The Evolution of Spam

By Melanie Lockwood Herman

Executive Director

Resource Type: Risk eNews

Topic: Data Privacy, Tech Risk, Cybersecurity

Where did those pesky, inbox-clogging spam e-mail messages go? According to an article titled “Long life spam” appearing in a series of three pieces on the topic in the November 18th edition of The Economist, “Spammers are moving onto social-networking sites such as Facebook because they find e-mail increasingly unrewarding.” Spam is alive and well despite reports that the volume of spam sent via old fashioned e-mail messages is down.

The Economist cites a number of reasons for the decline in spam e-mail, including successful efforts by online security firms to block more than 98% of messages from reaching their intended targets. Common tools to fight spam include the use of filters to quarantine emails containing suspect words and blacklisting spammer e-mail addresses. The use of “botnets” — legitimate networks hijacked by cyber criminals to successfully deliver spam — has also been curtailed.

No Rest for the Wary and Worried

The filtering of spam e-mail messages has been welcome relief for many nonprofit leaders, who now spend *less time* deleting messages offering bargain priced wonder drugs. But it’s too early to celebrate the decline in cyber fraud. Spammers have turned their attention to new ways to get your attention and raid your wallet, and today’s, harder-to-detect spam is proliferating at record speed.

One popular method to snare today’s Internet user is to embed links to shady sites and Trojans in social media tools, such as Twitter messages. A recent university-based study suggested that 8% of the links featured in Twitter messages may be suspect. Perhaps more frightening, researchers say that *users are 20 times more likely to click on a link in a Twitter message than a link in an e-mail message*. Cybercrime is in many respects a game of numbers. Spammers send millions of messages in the hopes of snagging a handful of customers. So it should come as no surprise that cybercriminals are paying attention to the numbers.

Another popular method to induce unwise clicks is to include links in comments posted on websites. With nonprofit organizations scrambling to make their websites more interactive, many may unwittingly become conduits for the publication of links that can, in a single click, infect a computer with a virus or software program that steals passwords or “uses your machine for other nefarious purposes.”

Human Behavior is the Culprit

As the writers of the series in *The Economist* so aptly note, the real danger with spam is not found in hardware or software. The real danger lies in human behavior. Online users, from the very young and understandably naïve, to more mature business users, are simply *too trusting*. We eagerly seek to build a network of online friends in unguarded ways that would never happen in a face to face world. We browse online purveyors of products and services while forgetting our digital footprints. We click and tweet while distracted with other tasks. We share personal information with people we have never met, and encourage our online "friends" to help us build an even larger circle of colleagues we won't ever really "know." And we knowingly, regularly break the rules that were established to protect the vital missions of the nonprofits we serve. And according to a Cisco "Collaboration Nations" study, 50 percent of end users "admitted that they ignore company policy prohibiting use of social media tools at least once a week."

What To Do

- **Be vigilant**. Remaining vigilant appears to be the best defense to the quickly-evolving threat of spam and "click with extreme care" is the new mantra. Vigilance includes paying careful attention to your nonprofit's websites and other social media activity. If your online strategy is working and your community of supporters is truly connected, don't be surprised to get bad news about an improper or embarrassing post from a donor or other key stakeholder, rather than your IT staff. Being vigilant also means determining appropriate controls for access to valuable data and electronic assets. Balance the lure of making everything "easy to access" with a reminder that open access may make it easier for cybercriminals to gain access as well.
- **Update your acceptable use and other IT policies**. Your acceptable use policy should reflect how various devices may be used while reminding users about the software and data assets key to mission fulfillment. Many nonprofits are adopting a separate policy addressing the use of social media tools and platforms. Assuming that employees and volunteers "know better" is a risky approach. Give careful thought to whether staff who aren't involved in communications and PR should be granted unlimited access to social networking sites during work hours. The Center's online tool, My Risk Management Policies, offers a quick and affordable way to create a custom acceptable use policy from scratch. Templates for social media policies are also available.
- **Revisit the risk and impact of cyberslacking**. Most nonprofit executives realize that online shopping, interactive games and chat are luring their employees from critical assignments. But few executives tally the costs of "cyberslacking" and hold employees accountable. According to Cisco Security Intelligence Operations research, 7 percent of a "global sample" of Facebook users spend an average of 68 minutes per day playing "FarmVille," currently the most popular interactive online game. Smaller, but still significant numbers of users may be wasting your nonprofit's time and resources playing other popular games, such as Mafia Wars and Café World. If you don't think that lost productivity is a security risk for your nonprofit, think again. The Cisco research also notes that "cybercriminals are believed to be developing ways to deliver malware via these games."
- **Take a closer look**. Consider taking a closer look at the lurking risks associated with your use of technology. For most nonprofits these risks include dependence on technology contractors, social media use (and misuse), compliance with the requirements of technology contracts, adequacy of safeguards for client and employee personal information, and clarity of and adherence to acceptable use policies. The Center regularly undertakes Risk Assessments that include an examination of technology risks. A special engagement focusing on technology risk is also available. Learn more about our consulting practice here.

Melanie Lockwood Herman is Executive Director of the Nonprofit Risk Management Center. She welcomes your feedback on this article and questions about the NRMC's resources at Melanie@nonprofitrisk.org or 703.777.3504. The Center provides free and affordable risk management tools and resources at www.https://nonprofitrisk.org/ and affordable consulting assistance.