The Challenge of Spam

An Internet Society Public Policy Briefing

30 October 2015

Introduction

The proliferation of spam email presents a harmful, costly, and evolving threat to Internet users. Governments can help reduce the impact of spam by deterring offenders via effective laws and enforcement measures, multistakeholder antispam efforts, the adoption of best practices, and citizen education about the dangers of spam.

Spam email, those unsolicited email messages we find cluttering our inboxes, are a challenge for Internet users, businesses, and policymakers alike. Estimates vary, but some suggest that more than 100 billion spam messages are sent every day, representing up to 85 percent of global daily email traffic.[1]

The term *spam* generally refers to unsolicited electronic communications (typically email) or, in some cases, unsolicited commercial bulk communications.[2] Some refer to this kind of email simply as *junk email.* While spam activity is largely concentrated in the form of email, spam is an evolving threat that has spread into virtually all types of electronic messages, including mobile Short Message Service (SMS) text messages, social media postings, instant messaging systems, and online forums.

Beyond the annoyance and the time wasted sifting through unwanted messages, spam can cause significant harm by infecting users' computers with malicious software capable of damaging systems and stealing personal information. It also can consume network resources.

Today, some of the most common types of harmful spam are financial scam messages, email messages with embedded phishing software[3], botnet malware[4], and/or ransomware.[5] Spammers are highly inventive and relentless. They are constantly creating ever-more-attractive bait to entice users to open malware-containing messages. And they continue to seek new email address lists and new communication media to target.

1 Cisco Systems, SenderBase real-time threat monitoring system, http://www.senderbase.org.
2 International Telecommunications Union World Conference on International Telecommunication's International Telecommunications Regulations Article 7, Unsolicited bulk electronic communication, http://www.itu.int/pub/S-CONF-WCIT-2012/en.
3 Phishing generally is an attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.
4 *Malware* is a term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, and other malicious programs that will infect the users computer with forms of executable code, scripts, active content, and other invasive software.
5 Ransomware is a type of malware that demands a ransom payment in order to remove it from the infected computer.

Key Considerations

Governments around the world are taking legal steps to combat spam, although so far these efforts are more prevalent in western and developed countries. This might be because those countries faced the spam threat earlier. Countries that have adopted legislation regarding spam also have defined what they consider to be spam. These countries have made spam illegal, provided consumer education on how to manage spam, and in some cases, enacted and used enforcement measures to deter spammers. The result has been a noticeable drop of domestic spam, as confirmed in the Netherlands in 2010. After the Dutch government enacted an antispam law, users in the country experienced an 85 percent decrease in domestic spam.[6] However, spammers might have moved to countries without antispam laws. In addition to individual national legislation, there exists an international spam enforcement community known as the London Action Plan (LAP), which works to collaborate on cross-border spam enforcement and related issues.[7]

Network operators and the technical community have developed best practices for managing network security threats, including spam. For example, the Messaging, Malware, and Mobile Anti-Abuse Working Group (M^3AAWG)[8] produces documents on approaches and tools available to address security issues, such as describing steps to better manage the impact of spam on a network.[9] The Spamhaus Project[10] tracks spam operations and sources to provide real-time network protection and works with law enforcement to combat spam. There are also national and international organizations that work on ways to better manage spam, including the Global System for Mobile Association (GSMA), Regional Internet Registries (RIRs), the International Telecommunications Union (ITU), and the Internet Society.

There are a variety of spam-blocking tools that can improve the way users deal with spam. But no matter how effective spam-blocking technology becomes, end users will always need to be vigilant about the possibility of harmful spam messages reaching them because no tool is perfect and spammers are always inventing new ways to spam. Also, it can be hard for users to recognize whether a message is malicious. Verizon's *2015 Data Breach Investigations Report* indicates that 23 percent of email recipients open phishing messages and 11 percent click on attachments, thereby compromising their computers and networked systems.[11]

Challenges

From a broad perspective, spam is a constantly evolving technical, economic, and security challenge for many countries. As such, a multifaceted approach is required to address its challenges. More specifically, the problem of spam offers the following challenges to consider:

---

6 Dutch antispam law success, https://www.spamexperts.com/about/news/dutch-anti-spam-law-has-success.
7 London Action Plan, http://londonactionplan.org.
8 Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) information, https://www.maawg.org/published-documents.
9 In June 2015, M3AAWG and LAP published Operation Safety-Net: Best Practices to address online, mobile and telephony threats, https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf
10 Spamhaus Project information: https://www.spamhaus.org/.
11 Verizon Corporation's *2015 Data Breach Investigations Report,* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015-insider_en_xg.pdf

- Spam is an expensive problem for both the Internet's infrastructure and its users. High volumes of spam consume valuable network resources, and are a particular burden on countries with limited Internet access and bandwidth. Internet service providers (ISPs) expend great effort to manage this traffic, and end users need to be vigilant of opening spam that contains malware or scams. For mobile data subscribers and those who subscribe to metered services, the cost of receiving or unwittingly sending high numbers of spam messages can be significant. In addition, there are remediation costs to repair systems infected and/or attacked by spam-enabled malware, as well as costs associated with stolen user data.

- In general, the economics of spam lean heavily in favor of spammers. Spam messages cost very little to send. In fact, most of the costs are covered by message recipients, ISPs, infected users, or network operators.

- The nature of spam changes as new applications and ways to exchange data on the Internet are introduced. Spammers advance in their ability to use those platforms to deliver more intrusive and damaging ways to steal personal data, damage networks, and infect systems.

- Spam affects a wide range of Internet users; no single organization can solve the threats from spam by itself. It takes a worldwide, multistakeholder community working together to address the problem.

- Beyond the direct harm to users and the burden on network resources, spam also insidiously creates a lack of user trust and is viewed by some as an obstacle to the use of the Internet and e-commerce. There is also the potentially negative impact on a user's reputation if their identity is stolen by spammers and used to send out spam.

- Communities involved in deploying antispam measures may be met with retaliation (e.g., victims of Distributed Denial of Service (DDoS) attacks, hacking), so it is important that members of the global antispam communities not only provide assistance on how to combat spam, but also provide technical and other support against retaliation attacks.

Guiding Principles

The Internet Society believes that a collaborative approach among all relevant stakeholders will provide the best spam-mitigation solutions and security protection. This general approach is emphasized in the Internet Society's Collaborative Security principles, which emphasize a shared and collective responsibility among online stakeholders to achieve desired outcomes.[12]

Governments can help combat spam by:

- **Understanding the changing spam landscape.** Spammers are constantly evolving their methods for spreading malicious email. Governments should make efforts to be up-to-date on spam techniques, trends, and evolving threats. Governments can also play a key role by

12 Internet Society's Collaborative Security Principles, http://www.internetsociety.org/collaborativesecurity

supporting research into the identification, tracking, and mitigation of spam and other online threats, as well as the development of related metrics to support policy making. Governments can also encourage privacy-respecting methods for information sharing among stakeholders on real-time risks and threats.

- **Partnering with stakeholders for success.** Spam is a multifaceted problem. A range of stakeholders have a role and should be involved in developing strategies, best practices, and approaches to the implementation of antispam measures, including the development of spam- and malware-mitigation tools. Coordination and partnerships among private and public sector stakeholders should be developed in order to produce robust solutions to spam. Useful entities to engage include antispam coalitions and working groups (such as M^{3}AAWG), computer security response teams, network operators, ISPs and online service providers, the Internet technical community, business and consumer advocacy groups, civil society, and others with an interest in combatting spam, malware, and other malicious online activities.

- **Enacting appropriate antispam legislation and enforcement measures.** As previously noted, antispam legislation, strong consumer protection laws, and strong enforcement measures can help deter offending players and reduce the amount of spam sent and received in a country.[13] Government agencies charged with enforcing spam laws and regulations should be well-resourced, publicize the outcomes of enforcement measures, and make it easy for Internet users to report problematic spam and malware distribution.

- **Collaborating with international counterparts.** Spam is a cross-border problem. Collaboration with government counterparts around the world in antispam efforts, including international enforcement actions, is critical to successfully addressing global spam proliferation.

- **Educating and empowering citizens.** Governments should support public- and private-sector initiatives that educate Internet users on how to recognize and protect themselves against spam and other online threats. Internet users also should be aware of their legal right to seek remedies for loss or damage caused by illegal spam and other malicious online activities.

13 A comprehensive source for tracking antispam legislation is available at http://www.spamlaws.com. Links to several national legislative approaches are also located in the Internet Society's Spam Took Kit at http://www.internetsociety.org/spamtoolkit.

Additional Resources

The Internet Society has published a number of papers and content related to this issue. These are available for free download on the Internet Society website.

- Internet Society Anti-Spam Toolkit, https://www.internetsociety.org/spamtoolkit
- Internet Society Spam and Online Threats (e-learning course), http://www.internetsociety.org/what-we-do/inforum-learn-online/inforum-course-spam-and-online-threats.
- A Short Guide to Spam, http://internetsociety.org/spam/short-guide-spam
- A History of Spam, http://www.internetsociety.org/doc/history-spam
- *Combating Spam: Policy, Technical and Industry Approaches,* http://www.internetsociety.org/doc/combating-spam-policy-technical-and-industry-approaches