上海市民个人信息安全素养评价研究

罗 力
(上海社会科学院 信息研究所,上海 200235)

摘要:信息安全已成为信息时代国家总体安全的基石。个人信息安全是保护个人隐私和财产的必然要求。文章对个人信息安全和信息安全素养的内涵进行剖析,运用问卷调查法对上海市民个人信息安全状况、个人信息安全环境、个人信息安全意识、个人信息安全能力等 4 个方面进行评价,发现上海市民遭遇个人信息安全侵害的频率较高,但损失程度不大;他们的个人信息安全意识有待提高,个人信息安全能力一般,尤其是大部分市民的密码设置能力有待加强。

关键词:个人信息安全;信息安全素养;信息安全意识;信息安全能力;评价
中图分类号:G203 **文献标志码**:A **文章编号**:1008-5831(2013)03-0095-05

21 世纪人类社会已然迈进了信息时代,信息成为促进社会经济、科学技术以及推动人类社会发展的重要因素。与此同时,信息安全的重要性日益凸显:从最高层次来讲,信息安全关系到国家的安全;对组织机构来说,信息安全关系到组织机构的正常运作和持续发展;就个人而言,信息安全是保护个人隐私和财产的必然要求。中国共产党十六届四中全会已将信息安全列入国家安全的四大重要组成部分之一。海因里希经过大量的研究,认为各种安全事故存在“88102”规律,即 100 起安全事故有 88 起纯属人为,10 起为人和物的不安全状态综合造成的,只有 2 起是难以预防。在 RSA2011 信息安全大会上,不少信息安全专家不约而同地提出了一个引人关注的问题,即众多缺乏安全意识的员工,正在成为黑客突破企业安全防护时,最大也最难修补的漏洞[1]。人员要素已经成为国家、城市和组织机构信息安全保障体系建设的一个重要组成部分。人员信息安全素养的培养在其日常工作和生活中处于十分突出的位置。笔者期望在调查研究的基础上,对上海市民个人信息安全现状和信息安全素养进行实证调查,为进一步开展信息安全素养理论研究、探讨市民信息安全素养教育的迫切性和具体制定相关政策提供真实的依据。

一、个人信息安全和信息安全素养的内涵

关于个人信息的概念,国内尚无法律依据,也无统一定义。1995 年的《欧洲联盟数据保护规章》认为个人信息是有关一个被识别或可识别的自然人(数据主体)的任何信息。可识别的自然人是指一个可以被证明,即可以直接或间接地,特别是通过对其身体的、生理的、经济的、文化的或生活身份的一项或多项的识别[2]。2003 年开始着手研究并于 2005 年推出的《中华人民共和国个人信息保护法示范法草案学者建议稿》指出,个人信息是指自然人的姓名、出生年月日、身份证号码、户籍、遗传特征、指纹、婚姻、家庭、教育、职业、健康、病历、财务情况、社会活动及其他可以识别该个人的信息[3]。个人信息与隐私存在联系,但不可简单等同。个人信息安全则是指确保个人信息不被泄露、盗用、滥用、删除、修改、伪造等,仅为那些被授权者获取使用,且处于安全可控状态。

收稿日期:2013 - 02 - 12
作者简介:罗力(1982 -),男,浙江省台州人,上海社会科学院信息研究所助理研究员,博士,主要从事信息计量与信息安全研究。

信息安全素养则是指人们在信息化条件下对信息安全的认识,以及针对信息安全所表现出的各种综合能力。素养被认为是经常修习的涵养,也指平日的修养。素养的形成有一个程度变化的过程,即从低到高逐步发展的过程[4]。信息安全素养的概念主要是源自日常信息安全管理的需要,较大程度上受到信息安全意识概念的影响,同时与目前比较流行的信息素养概念密切相关。信息安全素养内涵丰富,不仅包括信息安全意识,还包括后续各种防护能力、信息伦理道德和法律法规知识等内容。

二、数据来源

综合国内外对信息安全素养内涵的界定以及笔者提出的《国民信息安全素养评价指标体系》[5]中的17 个指标,笔者利用德尔菲法确定了问卷内容,共34 个问题,其中单选题 23 个,多选题 11 个。整个问卷内容涉及市民个人信息安全状况、个人信息安全环境、个人信息安全意识、个人信息安全能力等 4 个方面。

本次问卷主要通过上海市各个区县图书馆发放,共发放问卷 1 100 份,回收 1 080 份,有效问卷1 061份。本次调查时间为:2012 年 6 月 1 日至 9 月30 日。本次调查涉及上海 17 个区县的 1 061 个市民,受调研的市民男女性别比例分别为 48.4% 和51.6%,具体人数为 514 人和 547 人,涵盖了各行各业,有学生、工人、商业服务业职工、私营企业主、自由职业者、企事业单位职工、专业技术人员、党政机关干部以及下岗失业人员(无业或待业)等。受访者的教育程度中大专占 27%,本科占 40.3%。从年龄段看,21 ~30 岁的占 36.2%,31 ~40 岁的占20.9%,41 ~50 岁的占 17.3%。本次调研对象之所以选择上海市民,主要是因为上海信息化发展水平在全国范围内遥遥领先,各种信息化基础设施和应用比较普及,同时信息安全事件也相对较多,这样的分析结果具有发展性和前瞻性。

三、上海市民个人信息安全现状

(一)个人信息安全侵害的内容、形式和途径

个人信息安全侵害的内容是指日常生活中哪些个人信息会受到侵害。调查结果显示,个人联系方式、个人自然情况和家庭地址受到侵害的比例分别是 37.20%、20.20% 和 14.60%,位列前三位。个人联系方式是指个人的电话号码、手机号码、电子邮箱、QQ 号等信息。个人联系方式的侵害往往会使个人处于垃圾信息的包围中,经常会被匿名电话、匿名短信和垃圾邮件骚扰,甚至会被他人冒用个人身份实施欺诈等犯罪行为。个人自然情况是指个人的姓名、性别、年龄等信息。家庭地址是指个人的居住位置信息。身份证号码、工作信息和银行卡信息紧随其后,分别是9.80%、6.90% 和 6.30%,其中身份证号是指用于证明持有人身份的证件信息,一般特指中华人民共和国居民身份证信息。中华人民共和国公民在入学、就业、办理个体营业执照、提取汇款、邮件、参加社会保险等事务中均需提供有效身份证信息。身份证号的侵害往往会是持有人本身遭遇办理上述等事务的不便,甚至财产和生命损失。工作信息是指工作单位名称和地址。

个人信息安全侵害的形式包括信息泄露、盗用、滥用和伪造等。信息泄露是指让人知道了不该知道的个人信息,这是个人信息安全侵害的最基本形式,具体包括通过 U 盘、移动硬盘等拷贝泄露,通过有线、无线网络等传输泄露,通过纸质材料外带泄露以及自行在网络平台上发布与个人信息有关的内容而被他人有目的地搜集。信息盗用是指未经同意或批准而非法获取并使用个人信息,这经常发生在信息泄露之后。信息滥用是指没有限制地使用个人信息。信息伪造是指无权限人假冒他人的个人信息。调查结果显示,信息泄露的现象最为严重,比例为60.30%,其次是信息滥用,比例为 19.40%,信息盗用位居第三位,比例为 14.70%。

个人信息安全侵害的途径包括网络、商业机构、政府部门、公益机构和个人等。调查结果显示,其中商业机构、网络被认为是个人信息安全侵害的最主要的两种途径,比例分别为 39.20%、35.70%,而个人、公益机构和政府部门的比例则较低,分别是9.80%、6.60% 和 6.20%,这与目前商业机构普遍缺乏行业自律以及信息安全管理水平较低密切相关。

(二)个人信息安全侵害的频率和损失程度

个人信息安全侵害的两个主要形式是信息泄露和信息滥用,骚扰电话和垃圾短信是其最直接的表现形式。调查结果显示,97.4% 的受访者表示曾经收到骚扰电话或者垃圾短信。在关于每周接到骚扰性、欺骗性电话频率的调查中,57.1% 的受访者认为会偶尔接到骚扰性、欺骗性的电话,33.0% 的受访者认为经常接到类似电话。而在关于每周收到垃圾短信频率的调查中,48.8% 的受访者认为会经常收到垃圾短信,34.7% 的受访者认为会偶尔收到垃圾短信。由此可见,垃圾短信和骚扰性欺骗性电话的频率相当高,其中垃圾短信尤为严重。目前,垃圾短信和电话主要包括以下三种:第一是指具有违法犯罪信息内容的短信和电话,如办假证、卖枪支等违法信息;第二是指未经接受者同意而发布的具有广告性质的信息和电话,如某某公司通过短信和电话推销其新产品或服务;第三是指具有骚扰、报复等性质的信息和电话,如某人为报复某人恶意进行短信和电话骚扰。垃圾短信和电话的危害比较明显,比如利用短信进行勒索、诈骗的违法犯罪活动日渐猖獗,一些居心叵测、别有用心的人利用短信传播不实消息和谣言,在群众中造成大面积恐慌,搅得人心惶惶,境外少数敌对分子企图利用电话编造、散布各种谣言,引发社会恐慌,破坏社会稳定。

在关于个人信息安全侵害所造成的损失程度调

查中,36.9%的受访者认为损失程度轻微,36.1%的受访者认为损失程度一般,而11.7%的受访者认为无法评估其损失程度,只有8.9%和2.9%的受访者认为损失程度严重和很严重。调查结果显示,目前个人信息安全侵害的总体损失程度不严重,一方面是因为与个人信息安全泄露等行为尚未正式形成伤害有关,另一方面是因为部分损失程度主要是精神层面,尚未以物质形式体现出来。

(三)个人信息安全侵害的原因

个人信息安全受到侵害的原因,既有主观因素,比如个人信息安全意识淡薄,也有个人信息安全环境因素,比如信息安全产品功能不足、各种组织机构管理不善、买卖个人信息等。调查结果显示,42.2%的受访者认为个人信息安全环境不太安全,26.8%的受访者认为个人信息安全环境一般,19.3%的受访者则认为非常不安全,另有7.7%和1.5%的受访者认为比较安全和非常安全。从数据可以看出,大部分受访者对个人信息安全环境的认知倾向于不安全。信息安全立法、执法未到位,各种组织机构管理不善和买卖个人信息占据了个人信息安全受到侵害原因的前三位,比例分别是23.90%、22.10%和21.70%,个人信息安全意识淡薄位居第四位,比例为13.90%。至于信息安全产品功能不足、信息安全人才不够以及他人好奇心的比例均在10%以下。

个人信息安全意识淡薄的一个重要原因是缺乏信息安全知识普及教育。信息安全知识普及教育的形式有多种,且需要高校、非营利性组织和信息安全企业通力合作。调查结果显示,目前信息安全知识普及教育的供给非常缺乏。57.5%的受访者从来没有接受过类似教育,25.2%的受访者不定期地接受类似教育,10.6%的受访者在刚进工作单位时接受过类似教育,只有2.8%的受访者定期接受过类似教育。

四、上海市民个人信息安全素养现状

(一)上海市民个人信息安全意识现状

个人信息安全意识具有丰富的内涵,一方面是个人对信息安全问题的全面反映,包括感性认识和理性认识。感性认识层面是指对信息安全问题的基本态度和信息安全现状的情感体验;理性认识层面则是指对信息安全问题的认知,包括对信息安全的重要性、内涵、威胁来源、实现途径等方面的认知。另一方面是关心和维护信息安全的意识取向,具体表现为忧患意识、防范意识、责任意识、保密意识等。

1. 个人信息安全保护范围认知

在对个人信息安全保护范围认知的调查中,身份证号码、银行卡信息和联系方式是市民最为认可的三项,比例分别是16.70%、13.9%和13.4%。家庭地址、个人医疗信息和工资收入的比例分别是12.50%、11.90%和10.60%。选择个人自然情况和工作信息的比例相对较小,分别是10.4%和10.00%。

2. 主动学习信息安全知识的意愿

主动学习信息安全知识的意愿是个人信息安全意识中非常重要的组成部分。调查结果显示,69.0%的受访者只是偶尔关注过该方面的知识,19.3%的受访者则从来不关注这方面的知识,9.0%的受访者则非常关注该方面的知识。在一定程度上说明,在个人信息安全形势非常严峻的背景下,受访者关注个人信息安全知识的意识不强。

3. 接受信息安全意识教育的意愿

个人信息安全意识淡薄的一个重要原因是缺乏信息安全知识普及教育。信息安全知识普及教育的形式有多种,且需要高校、非营利性组织和信息安全企业通力合作。调查结果显示,目前信息安全知识普及教育的供给非常缺乏。57.5%的受访者从来没有接受过类似教育,25.2%的受访者不定期地接受类似教育,10.6%的受访者在刚进工作单位时接受过类似教育,只有2.8%的受访者定期接受过类似教育。79.5%的受访者认为有必要加强个人信息安全意识教育,11.5%的受访者则持无所谓的态度,认为这种教育与自己无关,5.2%的受访者则认为该教育没有任何必要。

4. 了解网站和机构的个人信息安全保护政策的意愿

目前个人会在很多网站和有关机构提交个人信息。这些网站和机构的用户个人信息管理政策备受用户关注,比如某网站在用户申请注册时会告知相应隐私保护政策。对于这些网站和机构的个人信息安全保护政策和各种公告是否主动了解,能在一定程度上反映其个人信息安全意识的强弱,因为他们所提供的政策和公告在一定程度上反映了他们对于市民个人信息安全保护的态度和政策。这些政策和公告可以成为市民在日后个人信息受到侵害时寻求救济的一个重要途径。调查结果显示,65.3%的受访者只是偶尔关注这方面的信息,22.9%的受访者从来没有关注,而7.2%的受访者则特别关注且采取了相应措施。调查结果反映出受访者对网站和有关机构在用户个人信息管理方面的政策和公告不是很重视。

5. 个人信息安全法律法规的认知

46.7%的受访者认为并不了解中国个人信息安全保护的法律法规,43.3%的受访者认为有部分了解,只有8.0%的受访者认为比较了解。反映出个人对有关法律法规的了解不到位,同时有关法律法规的制定和宣传普及工作有待加强。另外,85.0%的受访者认为应设立《个人信息安全保护法》。这一呼声与市民认为目前个人信息安全受到侵害的原因中信息安全立法、执法未到位相呼应。

6. 救济渠道的认知

当个人信息安全受到侵害后,受访者寻求的解

决办法通常有不予理睬、自行解决、向公安机关报案、媒体曝光等。在本次调查中,63.9% 的受访者选择不予理睬,21.3% 的受访者选择自行解决,只有 2.6% 和 1.7% 的受访者选择向公安机关报案和进行媒体曝光。这一方面跟目前信息安全侵害所带来的总体损失程度不严重有关,另外也跟目前社会上尚未培育信息安全侵害问题救济渠道有关。

7. 个人信息安全侵害的原因认知

个人信息安全受到侵害的原因,既有主观因素,比如个人信息安全意识淡薄,也有个人信息安全环境因素,比如信息安全产品功能不足、各种组织机构管理不善、买卖个人信息等。调查结果显示,42.2% 的受访者认为个人信息安全环境不太安全,26.8% 的受访者认为个人信息安全环境一般,19.3% 的受访者则认为非常不安全,另有 7.7% 和 1.5% 的受访者认为比较安全和非常安全。数据显示,大部分受访者对个人信息安全环境的认知倾向于不安全。信息安全立法、执法未到位,各种组织机构管理不善和买卖个人信息分别占据了个人信息安全受到侵害原因的前三位,比例分别是 23.90%、22.10% 和 21.70%,个人信息安全意识淡薄位居第四位,比例为 13.90%。至于信息安全产品功能不足、信息安全人才不够以及他人好奇心的比例均在 10% 以下。

(二)上海市民个人信息安全能力现状

个人信息安全能力是个人信息安全素养的重要组成部分,也是个人信息安全素养最终得以表现的形式,其内容包括正确设置密码确保信息私密性、防范计算机网络犯罪和计算机病毒等恶意攻击、防范垃圾信息的入侵(如垃圾短信、邮件等)、从多渠道获取解决个人信息安全问题的手段等。调查结果显示,55.9% 的受访者认为自身的个人信息安全保护能力一般,19.7% 的受访者认为自身的个人信息安全保护能力较强,10.6% 的受访者认为自身的个人信息安全保护能力较低,5.6% 的受访者认为自身的个人信息安全保护能力很强,4.1% 的受访者则认为自身的个人信息安全保护能力很低。总体来说,受访者对其自身的个人信息安全保护能力持正面乐观评价。

1. 个人密码设置能力

密码设置和保护是个人信息安全能力的重要内容,它包括是否在多个设备或网络服务上使用相同账号和密码、更换密码的频率以及是否会对电脑重要业务文件和数据设置密码。如果在多个设备或网络服务上使用相同密码,则会使个人信息安全侵害的风险大大增加。2011 年末大规模用户信息泄露事件的主要原因就是用户在多个设备或网络服务上使用相同密码。当其中一个账号和密码泄露后,则其他设备或网络服务对于他们来说是不设防的。调查结果显示,35.1% 的受访者使用大部分相同或相似的密码,32.1% 的受访者使用少部分相同或相似的密码,5.5% 的受访者使用完全相同的密码,而 24.8% 的受访者使用完全不同的密码。反映出相当部分的市民存在着一号多用的账号和密码现象。

更换密码的时间间隔是密码设定和保护的另一个重要指标。调查结果显示,63.1% 的受访者更换密码的时间间隔在半年以上或从不更换,14.6% 的受访者更换密码的时间间隔在 3 至 6 个月,7.4% 的受访者在 1 至 3 个月内会更换密码,只有 3.7% 的受访者会在 1 个月内更换密码。较低的密码更换频率潜藏着当密码泄露后遭遇各种损失的风险。

另外,对计算机重要业务文件和数据进行密码保护是现代使用计算机的一项基本技能,其中之一是计算机登陆的密码设定,另外则是对一些重要文件设定密码,这是为了防止用户离开计算机或者计算机数据泄露时保护计算机数据。调查结果显示,46.7% 的受访者会对计算机重要业务文件和数据进行密码保护,而 39.8% 的受访者则没有这个习惯。数据显示,对计算机重要业务文件和数据进行密码保护将会是一个大的趋势,并且也是个人信息安全保护能力的一个组成部分。

2. 个人防护计算机病毒的能力

计算机病毒是个人信息安全遭遇侵害的重要威胁。当病毒进入计算机时,会删除、修改或复制重要的个人信息,甚至会远程操纵计算机,窃取重要个人信息。对计算机病毒传播途径的了解,直接影响到计算机遭遇病毒侵害的可能性,进而影响到个人信息安全。调查结果显示,受访者对计算机病毒传播途径比较了解,软件下载、U 盘和网页的比例分别是 21.0%、20.8% 和 20.2%,电子邮件和聊天工具则分别是 19.7% 和 18.4%。

升级计算机系统和病毒库有利于提升计算机性能,减少计算机病毒入侵的机会。调查结果显示,55.6% 的受访者会定期升级计算机系统和病毒库,33.6% 的受访者会偶尔升级,只有 5.9% 的受访者不会升级计算机系统和病毒库。这表明在计算机大力发展和普及的今天,市民在这方面已经逐渐养成习惯。

对于网络上来历不明的邮件、聊天工具或论坛、网页弹出的链接是否打开也是有效防护计算机病毒的一个重要环节,因为很多病毒、木马会以来历不明的邮件、弹出的链接进行伪装。如果不加选择的打开,很有可能感染病毒或木马,进而让个人信息处于不安全的情况。调查结果显示,46.1% 的受访者从不打开类似邮件、链接,30.9% 的受访者对感兴趣的邮件或者链接会打开,13.3% 的受访者不会有意打开邮件或者链接,仅网页强行打开时查看。只有 5.8% 的受访者会经常打开类似的邮件或链接。而如何处理下载的文件、软件同样属于个人防护计算机病毒的一部分,因为所下载的文件、软件很有可能被嵌套了病毒或者木马。如果不经过任何处理就直接

使用,很可能会威胁计算机的安全,进而影响到个人信息安全。52.3%的受访者会先查杀病毒再使用,20.9%的受访者会根据对网站的信任度决定,15.0%的受访者会直接使用,另有6.9%的受访者从不下载。数据显示,市民防护计算机病毒的能力较强。

3. 个人备份重要数据以及安全使用U盘的能力

对计算机中的重要信息定期备份是保护个人信息的重要手段,也是个人信息安全能力的重要组成部分。定期备份重要信息可以在电脑发生故障时有效地防止信息丢失。调查结果显示,33.4%的受访者不会定期对重要信息做备份,31.0%的受访者想起来就备份一次,28.7%的受访者会定期进行备份。这表明,对计算机重要信息定期做备份的理念还需大力宣传。

U盘是信息社会中保存个人信息的重要工具。将存有个人信息的U盘借给别人存在着恶意拷贝、信息泄露、删除和修改等风险。经统计,44.3%的受访者会在查看U盘的信息后再借出,31.0%的受访者从不把自己的U盘借给别人,13.4%的受访者则不查看U盘就直接借出,只有6.9%的受访者从不使用U盘。从数据可见,市民具有较强的U盘安全使用意识。

五、个人信息安全保护对策建议

通过对本次有效调查问卷的分析,笔者发现,上海市民遭遇个人信息安全侵害的频率较高,但损失程度不大。他们的个人信息安全意识有待提高,个人信息安全能力一般,尤其是大部分市民的密码设置能力有待加强。要有效解决个人信息安全问题,必须围绕着"人"这个安全主体,关心人的行为安全,真正做到"以人为本"打造个人信息安全环境。

首先必须提高广大市民的个人信息安全素养,包括个人信息安全意识和个人信息安全能力,这需要广大市民严格要求自己,主动学习信息安全有关知识,不能光靠"三分钟热情",而应该持之以恒。市民要严格遵守所在单位颁布的与信息安全有关的规章制度。另外对自己发布的个人信息要深思熟虑,不可随意泄露个人信息。

其次要打造全方位、立体化的个人信息安全环境,包括加紧立法、严格执法、强化社会监督和行业自律、提高信息安全技术水平、加大信息安全普及教育力度、培养信息安全专业人才等。同时各个组织机构不仅要设置信息安全规章制度与信息安全管理员职责、安装信息安全管理软件、培养组织信息安全文化,而且还要摒弃过去照本宣科的方式,采取生动、形象、简洁的方式,比如借助信息安全海报、动画视频、屏幕保护、安全手册等提供信息安全教育培训来不断强化市民的个人信息安全素养。

参考文献:

[1]从索尼数据泄漏事件看网络安全的"人祸"[EB/OL]. [2011-10-23]. http://article.pchome.net/content-1331343.html.

[2]齐爱民. 个人资料保护法原理及其跨国流通法律问题研究[M]. 武汉:武汉大学出版社,2004:4-5.

[3]齐爱民. 中华人民共和国个人信息保护法示范法草案学者建议稿[J]. 河北法学,2005(6):2-5.

[4]罗力. 论国民信息安全素养的培养[J]. 图书情报工作,2012(6):25-28,37.

[5]罗力. 国民信息安全素养评价指标体系构建研究[J]. 重庆大学学报:社会科学版,2012(3):81-86.

Evaluation of Personal Information Security Literacy in Shanghai

LUO Li

(*Institute of Information, Shanghai Academy of Social Sciences, Shanghai 200235, P. R. China*)

Abstract: Information security has become the cornerstone of the overall national security in the information age and personal information security is essential for personal privacy and asset protection. The article analyzes personal information security and information security literacy, designs a questionnaire to evaluate the status of personal information security, environment, awareness and competence in Shanghai, finding that people in Shanghai suffer a high frequency but low loss of personal information security attack. Their personal information security awareness has to be improved and information security competence is so normal, especially their ability of setting correct code should be promoted.

Key words: personal information security; information security literacy; information security awareness; information security competence; evaluation

(责任编辑　胡志平)