

Subject: Security Warning — Latest Fraud — Stimulus Payments — For newsletters, other uses

Dear Colleagues,

As may be expected, the prospect of stimulus payments has received considerable interest from parties wishing to fraudulently obtain information from persons who may believe they are receiving money from the federal government. Therefore, please be advised of the following:

Phishing scams are circulating via fraudulent U.S. Internal Revenue Service emails offering users stimulus package payments. These emails include text that attempts to convince users to follow a link to a website or to complete an attached document. The website and document request that the user provide personal information.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

You are encouraged to do the following to avoid being a victim:

- Do not follow unsolicited web links received in email messages.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not respond to email solicitations for personal information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a web site's security.
- Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- **If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a web site connected to the request; instead, check previous statements for contact information.**
- Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org/phishing_archive.html).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic

s/

Emmett Schmarsow, Prog. Mgr. COAs & Senior Centers, ELD