**计算机网络信息当今社会进步和发展的重要因素**

**早该帮 编制**

计算机网络信息当今社会进步和发展的重要因素，计算机网络信息的普及率逐渐增加，网络信息的覆盖面积日渐增加。但是计算机网络信息技术，会受到一些不法分子的破坏，给计算机网络信息安全造成不同程度的破坏，制约计算机信息网络的正常使用。基于此，就计算机网络信息与防御技术展开探究，并着重对计算机网络信息与防御技术的应用实践进行阐释，旨在为相关人员提供参考，促进计算机网络信息的安全，构建健康的计算机网络信息环境。

计算机；网络信息；防御技术；应用实践

信息技术的不断发展，使得计算机网络覆盖面积变得更大。但在实际应用过程中，会受到一些不法分子的影响。这些不法分子通过网络信息漏洞，获取用户的相关资料，给用户造成不同程度的损失，影响计算机网络信息技术的安全。因此，需要对影响计算机网络信息技术安全的因素进行分析，采取有效的防御技术，确保计算机网络信息的安全，构建安全、健康的网络环境，为人们提供更加优质的服务。

1.计算机网络信息的相关概述

1.1计算机网络信息涵义

计算机网络信息主要是以计算机为基础，促使计算机与互联网进行有效衔接，用户能够通过计算机网络获得所要的信息。而且计算机网络能够根据不同的地理位置，实现多台计算机的连接，这一连接过程主要是通过通信设备和线路进行连接的，计算机网络信息技术是计算机技术与通信技术的结合产物，是信息技术发展的进一步成果，通过计算机网络信息技术能够有效的实现网络资源的共享和信息的传递。计算机网络信息主要是由各个大型模块构成的，主要包括广域网、局域网等。

1.2计算机网络信息技术的应用

计算机网络信息技术现已应用到社会的各行业各业，促进了社会进步与经济发展。人们的日常生活、学习和工作都与计算机网络信息技术息息相关，人们可以通过计算机网络技术进行资料搜索和下载，满足精神娱乐需求。在军事上可以优化教学和训练的效果，丰富了军事的各类手段，促进我国的长治久安。在教育领域，能够丰富学生的视野，拓展知识面，有效地构建综合化和现代化的教学体系，提高教学质量。而且，丰富的教学资源库的建立，极大地丰富了教学资源，实现了各类教学资源的传递和共享。在商业领域中，能够促使各类商业活动获得良好的发展，实现自动化办公，建立完善的商业平台和良好的服务体系，积极推动社会经济的持续进步。

2.计算机网络信息存在的安全隐患

计算机网络信息在实际的应用过程中，不可避免的受到各类安全隐患的影响，严重时会造成用户的相关信息流失，还会造成各类安全问题的发生，尤其是军事领域的计算机网络信息安全隐患，会对我国的社会安定造成影响，因此，需要加强对计算机网络信息安全隐患的分析。

2.1恶意软件

计算机网络信息技术在实际的应用过程中，具有开放性和多端性的特点，这也就会使得计算机网络信息技术在实际的使用过程中，可能会受到恶意软件的捆绑安装，这些恶意软件具有顽固性和不易清除性，影响计算机的应用质量，而且还会在用户不知情的情况下，对计算机网络信息造成巨大的安全威胁，导致计算机内部的程序被改写，用户的财产和利益会受到损害。

2.2黑客攻击

黑客是计算机网络信息技术安全的安全隐患，黑客主要是一些掌握一定计算机技术的人员，通过特殊的技术对他人的计算机进行攻击，并利用隐蔽性的木马程序对计算机进行病毒植入，获得客户的相关信息。这也就会导致客户的计算机网络安全不能得到有效的保障，严重时会给用户带来重大的经济损失。一般黑客攻击是会利用电子诱饵、邮件、IP地址等方式对用户的计算机网络进行攻击。例如在日常生活中，人们会受到电子诱饵的影响，造成个人信息和财产的流失，主从式的DDoS攻击结构图。

2.3计算机网络自身存在的漏洞

计算机网络信息在实际的应用过程中，会安装一些软件，但是这些操作软件自身可能存在一些漏洞，而这些漏洞的存在，会造成计算机网络信息存在安全隐患，这也就会影响计算机网络的安全。一些不法分子会对这些漏洞进行利用，就可能会对用户的计算机造成损害，运用病毒植入的方式，对用户的相关信息进行盗取，使得用户受到损失。

3.计算机网络信息的防御技术的应用实践

针对计算机网络信息技术应用过程中存在的安全隐患进行分析和分类，结合计算机网络信息技术的实际应用，采用合理的防御技术，构建健康、安全的计算机网络信息环境。现阶段计算机网络信息的防御技术主要是建立在动态自适应性网络安全模型PPDR的基础上。

3.1安全扫描

用户在使用过程中，需要具备良好的网络安全意识。因此，合理的启发式扫描、行为扫描、模糊匹配等安全扫描技术运用是必须的。通过动态性能的扫描，能够发现计算机中存在的安全隐患，通过扫描的反馈，能做出相关的处理措施。

3.2系统增强

在实际的运用过程中，计算机网络的安全架构不能有效发现一些新的威胁，这也就使得安全隐患的出现。可以通过系统增加的方式提高防御能力。系统增加能够对计算机网络信息中的一些恶意数据进行检测、拦截，避免恶意数据对计算机造成影响，以及伤害的扩大。

3.3学习、自适应

学习性、自适应的防御系统应用能有效提高计算机网络的防御能力。该防御系统主要呈现为智能化防入侵能力，根据计算机传统的检测、扫描反馈，进行智能学习，并形成新的防御能力，使计算机网络能够对新型的病毒充分免疫，针对各类攻击和入侵进行控制，提高计算机网络信息的安全。

3.4实时响应与黑客诱骗技术

实时响应建立在动态自适应性网络安全模型PPDR的基础上，当系统发现计算机网络遭受外部攻击和自身漏洞时，以实时响应和声音电子邮件等方式反映给用户，以便及时处理。黑客诱骗技术是通过释放虚假信息，拖延黑客入侵时间，给使用者足够的时间防御。将实时响应与黑客诱骗技术相结合，能够在黑客入侵的第一时间发出警报，促使用户尽快处理和防御，提高计算机网络信息的安全。

4.结语

计算机网络信息技术的覆盖面积不断增加，只有对计算机网络信息的安全隐患分析，制定合理的防御技术，才能有效提高计算机网络信息的安全系数，规避各类安全隐患的发生，营造一个健康、安全、可靠的计算机网络信息环境。

关键词：计算、算机、网络、计算机、计算机网络、信息、当今、社会、当今社会、进步、和、发展、的、重要、因素

参考文献：[1]早该帮https://bang.zaogai.com/item/BPS-ITEM-28481.html