U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

For Immediate Release
December 1, 2008

Washington, D.C.
FBI National Press Office
(202) 324-3691

Holiday Season Cyber Scammers Target Victims

The FBI is reminding people this holiday season that cyber criminals continue to aggressively seek ways to steal money and personal information. Scammers are using several techniques to fool potential victims including sending unsolicited e-mails that contain attachments such as electronic greeting cards containing malware (malicious software), setting up spoofing websites that look like legitimate commercial sites, and unleashing phishing and vishing attacks where individuals receive e-mails asking for personal data.

“These cyber scammers will do whatever they can to steal your money and personal information this holiday season and are trying many different ways to commit these crimes. The best way to protect yourself is to report these scams to law enforcement or the Internet Crime Complaint Center, IC3," said Shawn Henry, Assistant Director, FBI Cyber Division, Washington, D.C.

In the greeting card scam, the cards, which are also referred to as e-cards or postcards, are being sent via spam. Like many other Internet fraud schemes, the criminals use social engineering tactics to entice the victim, claiming the card is from a family member or friend. Although there have been variations in the spam message and attached malware, generally the spam directs the recipient to click the link provided in the e-mail to view the e-card. Upon clicking the link, the recipient is unknowingly taken to a malicious webpage.

Spoofing scams are when criminals create a false or shadow copy of a real website or e-mail in a way that misleads the recipient. All network traffic between the victim's browser and the shadow page are sent through the spoofer's machine. This allows the spoofer to acquire personal information, such as passwords, credit card numbers, and account numbers.

Even though the e-mail looks like the real thing, complete with authentic logos and working web links, it's a fake. The website where you're told to enter your account information is also fake. In some instances, really slick spoofers direct you to the genuine website, then pop up a window over the site that captures your personal information. The information entered does not go to the legitimate site, but rather to the spoofer's account. The information you entered will most likely be sold to criminals, who'll use it to ruin your credit and drain your account.

In phishing and vishing attacks, individuals report receiving e-mails or text messages indicating a problem with their account. They are directed to follow the link provided in the message to update their account or correct the problem. The link actually directs the individuals to a fraudulent website that looks legitimate where their personal information, such as account number and PIN, is compromised.

Other reported scams have included victims receiving an e-mail message asking them to complete an online survey. At the end of the survey, they are asked for their personal account information to allow funds to be credited to the account in appreciation for completing the survey. Providing this information will allow criminals to compromise the account.

Here are some tips you can use to avoid becoming a victim of cyber fraud:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders.
- Avoid filling out forms in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link that you are actually directed to.
- Log on to the official website, instead of "linking" to it from an unsolicited e-mail.
- Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine.

To receive the latest information about cyber scams please go to the FBI website and sign up for e-mail alerts by clicking on one of the red envelopes. If you have received a scam e-mail, please notify the IC3 by filing a complaint at www.ic3.gov. For more information on e-scams, please visit the FBI's New E-Scams and Warnings webpage.