Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

August 07, 2013

SPAM: DELIVERING MALWARE AND ADVERTISING DANGEROUS COUNTERFEIT GOODS

Cyber criminals have long used spam (unsolicited e-mails, usually containing links to websites selling counterfeit goods) as a method to make money and infect computers with malicious software (malware.) Spammers can send billions of these e-mails daily and some of them contain malware designed to steal usernames and passwords for online banking websites and harvest personal information such as names, addresses, or social security numbers.

Spam often takes the form of advertisements for illegal or counterfeit products. Buying these products is potentially harmful to the health and wellness of the purchaser because they are often low-quality or made with inferior materials. Counterfeit drugs are not only less potent than the real drugs, but are also unregulated and potentially dangerous. Many contain unknown ingredients that can interact badly with other medications and cause serious or life-threatening side effects.

Cyber criminals can also send spam e-mails that seem to be from a trusted individual such as a bank representative, a website administrator, or an employee of a company. These e-mails often look like they come from the purported source, but may have misspelled e-mail or website addresses. These e-mails try to get personal or financial information from the targeted recipients.

Cyber criminals are beginning to turn to other methods to deliver spam. Users of social media and social networking sites have begun to receive spam messages that often appear to be sent from trusted individuals or friends. Mobile devices are also becoming a target for spam and malware, usually being delivered through malicious applications. Cyber criminals can use this mobile malware to send text messages or harvest information about the phone or from the recipient’s contact list.

If you receive an e-mail that appears to be from a trusted source but are asked for personal or financial information, do not respond.

- Report the e-mail by calling or e-mailing the company’s customer service representatives. If the e-mail you are questioning is from your bank or credit card company, use the phone number on the statements you receive or the back of the credit card to get in touch.
- Never respond to e-mails asking for personal or financial information unless you ensure they are legitimate.
- Do not purchase products from spam e-mails, since they are very likely counterfeit and can be dangerous or deadly.
- If you receive a spam e-mail or message on social media or social networking websites, delete it immediately and do not click any of the provided links. These can contain malware that can take control of your computer and steal personal information.

If you have received a scam e-mail, file a complaint with the FBI’s Internet Crime Complaint Center, www.ic3.gov. For more information on scams, visit the FBI’s E-Scams and Warnings webpage, http://www.fbi.gov/scams-safety/e-scams.