# 中职学校校园网络安全现状分析与对策

苏秦

（佛山市华材职业技术学校　广东　佛山　528000）

[摘　要]在全球信息化的背景下，计算机网络的重要性日益凸显。对于中职院校来说，师生主要依靠校园网来进行日常的教学活动，并且还要依靠校园网实现教学研究和对外交流等教育任务，但随着信息技术的不断发展，越来越多的因素不利于校园网的安全稳定。基于此，本文对中职学校校园网络安全现状进行探讨分析，介绍相应的安全隐患，并提出一些防范对策。

[关键词]中职学校；校园网络安全；现状；防范对策

【DOI】10.12252/j.issn.2096-627X.2021.06.035

## 前言

近年来，随着计算机技术的不断发展，其应用范围更加广泛，中职学校也借助计算机技术不断完善校园网络。中职院校的教学活动和管理工作也逐渐朝向智能化发展，主要体现在多媒体教学和图书管理系统等方面的信息化建设。但随之而来的校园网安全问题也愈加严重。对于职业院校而言，保障校园网络的安全运行是当前亟须解决的一大难题。

## 一、中职学校校园网络安全现状与使用情况

### 1.学校校园网络安全现状

校园网作为一种局域网，具有一定的特殊性，主要为了满足学校教学和管理的需求，所以既对外开放，却又相对独立。因此，其网络安全具有一定的特殊性。中职院校的学生正处于人生发展的关键时期，由于年龄较小，对新鲜事物充满好奇心，但缺乏安全防范意识。在中职学校中，学生是使用校园网较为频繁的群体，由于好奇会勇于试验自己学到的各种攻击技术，但却没有考虑会产生怎样的影响，从而严重破坏校园网络。另外，中职学校受到资金等各方面因素的限制，缺乏对网络安全设备的投入，并且没有建立完善的网络管理制度，难以保障校园网运行的安全性和稳定性。

### 2.中职学校校园网络的使用情况分析

中职学校积极建设“三通工程”，不断对校园网络进行完善，以保障教学活动和管理工作的顺利开展。随着信息技术的发展，各种信息资源实现共享，中职学校利用校园网络满足学生的学习需求，增加学生的知识储备量，并为教师提供丰富的教学资源，充分体现出来校园网的应用价值。但随着校园网的发展，其存在的相应问题也逐渐显露出来，其中最主要的问题是缺乏有效的保障措施。在中职院校的实际教学过程中，重点是不断提升学生的操作能力，因此将学校内部资金大多用到建设实训基地和购买相关设施设备方面，缺乏对信息安全保障措施的投入。而这些有限的资金一般用于更新软件，以及维修相关设备上面，能够用于运维的非常有限。大部分中职学校没有相应的硬软件建设，导致校园网安全难以保障，学校教师和学生的网络安全防范意识也比较薄弱。如在下载更新软件的过程中，不能注意到一些恶性插件，危害到网络安全。同时在使用的过程中，不能考虑到一些网页缺乏安全性，而随意浏览网页，不仅导致信息遭到泄漏，也可能会破坏软件系统[1]。中职学校人群较为集中，使用校园网的人员比较多，若导致病毒入侵，将会产生严重的后果。因此，中职学校必须要重视网络安全，并加大相应建设和资金投入，有效预防网络安全隐患的发生。

## 二、中职学校校园网络存在的安全隐患

### 1.师生缺乏安全防范意识

对于中职学校的广大师生而言，他们往往会认为校园网络的安全问题与自己没有关系，应由相关技术人员负责，所以在使用过程中很容易出现各种安全问题。同时一些中职学生由于缺乏网络安全防范意识，而随意打开相关链接，在很大程度上增加了校园网络发生安全隐患的概率，无法保障网络的正常运行，也降低了相应维护管理工作的有效性。

### 2.无线密匙遭到破解

无线网络本身具有一定的特殊性，比较容易受到非法用户的攻击，所以相关管理人员为了保障数据传输的安全，会更加谨慎对待密匙的设置，同时增强加密认证，但这种方式也存在一定的不足，据相关人员测试发现在短时间内就可以破解被保护的网络。而对于一些不法分子而言，其可以利用特殊手段捕捉无线网络信号，进而取得数据包，不仅会破解密匙，也会对其进行相关的侦测。

### 3.计算机病毒的入侵

现阶段，计算机病毒严重威胁网络运行安全，病毒具有较强的适应性，并不断在增强其破坏性。一旦校园网接入网络，很容易遭到病毒的入侵，在安装软件或者浏览网页的过程中，都存在一定的安全隐患。中职学校校园网用户较多，不论哪台机器遭到病毒入侵，如果不能及时处理，都可能会导致系统被破坏，不仅信息资源受到影响，硬件也可能会被损坏。严重的话会降低整个网络系统的运行效率，导致校园网络系统瘫痪。

### 4.非法入侵

校园网一旦接入Internet，也经常遭到黑客攻击，导致非法入侵。随着互联网技术的发展，对于一些不法人员来说更容易学习一些黑客工具，很多网站甚至都有教程。一些非法分子利用相关手段攻击网络，入侵服务器，严重威胁数据信息安全，盗取或者修改数据，破坏网络系统。拒绝服务时入侵者经常使用的手段之一。在拒绝服务中，入侵者经常制造一个虚假的客户端，然后让其和AP相连，然后入侵者再通过攻击行为影响AP，使其出现错误的判断，进而拒绝服务[2]。另外，一些入侵者会通过耗尽网络系统的资源，而使其不能正常运行。此外，一些不法分子也会通过网络病毒来破坏无线物理链路，达成攻击的目的。通过这种攻击方式，会导致网络用户的数据丢失，也会造成校园网络出现严重瘫痪的现象。

### 5.数据安全隐患

通过破解密匙等行为可以让不法分子侵入到中职学校的校园网络当中，从而盗取师生的相关数据信息，侵犯个人隐私，信息的泄漏也会带来严重的经济损失。入侵者也可以使用相关手段传播网络病毒，使得大量终端用户出现中毒的情况，严重威胁校园网络安全。同时随着互联网技术的发展，也随之出现了一些控制网络设备的软件，而一些学生由于好奇而下载一些这些软件，从而导致校园网络拥塞，产生严重的后果。

### 6.硬软件安全隐患

一方面是中职校园网络硬件的安全隐患，主要体现在机房设备的安全性，相关管理人员在开展日常工作的过程中，要做好相应的预防措施，保障机房环境的干燥性，并保持设备的洁净，以免硬件出现故障。另一方面是中职校园网络软件系统的

安全隐患，其直接关系到整个系统的信息安全。对于大多数中职学校来说，一般不会定期检查网络系统的安全性，以至于运行过程中出现各种安全问题。

**三、中职学校校园网络安全问题解决对策**

1.建立完善的管理机制，增强网络安全防范意识

现阶段，中职学校的网络安全管理人员在实际工作的过程中，为了有效保障校园网络安全，应积极建立完善的网络安全机制。相关管理人员要重视网络安全问题，及时对网络信号传输情况进行检测，以便及时发现存在的安全隐患，制定相应措施解决问题。另外，中职学校的管理人员应不断增强广大师生的网络安全方式意识，定期组织相关培训，提升师生信息安全水平，并加强相关法律法规的教育，帮助整体师生形成良好的网络安全防范意识。同时，还应加大网络信息安全的宣传力度，通过校园网、广播、微信公众号以及校刊等方式拓宽宣传渠道，让所有师生真正意识到网络安全对他们的重要性。也可以开展相应的教育活动，如可以举办以网络安全为主题的研讨会，对相关安全问题进行深入的分析，以及举办网络信息安全辩论活动等，通过这些活动深化师生对网络安全重要性的认识。要想保障校园网络安全，其实防护要远远重于治理，但需要花费大量的时间，提高师生的防护意识，帮助他们养成安全使用网络的习惯，能够自觉保障网络安全。在实际使用网络的过程中，不要随意点击信息链接，下载安装软件需要选择安全的渠道[3]。另外，硬件系统的安全维护对于校园网络安全具有重要意义，广大师生要学会正确操作电脑，以免损坏硬件，真正从根源上避免出现安全隐患。

2.完善软件系统

在引发校园网络故障的众多因素中，网络系统问题占有较大的比重，所以必须要保障系统安全。一旦发现网络系统存在安全隐患，要及时进行完善。首先需要把控好校园网络入口的安全，必须经过实名认证才能登录校园网，提高密码强度，并重视防火墙技术的应用。随着互联网技术的不断发展，防护墙技术也在持续更新，中职学校应积极引入先进的防火墙技术，有效查杀病毒，保障校园网络的安全运行。这就要求学校增加相应的资金投入，不断研发新技术，有效保障学校信息安全。同时，要充分发挥管理人员的作用，如今很多中职学校都是由信息技术教师来管理校园网络，缺乏专业人员，而信息技术教师不仅缺乏相应的专业维护技术知识和维护经验，还需要做好自己的教职工作，没有充足的时间和精力来维护校园网络。这样就导致网络安全维护的实效性大幅降低。因此，现阶段的中职学校应聘请专业的维护人员，才能有效保障校园网络运行的安全性。

3.制定有效的防控应急措施

在校园网络安全建设的过程中，不仅要考虑到预防措施，也要注重问题发生后的应对方法，校园网络安全问题主要由外部因素和内部因素这两方面造成的。一旦不能做好网络疏导工作，会导致大量用户使用统一端口，进而使得校园网络瘫痪，影响教学活动的开展。现阶段，由于很多中职学校忽视网络安全问题，所以没有制定相应的紧急应对措施。在众多引发网络安全问题的因素中，病毒是长期最难以应对的一种，虽然不断在加强网络安全的防范能力，但还是不能避免病毒的侵扰，因此，必须药做好预警工作，以便能够及时应对新出现的病毒，以免造成更加严重的后果。在网络风险防范的过程中，为了更好的保障用户数据信息，需要设置使用权限，并设置相应的口令[4]。同时，对于校园网络的实际使用情况也要及时进行记录，这样才能更有效的排查病毒。要严格管控访问权限，验证不合格的用户不能进入校园网络，以阻挡黑客入侵。另外，可以引进先进的漏洞扫描机制，全方位检查服务器，并对其安全性进行分析。若发现安全隐患，及时采取有效措施，解决问题，进而保障校园网络安全。并选择科学的病毒查杀软件，及时更新病毒库，有效开展检测工作，以免病毒进一步传播。

4.构建校园网络信息安全架构

中职学校在校园网络建设过程中，应科学开展安全架构工作，以提升校园网络的利用率。在实际操作过程中，应基于整体的校园网络，对各个区域进行精细化管理，定期检查网络设备的运行状态，及时更换老旧设备。并且要划分有线线路和旧线路，在学生宿舍区域设置无线AP，在办公区域设置有线网络，并加密无线数据，有效降低发生校园网络安全隐患的概率。

5.加强网络信息安全软硬件技术管理

在中职校园网络安全防范的过程中，涉及各种软硬件，中职学校不仅要增加资金投入，还需加强技术管理。例如，在智慧校园网络体系中，包括入侵检测和病毒防御等。中职学校在做好技术管理工作的基础上，还要制定各种防御措施，主动监测各种网络病毒和不明链接，加强安全防范水平，确保落实相关安全管理制度，保障校园网络软硬件系统的安全运行。

6.打造高素质的安全巡查团队

为了更好的维护校园网络安全，中职学校应积极打造一支高素质的安全巡查团队，将学生作为主体对象，围绕信息中心，聘请专业的技术人员加强对师生技术操作的指导，帮助其在使用过程中能够察觉校园网中存在的安全隐患，并有效规避相应风险。加强校园网络安全维护的有效性，规范开展校园网络管理工作，强化中职学生的操作能力，促使广大师生积极参与到校园网络安全维护工作当中，营造良好的校园网络文化氛围。并引进先进的安全防范技术，完善安全管理制度，有效保障中职校园网络安全运行[5]。这样通过全体师生的广泛参与，自觉维护网络安全，才能真正发挥校园网络安全维护的实效性。

**结束语**

总而言之，对于中职学校来说，校园网络安全管理工作具有较强的技术性和专业性，必须重视该项工作，建立完善的管理机制，增强师生的网络安全防范意识，完善软件系统，制定有效的防控应急措施，构建校园网络信息安全架构，及打造高素质的安全巡查团队等，有效保障中职校园网络运行的安全性。

**参考文献**

[1]蒋会军.县域中职学校校园网络安全现状分析与对策[J].科技经济导刊，2020（07）：144.

[2]徐丹.计算机网络安全技术在中职学校校园网中的应用[J].信息记录材料，2020（07）：99-100.

[3]刘婷.中职校园网络信息安全问题及其防范策略[J].数字通信世界，2019（11）：125.

[4]刘炎火.探索中等职业学校校园网网络安全技术[J].中国科技信息，2019（07）：105-106+14.

[5]曲清.中职学校校园网络安全管理策略[J].电子技术与软件工程，2019（01）：191+231.

作者简介：

苏秦，1988.11，男，汉，陕西渭南，大学本科，网络工程中职初级教师，网络安全方向。