

Malicious Code Circulating via Social Security Administration Phishing Messages

Original release date: November 24, 2009 at 2:42 pm Last revised:
November 24, 2009 at 2:42 pm

US-CERT is aware of public reports of malicious code circulating via phishing email messages that appear to come from the Social Security Administration. The messages indicate that the users' annual Social Security statements may contain errors and instruct users to follow a link to review their Social Security statement. If users click this link, they will be redirected to a seemingly legitimate website that prompts them for their Social Security number. If users enter their Social Security number and continue to the next page, they will be given an option to generate a statement. If users attempt to generate a statement, malicious code may be installed on their systems. This malicious code attempts to collect online banking traffic to gain access to the users' bank accounts.

US-CERT encourages users and administrators to take the following preventative measures to help mitigate the security risks:

- * Install antivirus software, and keep the virus signatures up to date.
- * Do not follow unsolicited links and do not open unsolicited email messages.
- * Use caution when visiting untrusted websites.
- * Use caution when entering personal information online.
- * Refer to the Recognizing and Avoiding Email Scams (pdf) document for more information on avoiding email scams.
- * Refer to the Avoiding Social Engineering and Phishing Attacks document for more information on social engineering attacks.

Users are encouraged to contact the Social Security Administration to verify the authenticity of any messages. Additional information will be provided as it becomes available.