E-mail Threats Tip Sheet

Spam

Spam is any unsolicited message or posting that is sent to multiple recipients, or multiple postings of the same message sent to newsgroups or listservers. Spam is the electronic equivalent of junk mail.

Different studies show that roughly half of all spam mail is related to money—advertising get-rich-quick schemes, debt-reduction plans, and gambling opportunities. A third of spam mail is porn-based, and this figure is set to increase. About 10 percent is health-related, and the remainder covers a wide variety of topics.

i-SAFE Inc. has created this list of tips to help you respond appropriately to spam.

- **Protect your e-mail address.**
  - Avoid giving your personal e-mail address to anyone other than family, friends, or business associates.
  - Create and use a separate e-mail address for public use (i.e. for posting on Web forums, or registering or purchasing online, etc.).
  - Before registering on a Web site, read the site's privacy policy to ensure that your e-mail address will not be shared or sold to a third party.
  - Never display your e-mail address openly online, such as on public forums, in chat rooms, or in profiles.
  - When forwarding e-mails to others, copy and paste the text into a new e-mail before sending. Simply clicking "Forward" also forwards the e-mail address(es) of the prior recipients of the e-mail. Remind friends and family to use this technique to avoid having your e-mail address forwarded to a person(s) you do not know.
- **Use technology to block spam.**
  - Check with your Internet service provider (ISP) to see what spam-blocking utilities it offers and how to activate them.
  - E-mail clients, such as Microsoft Outlook Express, have spam-blocking features and message rules that can block e-mail from unwanted sources. Check the "Help" tab to determine how to activate these features in your e-mail client.
- **Never respond to spam.**
  - Ignore the "Unsubscribe" links in spam e-mails. If the e-mail you received didn't require a subscription, there is little probability that you will stop the spam e-mails by unsubscribing. Instead, by responding to the e-mail, you are essentially validating that your e-mail address is active and being read. Professional spammers will often subsequently sell your e-mail address to other spammers.
- **Report spam e-mails.**
  - The United States has the CAN-SPAM ACT (Controlling the Assault of Non-Solicited Pornography and Marketing Act). To report any spam e-mails, forward a copy of them to spam@uce.gov.

E-mail Threats Tip Sheet

Phishing

Identity thieves often "phish" for information by sending e-mail spam or pop-up messages that appear to be legitimate businesses or organizations (i.e. bank or online payment services that you may deal with). These phishers lure their victims to counterfeit Web sites that appear to be the legitimate sites. However, they are intended to trick you into divulging information needed to steal your identity or perform fraudulent acts. Viruses or malicious programs often accompany e-mails and are secretly downloaded onto your computer to gather your personal and financial information.

Recognizing phishing e-mails is not always easy. Here are some tips to help you.

- **Watch for bad spelling and grammar.**
  A careless scammer often makes spelling and grammar mistakes that would otherwise be caught by a legitimate company's proofreaders.
- **Be aware of generic greetings.**
  Most companies will address you by your name or Web site username when corresponding with you. Generic greetings, such as "Dear Valued Customer," should raise a red flag. Companies are not likely to send e-mails requiring urgent requests for personal information.
- **Look out for account suspension or cancellation warnings.**
  Scammers often use these scare tactics to trick their victims into disclosing personal or financial information.

Here are some helpful tips and reminders that can be used to avoid and respond appropriately to e-mail threats.

- **Never directly respond to pop-up messages or e-mails asking for personal or financial information.**
  Contact the organization via telephone, or go to the organization's Web site to verify your updated information. Legitimate companies never ask for customer information by way of pop ups or e-mails.
- **Never click on links within e-mails.**
  Open a new browser window, and directly type in the organization's Web site address—never copy and paste the link from the e-mail into the address bar. Phishers create links that look like legitimate Web site URLs and then redirect their victims to phony Web sites.
- **Be cautious about opening e-mails or attachments, or downloading files from e-mails, even if they appear to be from someone you know.**
  Scammers often spoof e-mail addresses to trick victims into believing they are receiving e-mails from someone familiar. Best advice: If you receive an e-mail with an attachment or file, contact the sender to see if they actually sent you the e-mail. If so, save it to your hard drive, and run a virus scan before opening it.
- **Never use e-mail to provide personal or financial information to an organization.**
  E-mail is not a secure method of transmitting personal data. If you must provide your personal or financial information online, go to the organization's Web site and look for the lock icon, which is on the browser's status bar on the bottom left-hand corner or the "https" in the URL address bar, to ensure it is a secure Web site.

- **Use antivirus, spam filters, pop-up blockers, and antispyware software to further protect your system.**
  Antivirus software is essential to protect your computer from malicious codes that might accompany spam. Using spam filters and pop-up blockers will reduce the amount of spam you get and lessen the number of phishing attempts. Install antispyware software to detect programs that have unknowingly been installed to track your online activities or gather information without your knowledge. To ensure that new threats are recognized, enable your software programs to regularly update via the manufacturer's Web site.
- **Install a firewall.**
  A firewall creates a barrier between you and the Internet, providing a further layer of protection against computer threats. A firewall is especially important if you have a broadband or other high-speed Internet connection.
- **Act immediately if you believe you have been hooked by a phisher!**
  Notify your account holders immediately. Don't forget to contact the credit bureaus and request a fraud alert on your credit files.