INVESTIGATOR TIPS

How to Respond to a Suspicious IRS-related Communication

The IRS does not initiate contact with taxpayers by any type of electronic communication, including email, text messages, and social media channels. Here the IRS gives direction for handling a suspicious IRS-related communication.

If you receive an email claiming to be from the IRS that contains a request for personal information:

- Do not reply.
- Do not open any attachments. Attachments may contain malicious code that will infect your computer.
- Do not click on any links.
- Forward the email as-is, to phishing@irs.gov. After you forward the email, delete the original email message you received.

  Note: Please forward the full original email to phishing@irs.gov. Do not forward scanned images of printed emails as that strips the email of valuable information only available in the electronic copy.

If you discover a website on the Internet that claims to be the IRS but you suspect it is bogus:

- Send the URL of the suspicious site to phishing@irs.gov. Please add in the subject line of the email, "Suspicious website."

If you receive a phone call from an individual claiming to be with the IRS but you suspect they are not an IRS employee:

- Ask for a call back number and employee badge number.
- Contact the IRS to determine if the caller is an IRS employee with a legitimate need to contact you.
- If you determine the person calling you is an IRS employee with a legitimate need to contact you, call them back.

If you receive a paper letter via mail from an individual claiming to be the IRS but you suspect they are not an IRS employee:

- Contact the IRS to determine if the mail is a legitimate IRS letter.
- If it is a legitimate IRS letter, reply if needed.
- If caller or party that sent the paper letter is not legitimate, contact the Treasury Inspector General for Tax Administration at 1-800-366-4484.

A service of the Investigators of Kroll Advisory Solutions

These materials are derived from the research and discovery activities of Kroll Advisory Solutions Fraud Specialists and Licensed Investigators, and have been gathered from personal, historical, and aggregated experience performing specialized restoration services on behalf of Identity Theft victims. While believed to be accurate, these materials do not constitute legal advice, and are not guaranteed to be correct, complete or up-to-date. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into a language or computer language, in any form by any means, electronic, mechanical, optical, chemical, manual or otherwise, without the express written consent of Kroll Advisory Solutions. These materials are provided for informational purposes only. MEM-057-2013-1-28

If you receive an unsolicited fax (such as Form W8-BEN) claiming to be from the IRS, requesting personal information:

- Contact the IRS to determine if the fax is from the IRS. If you learn the fax is not from the IRS, please send the information via email at phishing@irs.gov. In the subject line of the email, please type the word 'FAX'.

If you receive a text message or Short Message Service (SMS) message claiming to be from the IRS:

- Do not reply.
- Do not open any attachments. Attachments may contain malicious code that will infect your computer or mobile phone.
- Do not click on any links.
- Forward the text as-is, to 202-552-1226. Note: Standard text messaging rates apply.
- If possible, in a separate text, forward the originating number to 202-552-1226.
- After you forward the text, please delete the original text.