Oct. 01, 2006

From the Oct. 2006 Issue

In January 2004, a senior executive from a well-known technology company boldly proclaimed that "spam will soon be a thing of the past." Wow! Wouldn't that be nice? While significant strides have been made in the fight against spam, it is now three-quarters of the way through 2006 and Brittany Spears, herbal remedies, can't-miss-stock tips, discount mortgage offers, and the like are still showing up in way too many mailboxes. (My personal favorite is the message that offered the lucky recipient cash for selling their organs!) Just as annoying and far more sinister are phishing and malware scams that threaten even the most savvy computer users with identity theft and financial loss. As if the assault on e-mail boxes isn't sufficient, SPIM (spam over instant messaging) and SPIT (spam over Internet telephony) offer new challenges and threats to data security. Spam, SPIM, SPIT … what could possibly be next? Unfortunately, spam-free utopia has not yet arrived. Great awareness, caution and the proper use of technology are more essential than ever to protect vital information and electronic assets.

THE PROBLEM

According to a recent article posted on Information Week's website by Christopher Heun, the current state of spam in 2006 is a good news/bad news situation. Consider the following:

- Spam accounted for about 80 percent of all the e-mail traffic on the Internet during the first quarter of 2006. (I understand it will never reach 100 percent, though [wink]!)
- Microsoft and AOL block nearly 5 billion pieces of spam every day.

- Nearly 90 percent of messages at Microsoft's MSN Hotmail are spam;

PHISHING

Compounding the bad news, the frequency and sophistication of "phishing" is on the rise, as well. According to the "Anti-Phishing: Best Practices for Institutions and Consumers" McAfee Research Technical Report #04-004, security experts at McAfee define phishing as "a form of Internet scam in which the attackers try to trick consumers into divulging sensitive personal information. The techniques usually involve fraudulent e-mails and websites that impersonate both legitimate e-mail and websites." Another tact is to dupe users into clicking on links or visiting websites that will plant malware such as key loggers or Trojan software on machines for use in future scams. These types of scams, which have also infiltrated instant messaging, are no longer limited to sophisticated hackers or organized crime rings. You, too, can follow the readily available instructions on the Internet and design your own phishing scam!

In large part to phishing, identity theft is the fastest growing crime in the United States. According to the NYPD Cyber Squad, the average identity theft case costs the victim $808 and 175 hours to clean up ("Phishing: 21st-Century Organized Crime," CipherTrust, Inc.).

NEWER FORMS OF Spam — SPIM & SPIT

No longer confined to e-mail, spam has also infiltrated instant messaging platforms. Users of public IM systems (e.g., MSN, AOL, Yahoo!) with public profiles may receive unsolicited advertisements in real time. While SPIM is less common than spam, it can also be more intrusive and dangerous. Whereas e-mail can be quickly scanned and deleted at any time, SPIM must be dealt with in real time. And while e-mail users generally know to be aware of spam, IM users expect to receive messages from personal contacts ("buddies") and are more likely

to be duped by a spimmer. Even a file or link from a known contact could be

As mentioned previously, much progress has been made in the fight against spam. Spam-preventing filters and other technology tools have improved significantly so that the level of spam individuals actually receive has been greatly reduced. Various types of filters for anti-spam solutions include blacklists, whitelists and Bayesian filtering. Blacklists automatically filter e-mails based on identified individual e-mails or domains, blocking known "offenders." Whitelist filtering will only deliver messages from those e-mails or domains that have been pre-approved by the recipient. Bayesian filtering uses complex statistical techniques to classify e-mails based on content from past e-mails. Based on the content, each is e-mail is assigned a certain score and then tagged as spam or probable spam. The difficulty with any one of these types of filters is that it must be constantly monitored and updated to make sure that it is eliminating spam effectively without trashing legitimate e-mails. Upkeep and fine tuning are required, but this can be time consuming. And spammers are clearly aware of the defenses end users are working to employ, so they are constantly fine tuning their spam attacks to pass right through these defenses.

POTENTIAL SOLUTIONS

For individual computer users, any reputable ISP should provide an effective first layer of defense. To add an extra layer of protection, a number of inexpensive products are available. Ranging in price from $20 to $40, such products include SpamEater Pro, Qurb, ChoiceMail One, Spam Killer, Spam Buster, iHateSpam, and many others. For a side-by-side comparison of individual spam filters, visit http://spam-filter-review.toptenreviews.com.

For corporations, server-based solutions include products such as GFi MailEssentials and ChoiceMail. While they fight spam in two different ways, both solutions eliminate the need to install and update anti-spam software on each desktop. GFi uses Bayesian filtering, while ChoiceMail uses a challenge and response

system where each would-be sender has to be approved in order to be added to

has provided significant improvement over anti-spam products we've used in the past.

Disclaimer: In spite of the many excellent products available today to fight spam, there is no perfect spam filter. As a result, end-user education and training is essential. Users must be taught (and reminded) on a regular basis how to recognize spam and phishing attacks and how to respond appropriately.

CONCLUSION
The technology executive mentioned in the introduction was Microsoft's own Bill Gates. Needless to say, it appears Mr. Gates was overly optimistic about the speed with which spam would be eradicated. The reality of spam is that the high stakes chess game between spammers and their opponents will continue
for the foreseeable future. As a result, it's critical for all computer users to stay educated, remain alert, and take advantage of the very latest technology tools to protect their identity and personal information.

———————————————————————-

David Cieslak is a Principal in Information Technology Group, Inc. (ITG), a computer consulting firm with offices in Simi Valley and Huntington Beach, Calif. He is currently an instructor for K2 Enterprises and a frequent speaker on technology issues. He also currently chairs the AICPA IT Executive Committee and serves on the Information Technology Alliance board of directors and CalCPA Council.

Technology

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us