计算机网络信息安全及其防护策略

张晓 | 文

随着我国社会和经济的飞速发展，计算机网络被应用到生活中的各个方面。但是计算机网络在给人们带来便利的同时，也会威胁到人们的信息安全。面对这些问题，计算机用户必须要提高信息保护意识，这样才能减少犯罪分子有机可乘的几率。因此，人们在生活中还要学会利用恰当的方式进行计算机网络信息安全以及防护，并对计算机网络信息进行安全、有效的管理。

人类步入二十一世纪以来，就已经进入到信息时代，计算机技术也被广泛应用到各行各业。因此，面对计算机网络的迅速普及，网络信息安全逐渐受到重视，这也关乎着用户的切身利益。要想真正保护好计算机网络的信息安全，还要在此基础上实现新的突破和发展，首先在思想上就必须重视起网络信息安全的重要性，同时还要不断发现其中存在的问题，积寻找更加有效的防护策略。

一、计算机网络信息存在的安全问题

面对网络充斥人们生活方方面面的现状，这既是科技进步的必然，也是时代发展的结晶。现在，企业的发展、人们日常的生活都离不开计算机，网络信息安全和防护也成为人们所关注的重点。下面本文将论述计算机网络信息安全和防护中存在的问题，推动网络环境朝着良好有序的方向发展，减少个人财产、企业财产以及国家财产损失的几率，全面提升计算机网络安全防护作用。

（一）计算机病毒问题

计算机中病毒是最常见的安全问题。一些黑客经常会在一些计算机小程序中植入一些具有破坏性的数据代码，并带入到计算机中，进而盗取用户个人信息，造成数据的缺失甚至是网络的瘫痪。通常情况下，这些计算机病毒本身具有传染性和复制性，会造成一批计算机瘫痪，这会给用户造成难以估计的损失。除此之外，用户在网络上进行应用和发展时经常会进行个人身份验证，而在这一过程中，经常会中病毒造成信息被不法分子窃取，甚至被非法使用。更有一些不法分子会穿过防火墙直接盗取用户的个人信息，这对个人的信息安全造成极大的威胁，甚至对整个网络环境都有威胁。计算机存在的方式通常有 USB 接口、复制传输文件传染等，这些方式也会随着网络技术的发展不断进步，人们要多加警惕。

（二）网络环境恶意攻击

一般情况下，黑客对于计算机的攻击通常是有目的性以及针对性的。翻越防火墙进行信息窃取的方式还在不断升级，这对当下网络的发展造成了严重的威胁。对于网络恶意攻击来说，不仅对导致数据的丢失、网络的瘫痪，甚至会造成被攻击对象大量的财产损失，需要耗费人力、物力以及财力进行修复，严重的情况下会阻碍生产，带来不必要的损失。

（三）计算机自身存在的问题

当程序员在进行程序开发时，也会存在相应的技术问题。经常会出现没有发现漏洞的情况，还有发现漏铜没有及时进行修复和设置高级别防盗的措施，这些都会成为黑客入侵系统的方式。除此之外，就算程序员设置了安全级别、稳定性都比较强的防护措施，但也无法保证网络会百分之百的安全，这既是网络环境发展的限制，也是条件限制，这需要程序员在不断发展计算机技术的同时不断优化解决措施。

二、影响计算机网络信息安全的因素

近些年，随着计算机技术的发展，越来越多的领域

会使用计算机来提升工作效率，我们的生活中同样存在大量计算机的影子，但是它在促进社会发展的同时，还会影响信息安全。因此，这些年来，信息安全成为人们关注的重点。相关技术人员必须要清楚的了解影响计算机网络信息安全的因素，才能做出相关的实施对策来促进社会的发展。

（一）物理层的影响因素

物理层的影响因素主要是指计算机的硬件受损，造成信息泄露以及服务无法正常运行、服务中断的现象。这通常会有很多方面的影响因素，可能会因为信息化技术是由软件和硬件两部分组成，通常情况下，一部分出现问题就会导致服务器受损。此外，自然因素也会影响硬件，包括自然界中的风雨雷电，这些都会阻碍计算机的网络服务，此外还有高温、寒冷天气也会影响计算机的正常运行。

（二）软件层面的影响因素分析

在大数据发展的时代，黑客攻击已经成为数据被恶意破坏的主要原因，这也极大的影响了信息技术的发展。黑客作为当前面对信息化时代专门出现的破坏信息系统功能的群体，已经能够具有针对性以及目标性的恶意干扰或者攻击包括网站、相关信息化服务的系统。并且，世界上各国的系统都接受者来自不同程度的威胁，甚至还会为此损失数千亿美元，因此，现在黑客攻击已经成为信息安全下最大的威胁。有些人还会受利益的驱使盗取机密信息，主要分为主动型攻击和被动型攻击两种攻击目标类型。主动型攻击是电脑黑客通过程序或者手段选择特定的目标，并破坏目标信息的完整性和有效性。而被动型攻击目标则是为了获取机密信息，采用窃取的方式破译、拦截、窃取信息。

三、计算机网络技术的网络信息安全与防护措施

在现代社会中，计算机扮演着越来越重要的角色，人们也逐渐用计算机完成越来越多的工作。人们在网络上信息交互的越频繁，就越需要注意用户的信息保护。除此之外，由于计算机网络本身具有开放性并且还会存在不同程度的漏洞，不法分子就会通过漏洞威胁信息安全，也会给人们带来严重的经济损失。人们更要不断加强防护措施，保护个人以及企业的信息安全。

（一）应用防火墙技术，尽可能的隐藏 IP 地址

防火墙会根据规定的数据传输路线，协调保证用户信息的安全。通常情况下，防火墙作为重要的软件设施可以在一定程度上杜绝出现危险的机会，还能对流入流出防火墙的信息进行规范，减少出现数据入侵的几率。不仅如此，防火墙还能对网络进行扫描，并发现其中携带的病毒，达到防御的效果。因此，相关工作人员还要从根本上提升信息安全管理的强度，还可以通过建立计算机数据库的方式避免数据丢失的情况。同时，还要加强计算机病毒防范的技术，起到重要的防护作用。最重要的是，用户要从自身做起，尽量不下载存在问题的软件，即使要下载也要做好杀毒措施。在进行信息传输时也要采取加密措施，减少网络黑客破坏计算机系统的可能性，此外还可以利用代理服务器隐藏 IP 地址，不断提升网络信息的安全性。

（二）及时安装漏洞补丁，设置访问控制权限

在计算机进行网络安全防护的过程中，及时安装漏洞补丁是一项非常重要的措施。由于计算机会受到各种因素的影响，系统程序设计不合理、资源配置不当以及软硬件不完善等因素，都会在一定程度上产生计算机漏洞，若不及时进行处理，就很容易造成信息泄露。因此，用户在使用计算机的时候，要及时下载并安装漏洞补贴，并及时掌握最先进的检测技术，可以及时的检测病毒，达到防护作用。还可以使用人工智能以及网络通信的优势进行综合性的管理并定期进行风险预警，提醒用户进行病毒扫描，并在及时发现危险的基础上采取合理的措施。不仅如此，用户还要特别注意设置访问控制权限，学会合理利用文件、目录的资源。对于机密度较高的信息来说，还要采取适当的加密技术进行处理，将危险降到最低，对信息进行严格的管控。

四、结束语

综上所述，人们在利用计算机带来极大便利的同时，其中还会混杂各种交流信息，这就需要用户特别重视网络信息安全及其防护，并养成良好的安全防护习惯。除此之外，还要学会分辨信息种类，自觉抵制不良信息、广告诱惑，对于风险网站做到不点击、不打开，还要自觉使用正规网站，定期更新安全防护的软件，在全面提升信息安全防护水平的同时，保护用户的财产安全。

作者简介：张晓，单位：四川水利职业技术学院。