OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Fraud Advisory

FOR IMMEDIATE RELEASE
July 1, 2016
https://oig.ssa.gov

Contact: Andrew Cannarsa
Phone: (410) 965-2671

Social Security Inspector General Warns Public About Email Phishing Scheme

The Acting Inspector General of Social Security, Gale Stallworth Stone, is warning citizens about a suspicious email "phishing" scheme that recently surfaced. The Office of the Inspector General (OIG) received reports that several hundred employees of a private company, with offices across the country, recently received an email message that appears to be from the Social Security Administration (SSA). The message alerts a recipient of "unusual" activity with his or her Social Security number (SSN).

The email subject line reads, "Review Your Social Security Activity", and while the email sender displayed is "Social Security Administration," the corresponding email address is ceriley@centurytel.net. The message includes a PDF attachment with the heading "Notification." It advises the recipient, "We detected something unusual about a recent use of your SSN" and "to help keep you safe, we required an extra security challenge." The message states that if the recipient did not recently use his or her SSN, then a "malicious user" might have misused the recipient's number. It asks the recipient to review recent activity via an embedded link, which links to a suspicious SSA-like site. Further, to appear legitimate, the notice includes SSA's official seal and the words "Social Security Administrator, United States Of America" in the signature.

This type of phishing scheme could lead to identity theft or Social Security benefit theft. Therefore, Acting Inspector General Stone urges all citizens to be extremely cautious when receiving requests to provide personal information over the internet or the telephone. "Don't provide your Social Security number, bank account numbers, or other personal information, including account passwords, over the internet or by telephone unless you know and trust the source requesting it," Stone said. "You should be extremely confident that the source is a legitimate entity, and that your information will be secure after you provide it."

Before clicking an embedded email link, try to verify the source. One method of verifying the true source is to hover over the linked text, without clicking, to reveal the destination address. For instance, in the email described above, the attachment includes the text "Review your activity," which links to www.ssa.gov.kerodun.net/activity. While ssa.gov appears in the destination address, the "kerodun.net/activity" portion of the address is suspicious; users should be vigilant of similar questionable web addresses.

If a person has questions about any communication—email, letter, text, or phone call—that claims to be from SSA, Stone recommends contacting a local Social Security office, or calling Social Security's toll-free customer service number at **1-800-772-1213**, 7 a.m. to 7 p.m., Monday through Friday, to verify its

Fraud Advisory

legitimacy. (Those who are deaf or hard-of-hearing can call Social Security's TTY number at 1-800-325-0778.)

Individuals may report suspicious activity involving Social Security programs and operations to the Social Security Fraud Hotline at https://oig.ssa.gov/report, or by phone at 1-800-269-0271, 10 a.m. to 4 p.m., Eastern Time, Monday through Friday. (Those who are deaf or hard-of-hearing can call the OIG TTY number at 1-866-501-2101.)

For more information, please contact Andrew Cannarsa, the OIG's Acting Communications Director, at (410) 965-2671.