NASCIO Representing Chief Information Officers of the States

Research Brief

February 2005

Welcome to the Jungle:[1] The State Privacy Implications of Spam, Phishing and Spyware

Section I: An Overview

It's a Jungle Out There: In an environment in which 53% of all reported fraud complaints to the Federal Trade Commission (FTC) in 2004 were Internet-related, the Internet and email threats of spam, phishing and spyware all are real threats with real consequences.[2] They are increasingly used by criminals, instead of just novice teenage hackers[3] and can be lucrative alone or in furthering a larger criminal enterprise. Armed with these incentives, spammers, phishers and spyware purveyors are motivated and possess the expertise to avoid the attempts of law enforcement, industry and others to bring these threats in hand. Moreover, while banks, financial institutions, ISPs (Internet Service Providers) and even online auction site users have borne the initial brunt of threats like phishing, other sectors are becoming targets as the first wave of targeted sectors puts in place more effective security measures. ***This could place government and citizen information at risk of unauthorized disclosure and could lead to serious consequences, such as the release of sensitive homeland security and critical infrastructure information or personal information that could result in identity theft. In addition, spam, phishing and spyware infringe upon citizens' perceived "right to be left alone" while surfing the Internet and using email. The fact that so many individuals' privacy has been impacted to varying extents by these threats has compounded their significance.*** For example, a 2004 phishing attack spoofed[4] an email from the FDIC (Federal Deposit Insurance Corporation). It falsely claimed that the Secretary of Homeland Security had advised the FDIC to suspend all federal deposit insurance of the recipients' bank accounts[5] and sought to have users provide their personal information to the sender of the spoofed email. Healthcare agencies and entities are at risk for attacks due to their deep stores of patient information.[6]

---

[1] Title inspired by the song "Welcome to the Jungle" by rock band, Guns 'N Roses.

[2] "National and State Trends in Fraud and Identity Theft," Federal Trade Commission (FTC), February 2005, <http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf>.

[3] "Antivirus Firm Says Organized Crime Growing Online," Dan Ilett, Cnet new.com, December 9, 2004, <http://news.com.com/2100-7348_3-5486201.html>. Members of a Brazilian hacker ring had stolen around $80 million before they were arrested in 2004.

[4] Spoofing is the misrepresentation of the origin of an electronic communication, such as an email, a network or an Internet address.

[5] "Special Report on 'Phishing,'" U.S. Department of Justice, Criminal Division, 2004, <http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf>

[6] "Proposed Solutions to Address the Threat of Email Spoofing Scams," the Anti-Phishing Working Group (APWG), December 2003, <http://www.antiphishing.org/Proposed%20Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Paper.pdf>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Scope of this Brief: This brief is intended to provide the State CIOs with an overview of the privacy implications of spam, phishing and spyware and contains the following:

- **Section II:** Background on spam, phishing and spyware, including a look at the state business implications of these threats
- **Section III:** State privacy implications of spam, phishing and spyware
- **Section IV:** Update on recent activities regarding spam, phishing and spyware
- **What CIOs Need to Know & CIO Action Items:** Salient points for State CIOs
- **Appendix A:** Additional references & resources
- **Appendix B:** Tips from US-CERT (U.S. Computer Emergency Readiness Team) and the FTC (the Federal Trade Commission).

Section II: Background & State Business Impacts of Spam, Phishing and Spyware

Descriptions of Predatory Cyber-Inhabitants: While the delineating features of spam, phishing and spyware may be blurred at times, the following subsection provides an overview of each threat:

- **Spam:** Spam is the electronic equivalent of junkmail--it is unsolicited and peddles everything from prescription drugs to computer software. While spam has provided an inexpensive channel for bulk advertising, it has increased in severity from an unsolicited annoyance to a serious and costly threat that has the capability to transfer viruses, Trojans, and spyware and act as a lure in phishing attacks. Though there are many variations of the definition of spam, it usually is understood to be unsolicited commercial email. As illicit spammers have invaded the Internet space, users now may receive spam that does not have a return address, contains a fraudulent address or displays a misleading content description. According to an April 2003 report by the FTC, sixty-six percent of all email contains false "From" lines, subject lines or message text.[7]
- **Phishing:** Coined around 1996, phishing is a play on the analogy of "fishing" for personal information on the Internet. The replacement of the "f" with "ph" is a nod to an early form of telephone hacking, known as "phone phreaking."[8] A phishing attack normally has two steps: (1) a user receives an email that pretends to be legitimate and (2) the user is enticed through social engineering to click on a link to a purportedly legitimate website and asked to provide personal and other information. While there can be variations of phishing attacks, they typically involve an email that may qualify as spam and acts as a lure for a user to turn over personal information that can later be used in identity theft and fraud. Spoofed addresses, Trojans, and hijacked computers may be used to send phishing emails, and website links may install spyware and key-logger technologies with the unwitting click of a user's mouse. Organized crime operatives worldwide can use information gathered through phishing to execute high-value currency transfers or in pursuit of sophisticated identity theft schemes and credit card scams. Upwards of 20% of targeted users provide personal information as a result of a phishing scam.[9]

---

[7] "False Claims in Spam: A Report by the FTC's Division of Marketing Practices," Federal Trade Commission (FTC), April 30, 2003, <http://www.ftc.gov/reports/spam/030429spamreport.pdf>.
[8] "Proposed Solutions to Address the Threat of Email Spoofing Scams," the Anti-Phishing Working Group (APWG), December 2003, <http://www.antiphishing.org/Proposed%20Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Paper.pdf>.
[9] Ibid.

- **Spyware:** Though somewhat difficult to define, spyware is a generic class of software security threats with malicious intent that includes technologies such as keystroke-logging, malware, homepage hijacking, and adware. The hallmark of spyware is its installation on a user's computer without his or her knowledge, consent or permission while connected to the Internet. It can be transferred via spam emails or be contained in freeware, shareware or games downloaded from the Internet. Unsuspecting users may even consent to the installation of spyware with the click of a mouse in agreement to an application or program's licensing terms and conditions.

  Spyware is installed for a variety of purposes, including to track online behavior and browsing for market research and to steal a user's personal information that can later be used in identity theft and fraud. The dangers of spyware include its ability to:
  - Track a user's online activities without the user's knowledge or consent
  - Steal a user's personal information from his or her computer
  - Track a user's each and every keystroke (including the entry of password and financial information)
  - Hijack homepages and substitute unacceptable sites
  - Create an endless stream of pop-up ads
  - Change computer settings (such as changing a user's default homepage settings)
  - Disable hardware and software computer settings
  - Drastically slow infected computers
  - Remain on a user's computer in spite of attempts to uninstall it, and
  - Result in hard drive corruption.[10]
- **Other Cyber-Inhabitants Worth a Mention:**
  - **Supportware:** A legitimate type of software that can be used to deliver security services or support Internet access.
  - **Adware:** Software that can be legitimate in that it provides users with free or low-cost software in exchange for the user's agreement to be exposed to advertisements.
  - **Noticeware:** Legitimate software that provides notices for security technologies, such as anti-virus applications.
  - **Malware:** A general term that refers to malicious types of software, such as viruses, worms, and spyware. The defining feature of this software is that its main purpose is to cause harm to users.

Background on the Business Impact:

Spam, phishing and spyware can have an array of negative consequences including:

- A negative impact on employee productivity due to time expended deleting spam and phishing emails and slowed IT asset performance resulting from spyware infections
- Increased pressure on servers and other IT equipment due to large amounts of spam and phishing emails and spyware programs
- The expenditure of state funds to purchase and maintain prevention, detection, and response mechanisms, such as email filtering and anti-spyware solutions
- Increased liability risk due to the potential for the exposure of the state's information assets, especially through phishing and spyware attacks.

[10] While Internet cookies and similar technologies can be used to improve users' online experience, spyware is distinguishable in many cases from legitimate uses of cookies because of the ***malicious intent*** of spyware to ***surreptitiously*** track Internet users and, in some cases, ***steal users' personal information***.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Spam: At the state government level, the business impact of spam may be the most pronounced threat on a daily-basis because of the time that employees expend to delete it and the increased pressure that it applies to servers. States are especially attractive spammer targets because of their large number of email addresses, the adoption of consistent email naming conventions, and the placement of state employees' email addresses on the Internet. Although these vulnerabilities compound state spam problems, states must balance the negative impact of these vulnerabilities with the positive impact of making state employees more accessible to citizens with questions. Even though the use of spam-filtering technologies can assist states in alleviating spam's impact, such technologies can have the unintended consequence of blocking legitimate emails. This can cost states time and money in order to identify and unblock legitimate emails trapped by spam-filters.

Phishing and Spyware: While the impact of phishing and spyware may be felt more by citizens in their personal use of the Internet, ***states can expect to expend time and funds for technical trouble-shooting and remediation and removal efforts regarding spyware programs at the desktop-level without the implementation of adequate anti-spyware measures.*** In terms of phishing and spyware's impact on citizens' personal use, estimates for the total amount of consumer losses worldwide as a result of phishing range from less than $150 million[11] to $2.4 billion.[12] Citizens surfing the Internet, particularly via a broadband connection without a spyware detection program, may experience symptoms ranging from sluggish computer performance to hijacked homepages to even identity theft as a result of spyware infections. The net impact, in turn, may be citizens' loss of confidence in e-commerce and e-government leading to a reluctance to engage in transactions via the Internet and email. The end result is an appreciably negative impact on the growth of online government services and business processes, even though online services can provide much more efficient means to serve citizens' needs.

Section III: The Privacy Implications

Spam: While spam may be more properly characterized as a resource impediment to state business processes, its privacy impact has been exacerbated by citizens who perceive the massive amounts of unsolicited and often offensive emails as infringing on their "right to be left alone." The citizen privacy impact may be likened to the legal tort of trespass, since copious amounts of unsolicited email may serve as an invasion of privacy for those conducting business and personal correspondence via email. As evidence, one estimate suggests that approximately 67% of all email correspondence in December 2004 was spam.[13] Moreover, while spam as a percentage of incoming email appears to have begun to level off, there have been recent indications that the total number of spam messages continues to increase.[14] Most spam is generated by professional spamming firms and not by legitimate businesses. A particularly worrisome aspect of spam is that it may serve as the messenger for delivering potentially serious privacy breaches in the form of spyware and phishing attacks.

---

[11] "Report: Cost of Phishing Not So High," Robert Lemos, Cnet news.com, December 1, 2004, <http://news.com.com/Report+Cost+of+phishing+not+so+high/2100-7349_3-5473170.html>.
[12] "Good News: 'Phishing' Scams Net *Only* $500 Million," Cnet news.com, September 29, 2004, <http://news.com.com/Good+news+Phishing+scams+net+ionlyi+500+million/2100-1029_3-5388757.html?tag=nl>.
[13] "Has Spam Growth Stabilized? While the Amount of Unwanted E-Mail Hasn't Decreased, There is Some Good News," John E. Dunn, PC World.com, January 12, 2005, <http://www.pcworld.com/news/article/0,aid,119285,00.asp>.
[14] "Spam Not Leveling Off," Information Week, February 4, 2005, <http://informationweek.com/story/showArticle.jhtml;jsessionid=EUJCJ5VWBBIC0QSNDBCCKHSCJUMEKJVN?articleID=59301231>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Phishing: Phishing attacks have focused on conning citizens into divulging their personal information. ***However, states may experience privacy impacts from phishing. For example, a spoofed email could persuade a state employee to click on a link that will download spyware onto a state computer, thereby jeopardizing the privacy of state information.*** Furthermore, phishers tend to target industries that have deep stores of personal information,[15] which places states, with their vast amounts of citizen information, at risk. As stewards of citizens' information and other government data, states are obligated to protect against phishing. Moreover, if phishers execute attacks by spoofing state emails and websites, citizens' trust in government to protect them from such scams could be diminished. States can increase citizen trust by:

- Protecting citizens from phishing attacks with spoofed government-related emails and/or websites, and
- Helping to protect them generally from phishers and other malicious cyber-inhabitants.

Spyware: Spyware is very prevalent on home computers because of poor user choices and lack of configuration management that result in the unwitting installation of spyware. Given the seriousness of privacy threats to citizens that spyware has created, CIOs are obligated to help citizens address these threats to improve the quality of user choices and raise awareness of Internet and email threats. ***However, states have at their disposal the ability to control configurations and implement policies to guide state employees' choices and behavior while on the Internet at work.*** This is an important point for states, since spyware becomes a greater threat to the online experience as states increasingly turn to browsers as the desktop client for applications that assist the public. ***States should keep in mind, though, that spyware is a multi-faceted threat capable of rapid mutation to adjust to available solutions. Thus, there are no simple, silver-bullet solutions to the spyware threat.***

Spyware also poses a more direct threat to personal information than other forms of Internet and email fraud tactics, since it can track and harvest information from a user's computer without his or her consent. A recent study uncovered more than 20 spyware elements per corporate computer and concluded that thousands of desktop computers inside the surveyed organizations could potentially be infected with spyware.[16] The surreptitious installation of spyware can occur when a state employee is using the Internet for business purposes. However, when state employees use the Internet at work for personal reasons, the risk increases, even if such personal use is within the parameters of an acceptable use policy. Not only is personal information placed at risk, but sensitive government information, such as that related to homeland security, could also be at risk. While phishers have been concentrating on email as a delivery mechanism for spyware, in the future, states may face additional risks as those with malicious intent explore infecting computers via mainstream websites, Instant Messaging or P2P (Peer-to-Peer) networks.

Although spyware typically is thought to be an external threat, it may also pose an internal threat. Key-logger and similar technologies could be used to facilitate internal intrusions by state employees or contractors to state IT systems. These intrusions often go unnoticed being deceptively labeled as "remote systems administration tools," thereby providing an impression of legitimate authority to access internal networks and information.

---

[15] "Proposed Solutions to Address the Threat of Email Spoofing Scams," the Anti-Phishing Working Group (APWG), December 2003, <http://www.antiphishing.org/Proposed%20Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Paper.pdf>.

[16] "War on Spyware Widening," Jack M. Germain, TechNewsWorld, January 8, 2005, <http://www.technewsworld.com/story/39447.html>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Spyware has raised privacy concerns about similar technologies that are used or installed ***with*** a user's consent. For example, supportware, noticeware, and adware can be used for legitimate purposes as long as the user understands how and why the technology is being used and consents to its use. Additionally, employers' workplace monitoring of their employees via technologies that track Websites visited by employees or even employees' keystrokes has raised questions as to whether employees should have an expectation of privacy in the workplace. States' laws and regulations as to whether employees have an expectation of workplace privacy and when and how workplace monitoring may take place vary from state-to-state.

Section IV: Recent Activities on Spam, Phishing and Spyware

Spam: Spam has been the subject of regulatory efforts at both the federal and state levels. At the federal level, Congress enacted the CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003), which seeks to regulate unsolicited commercial emails by implementing such requirements as providing recipients with a means of opting-out of future unsolicited emails from the sender. However, the CAN-SPAM Act has had a limited impact with only an estimated 9.8% of all spam emails being compliant with its requirements.[17] The Federal Trade Commission (FTC) also has recommended against the implementation of a Do-Not-Email List, citing significant security, enforcement, practical and technical challenges.[18]

At the state level, 36 states have enacted anti-spam laws.[19] However, the CAN-SPAM Act pre-empts state laws that expressly regulate the use of email to send commercial messages, except to the extent that they prohibit falsity or deception of commercial email.[20] For state laws that are not pre-empted by the CAN-SPAM Act, they may face constitutional challenges, since state courts are split as to whether state anti-spam laws unconstitutionally burden interstate commerce.[21] This raises the question of whether state regulation of a problem that knows no jurisdictional boundaries, such as the conveyance of spam over the Internet, is appropriate or even in keeping with the U.S. Constitution.

While spam-filtering is common, the FTC has cited domain-level authentication as a promising anti-spam technology solution.[22] The viability and scalability of domain-level authentication solutions depend on how technological and education challenges associated with such solutions are addressed. Increasing user frustration has led commercial ISPs to improve filtering technologies, but spammers could adapt to such measures by beginning to target large organizations' email networks.[23]

---

[17] "Commtouch Reports Spam Trends for First Half of 2004: Viagra is King of Spam, 5 Countries are Hosting 99.68% of Spammer Websites and Nearly 10% of All Spam is CAN-SPAM Compliant," June 2004, <http://www.commtouch.com/news/english/2004/pr_04063001.shtml>.
[18] Federal Trade Commission (FTC), Email Authentication Summit Webpage, <http://www.ftc.gov/bcp/workshops/e-authentication/>.
[19] "State Laws Relating to Unsolicited Commercial or Bulk E-mail (SPAM)," National Conference of State Legislatures (NSCL), November 5, 2004, <http://www.ncsl.org/programs/lis/legislation/spamlaws02.htm>.
[20] CAN-SPAM Act of 2003, Public Law 108-187, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf>.
[21] "Judge Rules Maryland's Anti-Spam Law Unconstitutional," Juan Carlos Perez, IDG News Service, December 16, 2004, <http://www.nwfusion.com/news/2004/1216judgemaryl.html>.
[22] Federal Trade Commission (FTC), Email Authentication Summit Webpage, <http://www.ftc.gov/bcp/workshops/e-authentication/>.
[23] "Has Spam Growth Stabilized? While the Amount of Unwanted E-Mail Hasn't Decreased, There is Some Good News," John E. Dunn, PC World, January 12, 2005, <http://www.pcworld.com/news/article/0,aid,119285,00.asp>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Phishing: There currently is not a federal law that specifically prohibits phishing. However, laws identified by the U.S. Department of Justice as potentially applying to instances of phishing include identity theft, wire fraud, credit card fraud, bank fraud, and computer fraud laws as well as the CAN-SPAM Act. Terms of imprisonment for violations can be as high as 30 years for wire fraud and bank fraud violations or as low as 5 years for CAN-SPAM Act violations.[24] Also, on the law enforcement front, "Digital PhishNet," which is a joint law enforcement/industry initiative, seeks to bring phishers to justice. Its members include ISPs, online auction websites, and financial institutions as well as various law enforcement agencies, including the Federal Bureau of Investigation (FBI).[25]

The Anti-Phishing Working Group (APWG), an organization composed of financial institutions, e-commerce providers, ISPs, web email services, and software vendors, is seeking to develop a solution to email phishing. The three general classes of solutions the APWG has identified are:

(1) Strong authentication of any users visiting a business website, such as using two-factor authentication
(2) Using enhanced DNS capabilities to verify the IP address of a sender's email server, and
(3) Using S/MIME digital signatures to sign outbound mail and providing signature verification at the gateway or email client.

These proposed solutions have cost implications, scalability issues and technical challenges that will have to be addressed. However, the APWG believes that mail server IP verification for large web email providers to combat spam and digitally signed email when sending to corporate users may be a complete solution. It also characterized the U.S. Department of Defense (DoD) as a leader in IT security and authentication in citing DoD's roll-out of its signed email program that would require all DoD communications to be digitally signed.[26]

As of December 2004, 85% of phishers' targets have been financial institutions, while 7% of targets have been ISPs and 6% retailers.[27] However, phishers may be using new tactics such as fake job advertisements that entice users to fill-out a fake application form. Other new tactics of phishers are the use of new tools that automate attacks, the hosting of attacks from virus or worm-infected, hijacked home computers,[28] and sending phishing emails that contain a link that takes the recipient to an attacker-controlled page located on a target organization's server.[29]

---

[24] "Special Report on 'Phishing,'" U.S. Department of Justice, Criminal Division, 2004, <http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf>.
[25] Digital PhishNet, <http://www.digitalphishnet.org/default.aspx>.
[26] "Proposed Solutions to Address the Threat of Email Spoofing Scams," the Anti-Phishing Working Group (APWG), December 2003, <http://www.antiphishing.org/Proposed%20Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Paper.pdf>.
[27] "Phishing Activity Trends Report," the Anti-Phishing Working Group (APWG), January 2005, <http://antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20December%202004.pdf>.
[28] "Hi-Tech Tools Fuel Phishing Boom," BBC News, November 24, 2004, <http://news.bbc.co.uk/2/hi/technology/4037975.stm>.
[29] "Scammers Exploit DomainKeys Anti-Phishing Weapon," Dennis Fisher, eweek.com, November 29, 2004, <http://www.eweek.com/article2/0,1759,1732576,00.asp>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Spyware: Congressional efforts during the 108th legislative session to enact spyware legislation passed the House but were not the subject of a Senate vote. However, anti-spyware legislation is currently pending before Congress and potentially could be enacted.[30] The FTC hosted an anti-spyware summit in 2004 as a first step to deal with this problem. FTC Commissioner Orson Swindle, though, has identified issues with addressing consumer spyware concerns without unnecessarily burdening legitimate software developers or hindering innovation.[31] Similar to anti-spam efforts, two states have enacted anti-spyware legislation and several others are considering such measures.[32] However, given the amorphous nature of the Internet, the same jurisdictional and enforcement problems that have plagued state anti-spam efforts may arise with similar state anti-spyware legislation.

While many software firms are making anti-spyware solutions available, both bundled with other products and as stand-alone software, these solutions are not fool-proof. Spyware program writers are constantly adapting their spyware applications to circumvent anti-spyware solutions.[33] Hundreds of new spyware variants are released each month. Another concern is that anti-spyware programs running in the background can cause computer performance lags and slow-downs.[34]

The Future: As new laws are created to address spam, phishing and spyware, currently existing laws, including computer trespass and fraud laws, may be applicable to prosecute spammers, phishers and spyware purveyors. However, while law enforcement efforts may be part of the solution to these Internet and email menaces, jurisdictional difficulties and the movement of spammers, phishers and others to foreign soil have rendered those efforts an incomplete solution.

Technical solutions and education efforts also must be included to protect citizens as well as public and private sector organizations. Enterprise content security management solutions may be preferable for states as opposed to free or stand-alone solutions, which may be more appropriate for use by individuals. Discipline in ensuring that a state's IT asset configurations consistently are set and updated to fend off ever-morphing Internet and email threats can serve as another helpful step states can take. In addition, states may choose to migrate to Internet domains that citizens can easily identify as more trustworthy domains in order to avoid being duped by spoofed government emails and websites from less trustworthy Internet domains. For example, most states have domain names that are either [state name].[state postal abbreviation].us or [state name].gov. Citizen education as to which domains (such as dot-gov and dot-us) tend to be more trustworthy can help citizens avoid phishing attacks. Industry and governmental officials must work together to blend and synergize law enforcement, technical and education solutions for a maximum impact on spam, phishing and spyware. These efforts are especially important given the fact that the criminals' motivation to commit these crimes is not likely to end anytime soon.

---

[30] The Securely Protect Yourself Against Cyber Trespass Act (the Spy Act), HR. 29, introduced January 4, 2005, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h29ih.txt.pdf>.

[31] "Monitoring Software on Your PC: Spyware, Adware and Other Software," Remarks by Commissioner Orson Swindle, Federal Trade Commission (FTC), April 19, 2004, <http://www.ftc.gov/bcp/workshops/spyware/remarks_swindle.pdf>.

[32] "2004 State Legislation Relating to Internet Spyware or Adware," National Conference of State Legislatures (NCSL), January 28, 2005, <http://www.ncsl.org/programs/lis/spyware04.htm>.

[33] "Lawmaker Wants Spyware Deleted," Joe Rogalsky, Delaware State News, <http://www.newszap.com/articles/2004/12/04/dm/central_delaware/dsn04.txt>.

[34] "War on Spyware Widening," Jack M. Germain, TechNewsWorld, January 8, 2005, <http://www.technewsworld.com/story/39447.html>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

As the Internet continues to be an ever-frustrating jungle to traverse, states must be vigilant in protecting the personal information they possess from privacy breaches caused by predatory cyber-scum. State CIOs must remember that the spam problem began with a relatively small impact—three-to-four emails a day--but has now grown to overtake state employee and citizen email inboxes. Moreover, as each new threat is addressed, additional threats that cannot be anticipated loom upon the horizon. For example, pharming, a malicious website redirect that takes a user who is trying to reach a legitimate website to a fake website without his or her knowledge, has been identified as a potential new threat that is surfacing.[35] ***States must take sufficient measures now against current Internet and email threats and avoid being lulled into complacency by emerging threats that are small at the start but have the potential to rapidly expand. If states do not take appropriate steps now, Internet and email users, frustrated by the savage nature of the Internet, may unplug themselves from the electronic world. This would diminish the use and value of e-government applications that would otherwise bring efficiencies, cost savings, and better services to citizens.***[36]

What CIOs Need to Know

- CIOs need to understand the privacy and other business implications of spam, phishing and spyware in order to educate policymakers as they may try to address these threats through legislation or other legal mandates.
- Enterprise content security management solutions act as an insurance policy against the erosion of citizen privacy and trust in government.
- States should be aware that, while phishing and other menacing cyber-inhabitants have focused on the financial and other sectors, these threats have the potential to migrate to the state government sector. States are an attractive target for menacing Internet and email threats, due to their deep information stores, increasing presence on the Internet and publicly available email addresses.
- As each existing threat is addressed, new threats, such as pharming, may be waiting to make their respective mark on the Internet. Currently existing threats, such as phishing and spyware, are becoming more sophisticated and are using foreign resources to deflect legal and enforcement remedies.
- State CIOs should be aware that there is the potential for citizens to become overwhelmed by the Internet jungle and its predators that include spam, phishing, spyware and other potentially harmful Internet and email applications. This may lead to some citizens' decision to "unplug" from the Internet and email, thereby diminishing the value and benefits of e-government applications. Hence, dealing with these problems now is imperative to protect the expansion and enhancement of e-government applications.

CIO Action Items

- ***State CIOs have a leadership responsibility to promote an online experience that is positive for the end user and fosters citizen trust, while taking advantage of opportunities, such as through the state's portal, to educate citizens on how they can protect themselves against the cyber-threats that lurk about on the Internet. State CIOs must take a more proactive approach to combating spam, phishing, spyware and future Internet and email threats.***

[35] "Is a New ID Theft Scam in the Wings?" William Jackson, Government Computer News, January 14, 2005, <http://www.gcn.com/vol1_no1/daily-updates/34815-1.html>.
[36] "Safety in Numbers," John Surmacz, CSOonline, January 28, 2005, <http://www.csoonline.com/metrics/index.cfm>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

- CIOs should examine the extent to which currently existing computer trespass and similar laws are applicable to Internet and email threats.
- To the extent that technical solutions are available, such as content filtering for spam and phishing emails, states should consider these measures as a way to alleviate the risks posed by these threats. Among the variety of technical solutions available, states should focus their attention on enterprise solutions. Free solutions may be better suited for use by individual consumers.
- Discipline in ensuring that state IT asset configurations are reviewed and updated on a regular basis is needed to keep pace with ever-morphing cyber-threats.
- At the enterprise level, states should publish policies for controlling client configurations, using network configuration tools, and implementing security measures, including patch management, to address Internet and email threats.[37]
- Migrating to more trustworthy Internet domains, such as the [state name].gov or [state name].[state postal abbreviation].us, may be a way that states can assist citizens from being duped by phishing attacks that originate from less trustworthy Internet domains.
- State CIOs may consider using their state portals to educate citizens on how they can protect themselves from Internet and email threats. One option would be to provide a link on the state portal to the National Cyber Security Alliance's (NCSA) Stay Safe Online website at: http://www.staysafeonline.info/. That website provides easy-to-understand tips for how citizens, small businesses and others can protect their computers and personal information while using the Internet and email.
- CIOs need to educate citizens and policymakers alike on these issues, clarifying the threats to privacy as well as business processes and identifying ways that these threats can be managed. States can serve as good portals of information.

[37] For more information about security measures that may assist in thwarting Internet and email threats, please see the National Institute of Standards and Technology's (NIST) Special Publication 800-53 "Recommended Security Controls for Federal Information Systems," January 2005, at <http://csrc.nist.gov/publications/drafts/SP-800-53-FinalDraft.pdf>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Appendix A: Need More Info? References and Resources

NASCIO Privacy Committee Webpage, <https://www.nascio.org/nascioCommittees/privacy/>.

U.S. Computer Emergency Readiness Team (US-CERT), <http://www.us-cert.gov/>.

Federal Trade Commission (FTC), <http://www.ftc.gov/>.

FTC Spam and Phishing Webpage, <http://www.ftc.gov/bcp/conline/edcams/spam/report.html>.

FTC Spyware Workshop Webpage, <http://www.ftc.gov/bcp/workshops/spyware/>.

Information Technology Association of America (ITAA), <http://www.itaa.org/>.

"Spyware, Supportware, Noticeware, Adware and the Internet," ITAA, September 2004, <http://www.itaa.org/news/docs/adwarewp.pdf>.

National Conference of State Legislatures (NCSL), <http://www.ncsl.org/>.

Spyware and Adware Webpage, <http://www.ncsl.org/programs/lis/spyware04.htm>.

Spam Webpage, <http://www.ncsl.org/programs/lis/legislation/spam04.htm>.

The Anti-Phishing Working Group (APWG), <http://www.antiphishing.org/>.

Digital PhishNet, <http://www.digitalphishnet.org/default.aspx>.

FTC's SPAM Rules and Acts Webpage, (including the CAN-SPAM Act of 2003), <http://www.ftc.gov/bcp/conline/edcams/spam/rules.htm>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Appendix B: Excerpts from US-CERT National Cyber Tips and the FTC

The following are excerpts from US-CERT and the FTC on spam, phishing and spyware. They may be helpful for State CIOs, policymakers, employees and citizens so that they may protect themselves from spam, phishing and spyware.

Spam:

How can you reduce the amount of spam?

- **Don't give your email address out arbitrarily:** Email addresses have become so common that a space for them is often included on any form that asks for your address—even comment cards at restaurants. It seems harmless, so many people write them in the space provided without realizing what could happen to that information. For example, companies often enter the addresses into a database so that they can keep track of their customers and the customers' preferences. Sometimes these lists are sold to or shared with other companies, and suddenly you are receiving email that you didn't request.
- **Check privacy policies:** Before submitting your email address online, look for a privacy policy. Most reputable sites will have a link to their privacy policy from any form where you're asked to submit personal data. You should read this policy before submitting your email address or any other personal information so that you know what the owners of the site plan to do with the information.
- **Be aware of options selected by default:** When you sign up for some online accounts or services, there may be a section that provides you with the option to receive email about other products and services. Sometimes there are options selected by default, so if you do not deselect them, you could begin to receive email from those lists as well.
- **Use filters:** Many email programs offer filtering capabilities that allow you to block certain addresses or to only allow email from addresses on your contact list. Some ISPs offer spam "tagging" or filtering services, but legitimate messages misclassified as spam might be dropped before reaching your inbox. However, many ISPs that offer filtering services also provide options for tagging suspected spam messages so the end user can more easily identify them. This can be useful in conjunction with filtering capabilities provided by many email programs.
- **Don't follow links in spam messages:** Some spam relies on generators that try variations or email addresses at certain domains. If you click a link with an email message or reply to a certain address, you are just confirming that your email address is valid. Unwanted messages that offer an "unsubscribe" option are particularly tempting, but this is often just a method for collecting valid addresses that are then sent other spam.
- **Disable the automatic downloading of graphics in HTML mail:** Many spammers send HTML mail with a linked graphic file that is then used to track who opens the mail message—when your mail client downloads the graphic from their web server, they know you've opened the message. Disabling HTML mail entirely and viewing messages in plain text also prevents this problem.
- **Consider opening an additional email account:** Many domains offer free email accounts. If you frequently submit your email address (for online shopping, signing up for services, or including it on something like a comment card), you may want to have a secondary email account to protect your primary email account from any spam that could be generated. You should also use a secondary account when posting to online bulletin boards, chat rooms, public mailing lists, or USENET so that you can get rid of it when it starts filling up with spam.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

- **Don't spam other people:** Be a responsible and considerate user. Some people consider email forwards a type of spam, so be selective with the messages you redistribute. Don't forward every message to everyone in your address book, and if someone asks that you not forward messages to them, respect their request.

For more information, please see "Reducing Spam," Cyber Security Tip ST04-007, National Cyber Alert System, US-CERT, at <http://www.us-cert.gov/cas/tips/ST04-007.html>.

Phishing:

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a web site's security.
- Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group <http://www.antiphishing.org/>.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission <http://www.ftc.gov/>.

For more information, please see "Avoiding Social Engineering and Phishing Attacks," Cyber Security Tip ST04-014, National Cyber Alert System, US-CERT, <http://www.us-cert.gov/cas/tips/ST04-014.html>.

Spyware:

How do you know if there is spyware on your computer?

The following symptoms *may* indicate that spyware is installed on your computer:

- You are subject to endless pop-up windows
- You are redirected to websites other than the one you typed into your browser
- New, unexpected toolbars appear in your web browser
- New, unexpected icons appear in the task tray at the bottom of your screen
- Your browser's home page suddenly changes
- The search engine your browser opens when you click "search" has been changed
- Certain keys fail to work in your browser (e.g., the tab key doesn't work when you are moving to the next field within a form)
- Random Windows error messages begin to appear
- Your computer suddenly seems very slow when opening programs or processing tasks (saving files, etc.).

How can you prevent spyware from installing on your computer?

- **Don't click on links within pop-up windows:** Because pop-up windows are often a product of spyware, clicking on the window may install spyware on your computer. To close the pop-up window, click on the "X" icon in the titlebar instead of a "close" link within the window.
- **Choose "no" when asked unexpected questions:** Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. Always select "no" or "cancel," or close the dialog box by clicking the "X" icon in the titlebar.
- **Be wary of free downloadable software:** There are many sites that offer customized toolbars or other features that appeal to users. Don't download programs from sites you don't trust, and realize that you may be exposing your computer to spyware by downloading some of these programs.
- **Don't follow the email links claiming to offer anti-spyware software:** Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating.
- **Adjust your browser preferences to limit pop-up windows and cookies:** Pop-up windows are often generated by some kind of scripting or active content. Adjusting the settings within your browser to reduce or prevent scripting or active content may reduce the number of pop-up windows that appear. Some browsers offer a specific option to block or limit pop-up windows. Certain types of cookies are sometimes considered spyware because they reveal what webpages you have visited. You can adjust your privacy settings to only allow cookies for the website you are visiting.

How do you remove spyware?

- **Run a full scan on your computer with your anti-virus software:** Some anti-virus software will find and remove spyware, but it may not find the spyware when it is monitoring your computer in real time. Set your anti-virus software to prompt you to run a full scan periodically.
- **Run a legitimate product specifically designed to remove spyware:** Many vendors offer products that will scan your computer for spyware and remove any spyware software. Popular products include Lavasoft's Ad-Aware, Webroot's SpySweeper, PestPatrol, and Spybot Search and Destroy.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

For more information, please see "Recognizing and Avoiding Spyware," Cyber Security Tip ST04-016, National Cyber Alert System, US-CERT, <http://www.us-cert.gov/cas/tips/ST04-016.html>.

Securing Your Server:

The bottom line is that "[a]n open proxy or open relay is an open door to theft of your computer services and the impression that your organization is sending unwanted junk mail." The following list of questions will help you to identify proxy server vulnerabilities:

- Does your proxy allow connections from untrusted networks such as the Internet?
- Are you using the most current version of your proxy server software and hardware?
- Have you applied the latest patches or upgrades available?
- Are you using proper access controls for your server?
- Is someone regularly checking for unauthorized uses of your proxy server?
- Do you have and monitor an "abuse@[yourDomainName]" email account where people can report abuses of your proxy server?

For more information, please see "FTC Facts for Business—Securing Your Server: Shut the Door on Spam," Federal Trade Commission (FTC), January 2004, <http://www.ftc.gov/bcp/conline/pubs/buspubs/secureyourserver.pdf

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org