导致计算机完全无法使用。木马病毒主要是通过携带病毒的文件进入计算机系统,植入具有信息破坏、篡改等能力的代码指令,攻击计算机程序及信息,蠕虫病毒则具有繁殖、复制等能力,因此想要全面的清理病毒是十分难的,对其进行恢复也是比较困难的。

2.1.2 软件漏洞导致的安全问题

一些网络软件因自身编码或相应的加密系统存在一定的缺陷,会给不法人员以可乘之机。当前,腾讯QQ、

支付宝等软件已是行业的领头羊,软件发展的时间已较长,但用户账户密码被盗等情况依然存在,可能使原用户及其好友损失钱财。还有一些网络黑客可能利用非官方网站,在软件中添加恶意代码,导致用户下载软件后,计算机被黑客远程控制。

2.1.3 互联网开放性等因素隐藏的安全问题

互联网的开放性特征十分明显,但为人们提供便捷、多元的信息传输服务的同时,也为非法信息提供了隐蔽之地,各式网络及其信息,会对人们的行为产生不良引导。同时,网络的开放性也使得一些人员出于金钱利益、心理需求等目的,在互联网上的大肆发布不实信息,导致网络文化、网络环境更加糟糕,给更多的人造成不良影响。

2.2 计算机网络通信安全问题产生的原因

2.2.1 缺乏科学、完善的网络法律

我国当前的计算机通信相关技术的发展飞速,各式的网络安全问题却不断凸显,但相关法律规范却并未完善。现有的网络法律条例十分粗略,无法针对具体的网络通信问题进行规范化的管理,也没有标准化的法律参照,如《计算机软件保护条例》等法律虽一定程度促进我国网络向规范化方向发展,但不适应当前计算机网络通信的安全现状,滞后性明显。

2.2.2 大众的安全防范意识低

许多用户在使用计算机网络时,不重视自己的信息,随意的向相关网站、软件提交自身的身份信息,对其提供的相关信息条例毫不关心,导致自身信息被相关企业乱用。同时,一些用户对计算机的安全防范体系认识不足,没有安装安全防护、杀毒等软件,或随意的此类软件的安装,或非浏览色情、赌博等不安全网络,导致一些存在风险的文件进入计算机。

2.2.3 缺乏系统、有效的安全防范

计算机网络通信需要应用防火墙、信息加密等多重技术才能实现系统、有效的安全防范,然而无论是个人,还是企业在信息体系建设时,往往没有充分的利用多种手段建设系统的防范体系。

3 防范计算机网络通信安全问题的策略研究

3.1 健全计算机网络通信相关法律

相关政府部门应根据当前及未来的信息发展态势,科学的健全计算机网络相关法律法规,具有前瞻性的为相关行业提供工作规范,从源头扼制不安全行为、因素,同时为相关的计算机网络监管工作提供更强大的法律支持,使其更好的维护网络秩序。首先,可以对当前已有的相关法律内容进行细化,健全或更新其中不适宜的内容,使其与当前及未来的网络通信形势相协调;其次,需要结合计算机网络的发展情况,制定新的网络安全管理规范条例,细化完善各个流程及具体环节的工作内容,如规范病毒防

治、软件保护管理等内容。

3.2 用户提高安全防范意识

很多用户的网络通信安全意识及防护水平都十分弱,即使相应的法律和软件都已完善,个人不安全的操作依然可能造成信息泄露等问题,因此用户需要提升自身的安全意识及防范水平,安全、规范的使用计算机网络。例如,在使用计算机前,需要在相关官网下载正规软件,以避免接触携带病毒的非正规软件,同时,在合理的应用防火墙等防护工具的同时,还可以下载 360 安全卫士等计算机杀毒、清理软件,其通过及时的更新网络病毒数据库,比对计算机所以文件来查杀各类病毒,以发挥病毒查杀等作用,提升用户计算机通信的安全水平。对于公司而言,为避免员工随意的网络通信行为导致信息泄露等问题,在对员工进行全面的计算机网络使用安全宣传的同时,应制定相应的管理条例,如在常规情况下不得使用他人电脑,不得浏览、下载、传递上级电脑内的任何信息,为使相应的工作更为规范,企业还应建立自身的信息系统,为每位员工提供不同权级的账号。

3.3 应用防火墙等技术,建设系统有效的安全防范体系

首先,合理的应用防火墙技术,阻止非法或不安全信息访问计算机,为用户登入计算机及网络浏览等过程提供安全屏障,如及时的阻隔非法用户,并通过相关邮箱等形式提醒原用户中止进程,企业可以通过在控制主机中设置防火墙,对局域网内所有子机进行快捷、统一的通信防护。

其次,做好数据加密、备份等措施。通过更为复杂的密码或加密形式提高信息被破解的难度,防止通信过程中数据被窃取,各类计算机软件及网络平台一般都要求用户注册账户时设置密码,用户应尽量设置组合密码,而相关企业应当丰富账户认证方式,如加入人脸识别、设备识别等手段,更有利保障用户信息的安全。数据备份是指用户手动将关键信息通过 U 盘、云盘等方式进行备份,或在使用相关软件时设置自动备份措施,以避免重要信息丢失或被破坏、篡改。

4 结语

综上所述,计算机网络快速发展,其通信安全是人们十分关注的问题。当前尚存在一些相关的安全问题,产生的原因也是多样的,因此相关的主体需要更加重视计算机网络通信的安全防护工作,从完善法律、提高安全意识和防范水平、建设系统的防范体系等方面入手,全面、有效抵御各类网络安全问题。

作者简介:杨萍(1967.4—),女,新疆阿克苏人,讲师,研究方向:计算机应用。

【参考文献】

- [1] 张麦龙,关于计算机网络信息安全和防范策略的探索[J].中国新通信,2018(13):153.
- [2] 孙伟俊,关于计算机网络信息安全及防护策略探究[J].信息通信,2018(6):114-115.
- [3] 戴晨昱,企业云计算应用中的安全风险防范策略[J].智库时代,2018(25):257-258.
- [4] 焦智灏,关于计算机网络信息安全及其防护策略的探讨[J].电子世界,2018(18):108.