

Research on Computer Network Security and Preventive Measures in the Era of Big Data

Yongrui Wang

Beijing ByteDance Technology Co., Ltd, Beijing, 100086, China

【Abstract】 In the era of big data, computer and network technology have long since penetrated into all aspects of human society, providing quite a lot of convenience to human daily life. However, these conveniences are not without a cost. The frequent occurrence of information leakage, online fraud, network violence, cyber crime and other information security problems has also affected people's normal work and life to a certain extent. To promote the computer and network technology to better serve mankind, we must actively strengthen the management of computer network security. This paper intends to study this and provide some preventive measures according to the current situation.

【Keywords】 computer network security; third-party payment; big data; precautions

大数据时代的计算机网络安全及防范措施研究

王勇睿

北京字节跳动科技有限公司, 中国·北京 100086

【摘要】 大数据时代, 计算机与网络技术早已渗入了人类社会的方方面面, 给人类的日常生活提供了相当多的方便。不过这些便利并非没有代价, 信息泄漏、网络诈骗、网络暴力、网络犯罪等信息安全问题的频频出现, 也一定程度上影响了人们的正常工作生活。要推动计算机与网络技术更好地为人类服务, 必须积极加强计算机网络安全管理工作。论文拟对此进行研究并根据当前情况针对性地提供一些预防措施建议。

【关键词】 计算机网络安全; 第三方支付; 大数据; 防范措施

DOI: 10.26549/bdai.v3i3.11822

1 引言

现如今, 信息化时代正在全面来临, 人类通过电脑与互联网信息的应用, 全面提升了工作能力、学习效果和生活品质, 但也因为互联网环境信息高度公开的特点, 难以避免出现个人隐私信息的泄露, 与此同时, 也有很多不良分子借助计算机网络技术进行诈骗, 衍生出很多网络违法行为, 而这些情况的发生都会严重危害人类的生活品质, 造成人类的财产和精神损失。在这样的时代背景下, 人们必须主动增强自己的网络安全意识, 政府有关部门必须主动提高安全管理水平, 一起建设具备良好风气的互联网环境, 使互联网更好地服务于人类生活。

2 大数据下的计算机系统安全风险评估

2.1 人们网络安全意识不足

计算机网络技术的迅速发展和运用极大改变了我们的日常生活, 大部分人在享受计算机网络技术所提供的便捷的同时, 忽视了他们所面临的安全隐患, 即缺乏了相应的计算机网络安全意识。许多不法分子利用计算机网络技术来非法掌握个人信息进行网上欺诈。比如有不少人由于不良的网站访问习惯或非正

规注册等原因造成了自身隐私信息泄露, 在与掌握了这些泄露隐私资料的犯罪分子接触时很容易轻信进而受到财产欺诈。在大数据时代里, 民众的切身利益已和互联网世界紧密的绑定在一起, 如果缺乏足够强的互联网安全意识, 则民众的财富安全, 甚至是人身安全都将不能得到保证^[1]。

2.2 网络垃圾信息泛滥严重

在互联网技术高速发展的大数据时代背景下, 广告行业也享受到了技术发展的红利, 利用互联网技术能够更大范围地开展广告业务的同时, 还拥有受众多、成本小的优势。在这样的背景下, 各种广告信息频频地出现在我们的视线中, 与此同时因为行业的监督程度有限, 使得网上垃圾广告严重泛滥, 极大限度挑战我们辨别真假信息的能力, 人们只要辨别真假信息的能力不足就有可能被人欺骗, 因此, 网上垃圾信息的泛滥成为当前一种相当严峻的网络安全难题^[2]。

2.3 网络违法犯罪行为猖獗

现如今, 人类很多重要的生产生活事务都通过互联网来进行, 包括利用互联网上学、上班和消费等, 这也给互联网犯罪提供了可乘之机, 利用互联网实施犯罪有着较好的隐秘性, 这也导致互联网犯罪越来越猖狂。特别是针对部分掌握了高级互联网信息技术的罪犯来说, 其可以利用互联网途径轻而易举地

【作者简介】 王勇睿(1979-), 男, 中国吉林长春人, 硕士, 从事第三方平台支付、消费金融、金融业务风控、计算机技术算法研究。

掌握个人隐私信息,包括身份证号、密码等,进行网络欺诈等犯罪活动,互联网犯罪得肆虐对人民的财富安全构成了极大挑战^[3]。

2.4 网络黑客技术发展迅猛

在互联网科技高速发展的今天,我们对互联网的了解日益加深,同时也日益认识到掌握高端互联网科技的必要性。由于利用互联网等高端技术手段进行非法操作所获取的收益往往远比一般工作所获取的收益还要大,于是有更多的投机分子纷纷加入了黑客队伍,钻研黑客技术。在这样的形势下,随着互联网黑客技术的发展日益快速,也更容易对国家安全的重要领域构成冲击与威胁,使得越来越多的大企业与大公司频繁遭遇互联网黑客技术入侵,造成大量损失。

2.5 第三方支付平台信息安全保障中存在的问题

2.5.1 网络违法犯罪问题

因为第三方支付系统在使用过程中往往具有一定的隐蔽性,而交易当事人也有可能在网上隐瞒了自身的真实信息,这也导致了第三方支付系统在实际使用过程中,很难逐一核查交易当事人的真实身份资料 and 所支付资金的来历和去向。第三方支付系统也因此很容易沦为非法分子所使用的工具,主要用来实现资金的非法流转、洗钱、行贿和欺诈等行为。同样,使用第三方支付者也可能实行刷卡套现,不法分子可能采用刷卡套现来规避相应利息费用,或者无偿地侵占了商业银行的信用资本。而最终结果,正是因为中国目前对第三方支付的监管出现了问题,商户可以借助对商业、税收部门的监管漏洞,以个人名义从事商业贸易,从而规避税费,让整个国家蒙受巨大的经济损失^[4]。

2.5.2 网络安全问题

第三方支付实质上是一个网络银行的付款手段,这样就必然地要面对黑客攻击、网络病毒和网络系统崩溃的危险,就算第三方支付体系具备庞大的安全维护中心,也无法完全避免安全漏洞的出现。

2.5.3 信息泄露问题

近年来,用户在网络的个人资料遭遇泄露的事件频发。在出现严重网络问题和重大网络违法犯罪事件的前提下,怎样保护消费者权益,减少第三方支付经营风险和投资风险对消费者权益的危害,防止第三方支付平台通过科技和网络优势侵害消费者权益,是中国第三方支付企业在成长进程中必须妥善解决的重点问题。

3 大数据时代下计算机网络安全防范措施

3.1 强化人们的网络安全意识

大力增强民众的网络安全意识是有效预防网络安全案件的有力措施,只有当民众在上网时保持清醒的头脑以及较强的预防能力,包括有效地抵御各类互

联网威胁和清晰的识别各种互联网常识,犯罪分子才没有可乘之机。民众网络安全意识的提高主要应该通过以下三个层面来努力实现,首先互联网使用者必须积极主动地去掌握各种互联网常识,形成良好的上网习惯,如不访问违规网站,不登录莫名账号等。其次,政府部门及其互联网治理机构必须主动利用互联网宣传来帮助民众提高网络安全意识,在这一任务中,推广方式可以是线上的宣传,也可以是线下的互动推广,同时宣传重点必须包括怎样准确识别虚假互联网内容、怎样合理开展网络应用以及当出现安全问题后需要怎样有效解决等。最后,政府部门及其有关机构必须加大对互联网平台的监管,包括加强对各大平台的审查,以及加大不良信息的管理措施等。这样,经过人们的自主学习与全民性的安全教学和管理,就能够有效增强人们的网络安全意识,从而有效减少安全事故的发生率,进而使计算机与网络等科学技术更好地服务于人类的日常生活。

3.2 做好漏洞扫描及补丁工作

人们在使用电脑的时候,多多少少都会存在着一些漏洞问题,而这种漏洞问题往往就是不法分子用来入侵人们计算机、盗取个人隐私信息的主要途径,因此,充分进行电脑漏洞扫描和补丁工作是十分必要的。首先,当出现电脑资料泄漏问题的时候就必须安装和执行正确的漏洞补丁程序,以此来保障自己电脑的上网操作安全性。然后,还必须充分地利用当前的中高端计算机技术来设计科学完备的电脑防护程序,以便更为合理地对电脑漏洞问题进行扫描和修补。最后,安全管理者还必须主动获取计算机入侵信号,以便做好统筹分析,并将分析结论作为今后的安全防范措施地执行支点。因此,必须全面进行计算机系统漏洞扫描和补丁工作,才能有效维护所使用计算机系统的安全,从而最大化减少使用者的权益损失^[5]。

3.3 科学合理的应用杀毒软件

采用完善的电脑防护体系设计,就可以有效防止不良信息的侵入,从而有效提高互联网应用的安全程度。而电脑防护体系一般都是由杀毒软件、攻击防范体系和防火墙系统所构成,其中对杀毒软件的使用也必不可少。而杀毒系统一般都包括了自动升级、病毒扫描、病毒清理以及数据恢复和流量管理等功能,可以有效防范侵入电脑的木马程序和病毒,从而有效地保护计算机安全。也因此,我们在应用计算机的同时也必须合理地使用杀毒软件,并借此提高互联网安全指数。具体来说,我们必须选用专业公司制作的正版杀毒软件,对杀毒显示的警告内容引起高度关注,同时经常通过杀毒软件对电脑进行彻底地杀毒,这样才能有效保证计算机的应用安全性和个人隐私信息系统的的天性。

3.4 积极做好黑客的入侵防范

黑客往往是握有高超计算机技术的不法分子,对人类安全使用计算机网络的威胁性极大,如果遭遇黑客的入侵将会面临极其巨大的经济损失,因此,积极进行对黑客的入侵预防工作是十分必要的。首先,必须积极增强网络安全管理部门人员对黑客的预防能力,即安全管理者必须积极通过专业培训来提高自身对黑客的认识能力,如黑客的各种攻击方式,以便于在平时的安全管理中及时发现黑客行为并予以拦截。其次,也必须积极增强网络安全管理部门人员的计算机应用技能,如业务技能。在这一方面的工作上,各单位必须定时对人员进行业务培训,使他们了解更为先进的计算机技术,并且具备更加端正的技能素质,以便更好地进行安全管理。最后,安全管理单位必须积极联系众多高级计算机人员共同进行更高层次防火墙的研发建设工作。如此,通过积极进行上述三个层面的操作,才能有效防止黑客侵入,充分保障我们的计算机网络应用安全。

3.5 加强严厉打击力量,有效净化网络自然环境

现如今互联网犯罪层出不穷,不仅与互联网科技的高速发展密切相关,也与对互联网犯罪行为的打击程度不足密切相关。如果有关部门对互联网犯罪缺乏足够分量的严厉打击力量,就不能对互联网犯罪行为投机分子产生强有力的震慑,难以达到有效的互联网生态净化作用。因此,政府部门及其有关单位必须全面加大互联网犯罪的打击力度,呼吁社会各界人士共同发力,对互联网犯罪开展举报。政府部门应该制定出内容更为详尽及惩罚幅度更大的互联网犯罪打击措施和机制,通过这些机制的建立和全民参与,对互联网犯罪围追堵截,才能有效减少互联网犯罪的风险,为社会营造出一个安全、文明、和谐的网络环境。

3.6 强化第三方支付安全

3.6.1 第三方支付系统要将客户安全保障作为首要任务

由于网络技术的高速发展,网络金融问题也被网络消费者们不断提起,所以第三方支付平台应该将用户安全保障放在首位。只有将用户的安全防护放在首位,作为第一任务才能在出现个人信息泄漏情况时,更好地维护个人用户的合法权益,同时,要把个人用户安全防护作为首要任务,如果发觉有非法商户在开展不法行为,就要予以严厉打击,并以此来有效净化第三方支付平台的环境。

3.6.2 第三方交易平台应完善安全防范保护技术

第三方支付平台对网络安全的维护不仅仅是单方面对互联网消费者负责,还是对公民诚信与公民形

象的展现。所以第三方支付平台也应该完善自身的安全防范与保护技术,方法一是通过构建系统的防护制度,来防范、监测与减少计算机病毒对网络安全的威胁;二是通过引入各种安全机制与运行管理系统相结合,来达到对第三方电子支付平台数据库的安全性保障;三可以是通过数据加密、密钥等技术手段,对电子付款时的数据传输实施密码管理;四可以采用加强认证、鉴别用户权限与禁止公共网站注册平台等技术措施和管理手段,来实现保障安全的目的。

3.6.3 建立健全完整的律法规范,明晰第三方支付平台的法律身份和职责

从立法方面考虑,由于与第三方电子支付平台所履行的法定身份和法律责任相应的立法规定还没有完成,且现行政策所规定的立法地阶也不高,而法规的修订又是一个比较漫长的过程,所以可从以下两个方面暂时性处理此问题,一是为了提高现出台相应政策性法规机关或组织的立法地位,使其所出台的相应政策性法规更具有国家强制性;二是在可实现地方推广或在本地方实现的有关规章制度以及法律性文件中,其结果往往是依赖于中国人民代表大会出台一个与此相应的法律条文,以确定第三方支付平台的法定身份和责任范围,以永久地解决此问题。

4 结语

综上所述,在大数据时代背景下,主动改善电脑安全性是十分必要的,这既是对人类财产安全的保证,更是对人类幸福生活的保证。在具体的实施过程中,政府必须通过积极地增强人民的网络安全意识,并充分地进行计算机系统漏洞扫描、补丁修改和黑客侵入等工作来有效地预防安全事故的出现,并以此构造出一种安全可靠的互联网应用环境,从而使互联网更好地为人类服务。

参考文献

- [1] 吴家存.试谈大数据时代的计算机网络安全及防范措施[J].网络安全技术与应用,2022(04):69-70.
- [2] 常祖国.探讨大数据时代的计算机网络安全及防范措施[J].网络安全技术与应用,2022(03):173-174.
- [3] 徐贝加.基于大数据时代的计算机网络安全防范措施研究[J].网络安全技术与应用,2022(02):68-69.
- [4] 庞涛.大数据时代的计算机网络安全及防范措施[J].数字技术与应用,2022(01):225-227.
- [5] 孙政伟.大数据时代的计算机网络安全及防范措施研究[J].网络安全技术与应用,2022(01):53-54.