远程办公，在线教育中的网络安全隐患与防范对策分析

杨 帆
重庆市教育信息技术与装备中心，重庆 400020

[摘要]互联网技术的发展让远程办公、线上教育成为了现实，人们可以通过计算机、平板电脑等电子产品在家中开展自己的工作或进行学习。但即便如此，人们在线上开展办公、教育等活动时，却仍然需要面对很多问题，如网络病毒、木马就将会对网络安全造成非常大的影响，因此必须找出解决网络安全问题的方式，以此来降低风险隐患。文章对网络安全隐患进行分析，并对远程办公，在线教育中的网络安全防范对策提出个人看法，希望为关注网络安全的人群带来参考。
[关键词]远程办公；线上教育；网络安全；网络风险防范
DOI：10.33142/fme.v3i5.7108　　中图分类号：TP3　　文献标识码：A

Analysis of the Hidden Dangers of Network Security and Countermeasures in Remote Office and Online Education

YANG Fan
Chongqing Education Information Technology and Equipment Center, Chongqing, 400020, China

Abstract: The development of Internet technology makes remote office and online education a reality. People can carry out their own work or study at home through electronic products such as computers and tablets. But even so, people still need to face many problems when they carry out office and education activities online, such as network viruses and Trojans, which will have a great impact on network security. Therefore, we must find ways to solve network security problems to reduce potential risks. This paper analyzes the hidden dangers of network security, and puts forward personal opinions on the network security countermeasures in remote office and online education, hoping to bring reference to the people concerned about network security.
Keywords: remote office; online education; network security; network risk prevention

引言

网络安全问题是信息技术发展期间人们关注的一项重点问题，因为网络安全风险无所不在，难以处理，只要借助网络开展网上操作，就存在受到网络攻击的可能性。在远程办公与在线教育期间，如果因为网络安全风险而丢失文件或影响教育效果，就会给人带来无法估量的损失。因此，有必要对网络安全隐患进行分析，并提出网络安全防范对策，以此来让人们的网络活动变得更加顺利。

1 网络安全风险分析

在信息技术高速发展的今天，世界上的网民数量正在与日俱增，人们如今已经习惯了由网络所带来的各种便利。通过网络来开展线上教育、远程办公已经成为了常见的事情，而且由于网络对人们的生活影响在逐年增加，网络安全问题已经成为了人们关注的焦点问题。网络信息安全作为人们在上网期间必须面对的安全问题，非常容易因为安全风险给人们造成损失。例如，在 2015 年 5 月，国内著名旅游网站“携程网”的服务器便在不知名网络攻击下受到了冲击，携程网直接宕机了 12 小时，这不仅对网站造成了严重经济损失，还刷新了国内互联网公司的宕机记录。在 2017 年 5 月，名为 WannaCry 的网络勒索病毒蔓延了全球，该病毒可以对各种有价值的网络进行冲击，大量高校、企业等机构的网络在病毒冲击下出现了文件恶意加密的情况，其引发的数据经济损失上亿。2020 年 5 月，由 ISC 所发布了 BIND 漏洞，网络攻击者通过在短时间内发送大规模的无意义数据，导致 BIND 服务器崩溃[1]。

各种网络安全事件表明了如今的网络并不安全，人们在开展远程办公，在线教学等活动时，都有可能因为病毒、漏洞等情况而导致网络受到冲击。每个国家都在积极寻找可以解决网络安全风险的方式，防火墙、漏洞扫描等网络技术也因此而出现。在国内，互联网技术的发展同样导致了网络安全问题的发生，网络安全条例中的内容也逐渐变得愈发完善。但是法律法规却无法真正解决网络安全问题。需要注意的是，随着时代的发展，网络问题将会逐渐变得越来越复杂，为了进一步提高网络安全防护能力，就应该对网络安全隐患进行分析，并结合实际需求来不断完善切实可行的网络安全防范对策，以此来降低网络安全风险所带来的影响性。

2 远程办公与在线教育中的网络安全风险隐患

在远程办公与在线教育期间，网络供给与系统漏洞将会带来非常严重的负面影响，虽然没有绝对完美的网络系统，但只要能找出远程办公与在线教育期间存在的网络安全隐患，就能够让网络安全防护工作开展得更加顺利。在远程

办公与在线教育中，较为常见的网络安全风险隐患如下：

2.1 WIFI 网络环境风险

网络环境风险是一种常见风险，由于路由器本身便存在网络安全隐患，因此一旦配置不当，就容易导致其他人进入 WIFI 网络，他人进入 WIFI 后不仅会导致网速下降，还有可能引发信息泄露等问题的出现。例如在使用通过 WEP 认知的路由器时，就容易导致 WIFI 被不法人员突破。与此同时，在远程办公与在线教育期间，由于人们可以借助任何网络来参加工作与学习，所以很多人还会选择借助公共 WIFI 来开展活动。然而公共 WIFI 的安全性却远远低于家用 WIFI，因为部分不法人员会通过主动搭建与公共 WIFI 名称相同、近似的 WIFI 网络，在吸引用户后会通过 DNS 劫持的方式进行网络攻击，并窃取用户的各种隐私信息。因此 WIFI 网络安全风险是人们必须面对的问题，需要通过加强安全防护来保障系统安全。

2.2 软件下载期间的网络安全风险

人们在下载远程办公与在线教育软件时，遇到的网络安全风险的情况特别常见，部分不法人员会选择入侵安全防护能力较弱的应用软件，并将软件替换成为具有木马病毒的恶意系统软件，这种替换后的恶意软件的界面与原版软件相同，人们在下载此类恶意软件并安装之后，就会在计算机后台自动打开并运行木马病毒，由于木马病毒的隐蔽性极高，又能在一定程度上规避主流杀毒软件，因此能够给用户带来非常大的负面影响[2]。例如 2018 年初出现一款译名为“坏兔子”的勒索软件，该软件能够利用水坑攻击的方法带来完成病毒传播。不法分子通过在各类合法网站中植入恶意代码，并将勒索软件伪装为 Adobe Flash 程序，可以利用网页弹窗的方式来进行诱导点击，当用户下载安装软件后，就会直接对用户设备的所有文件进行加密，此时便可以勒索用户通过提供赎金的方式来接触加密。该情况发生后在短时间内在俄罗斯、乌克兰等国家勒索了大量资金，并造成了网络恐慌。

2.3 远程办公与在线教育系统安全隐患

很多远程办公、在线教育系统在开发期间往往并不会在系统安全投入大量资金，而且系统在运行期间也缺少更新与维护，所以系统本身的安全防护能力相对较弱，当系统本身的安全防护能力无法应对网络威胁时，就会导致系统安全风险激增。在 2021 年 5 月，用友网络公司所开发的 ERP 企业管理系统与该公司旗下的电商平台被检测出了远程代码执行漏洞，该漏洞的存在导致了电商平台不当开放了错误测试接口，不法分子针对漏洞违规打造了 HTTP 请求并获取了平台服务器权限，造成了非常大的恶劣影响。

2.4 钓鱼邮件

自互联网普及开始，钓鱼邮件便成为了最为常见的一种网络安全隐患，不法分子可以编造发件人信息并投递带有违规链接、恶意代码的邮件。一旦收件人打开了这种钓鱼邮件，就会在计算机内部开展网络攻击，并窃取收件人的用户隐私数据。而且当钓鱼邮件打开后，不法分子还可以将系统作为踏板，对其他相同网段的网络终端进行攻击。

3 远程办公与在线教育中的网络安全风险防范对策

3.1 普通用户视角的安全风险防范对策

从普通用户的角度出发，网络安全风险防护只能坚持以预防为主的防护原则，因为绝大多数的普通用户在面对网络攻击时，并不具备解决网络安全问题的能力。所以在面对远程办公与在线教育期间的网络安全隐患时，要主动规避出现的网络风险，以此来降低网络威胁，并提高安全防护能力[3]。

3.1.1 计算机软件安全防护

在使用计算机时，用户可以试着在电脑中安装各种主流杀毒软件，并将病毒库的版本升级为最新版本。借助杀毒软件可以定期开展电脑全盘检查，而加装的防火墙则能阻绝部分恶意软件所带来的影响。为了避免计算机受到公共网络攻击，在非必要的情况下要关闭共享端口，并对网络共享进行处理。需要注意的是，很多人在使用计算机时，往往对各类免费杀毒软件中携带的捆绑软件记忆深刻，因此并不想在计算机中添加各种杀毒软件，这将会导致计算机遭遇网络安全风险的概率大幅提高，因此必要时可以通过购买主流收费软件等方式来加强对计算机系统的安全防护。

3.1.2 坚持从正规渠道下载各类软件

在远程办公与在线教育期间，用户往往需要安装要求来下载各类系统软件，不同单位、学校所支持的软件往往各不相同，所以为了提高网络安全性，应该始终认准各类软件的官网下载渠道，不随意点击不明下载链接。若无法明确各种软件的具体安装来源，就不能轻易下载系统软件。为了避免因为重要数据丢失，还应该坚持在不同的存储介质中对自己的信息进行备份与储存。除此之外，还应该尽量避免安装公共 WIFI，并在使用 U 盘等一系列存储介质时关闭自动播放功能，以此来降低安全风险的发生概率。

3.1.3 加强邮箱安全管理

为了避免钓鱼邮件所带来的影响，普通用户可以将自己的邮箱账号与手机号进行绑定，这样有利于及时发现不法分子的异常登陆问题，发现异常登陆之后要立刻修改邮箱密码，通过设置高强度密码可以有效加强邮箱的安全防护能力。与此同时，在邮箱使用过程中，应该养成不随意点开不明邮件的习惯，通过对不明邮件保持自己的警惕心理，可以有效避免因为钓鱼邮件而对计算机网络造成影响。如果某个熟悉的邮箱地址突然发来了邮件，可以试着通过电话以及其他沟通方式来进行了解，避免因为伪装邮箱而导致网络安全风险的发生。需要注意的是，在发送各种重

要邮件时，应该注意对邮件进行加密，并利用手机、短信等方式来告知收件人邮件的解锁密码，这样不仅可以降低邮箱风险，还可以避免收件人点击其他可能存在的钓鱼文件。

3.1.4 计算机接触恶意软件后的应急处理

如果用户确定了计算机的接触到了恶意软件，就应该第一时间拔除网线并将计算机断网，通过将计算机与其他同网段的电子设备物理隔离，可以有效防止不法分子通过计算机攻击其他电子设备。在此期间，如果发现了计算机内存在未加密的重要文件，可以选择利用关机等方式来防止损失继续扩大。如果重要文件均已加密，就可以继续保持计算机的开机状态并联系专业人员来开展恢复处理。如果存在重大影响，应该主动联系网信部门[4]。

3.2 网络安全风险控制对策

3.2.1 网络安全防范中的入侵检测优化

机器学习技术的发展让各种算法与模型应用到了各个领域，网络安全领域同样可以借助机器学习来提高网络安全性。在入侵检测中，随机森林是较为成熟的集成算法，但是却存在泛化能力不足等缺陷。在对入侵检测进行优化时，可以结合果蝇优化来对算法进行调整。调整后的算法在运行期间可以收集网络入侵数据，然后借助遗传算法来对网络攻击进行特征提取，此时就可以对随机森林决策树数目、选择分类属性来进行分析，并找出随机森林的最优算法，然后将优化后的随机森林算法与网络攻击流量中的数据别瞎扯进行分类对比，能够从横向对比中发现网络数据中的各种异常情况，进而达到实现入侵检测的目的。从入侵检测的原理角度出发，可以将入侵检测看作分类问题，入侵检测可以将网络数据划分为不同分类，结合所使用的算法来分析数据集中的异常情况，进而达到提前发现网络风险的作用。

3.2.2 网络安全防范中的态势感知优化

网络技术进步让网络攻击逐渐变得愈发复杂，态势感知技术的出现，其目的就是对整个网络的安全情况进行检测，通过提前对异常进行态势感知，可以提前进行风险预防。若态势感知技术不足，就很难实现事先预防，所以应该对态势感知进行优化，以此来让网络安全防范效果得到进一步提高。

在对态势感知进行优化时，可以借助 BP 神经网络技术来进行针对性优化，通过在态势评估阶段加入采用附加动量法与自适应学习的 BP 神经网络算法，可以让感知效果大幅提高。该算法相较于传统 BP 神经网络而言，其反馈误差速度将会得到大幅提高，能够避免因为态势感知速度过慢，而导致态势感知成为网络安全管理期间的“摆设”。需要注意的是，由于态势评估指标可以直接反映出系统可行性，所以评估指标的选择极为关键，若网络数据相对比较复杂，可以试着选取更多的态势评估指标来提高态势感知精度[5]。

3.2.3 网络安全防范中的关联分析优化

关联分析的主要算法为 Apriori 算法，通过利用该算法挖掘网络数据中的频繁集项，可以找出网络异常数据。传统关联分析在挖掘期间往往会产生大量候选项目集，这将会导致的算法开销大幅提高，而且在面对目标事务库时，还会在遍历期间扫描很多无效记录。通过对关联分析进行优化，可以对 Apriori 算法进行调整，通过将目标事务库中的各种无效、项目是 1 的记录删除，并在出现候选项目集后优先开展剪枝作业，可以大幅降低关联分析期间的数据规模，算法性效果将会有所增加。在算法挖掘期间，应该更多关注数据之间的关联情况，这样便可以在遍历目标事务库时将仅仅只有一个项的记录删除，提高算法效率。除此之外，因为该算法在应用期间往往需要循环对目标事务库进行扫描，这会导致 I/O 开销激增，所以通过在初次扫描中删除各种无关记录，可以实现对 I/O 开销的合理优化。

4 结论

总而言之，在远程办公、在线教育期间难免会遇到网络安全隐患，通过对网络安全风险进行分析并提出应对思路，可以让用户在使用网络时变得更加安全，降低网络风险所带来的负面影响。相信随着过多人意识到网络安全隐患的恶劣影响，网络安全防范将会变得越来越简单。

[参考文献]

[1]苏泳睿,赵玲.复杂网络视域下在线教育用户选择行为特征研究[J].继续教育研究,2022(5):85-90.
[2]孔欣怡.远程办公、在线教育中的网络安全隐患与防范对策[J].网络安全技术与应用,2022(3):20-21.
[3]方贤洁,卢毅刚.新闻学在线教育的契机、模式与进路——基于 SCP 模型分析新闻学课程网络在线教学范式转型[J].传媒,2020(21):85-87.
[4]魏玉峰.浅析远程办公网络安全风险与防护措施[J].网络安全技术与应用,2020(4):31.
[5]朱莉茹,云龙.创新业态 开食品安全网络教育先河——中安食品安全培训网为保障食品安全助力[J].中国食品,2018(15):92-93.

作者简介：杨帆（1981-）男，汉族，重庆人，成都理工大学电子信息科学与技术专业本科毕业，现就职于重庆市教育信息技术与装备中心，担任该中心信息技术部副主任。