INVESTIGATOR TIPS

Beware of "ishing"

A favorite tactic of fraudsters is to pretend to be someone that they are not in order to trick someone else into giving up sensitive personal information (SPI). They usually represent themselves as a legitimate, often well-known business and seek the victim's Social Security number, bank account information, or credit card data to use for their own fraudulent purposes. There are a number of methods a perpetrator can use to attempt to steal such desirable information, and each has its own clever name that ends in "-ishing."

- Phishing occurs via email.
- Fax phishing occurs via facsimile (fax) machine.
- Vishing occurs via telephone voice messaging systems.
- Smishing occurs via SMS (short messaging service), also known as texting.

Several characteristics are common to any "ishing" scam. For example, the message frequently heightens the recipient's sense of urgency by either stating they will lose access to something (e.g., bank account) if they don't respond quickly, or they will gain a benefit (e.g., faster tax refund) that requires certain personal details to access. The victim will be prompted to share the information by return email, fax, phone call, or text message or may be asked to visit a particular website. Once the person responds to the initial point of contact, all other information provided is designed to make the responder comfortable about sharing SPI.

To avoid becoming a victim, remember the following advice:

- Don't react too quickly. It's very important to remain calm, even if you think you are about to lose a service or if you think a punitive action is about to be taken. Remember, if you are already doing business with the company represented, they should already have all of your information—why would they need to suddenly demand it from you?
- If a communication is unsolicited, don't follow the directions to click, call, fax, or text. Instead, independently verify that the message was sent by a legitimate source. This could include visiting the company website, calling customer service directly, or some other form of contact, as long as it is initiated by you.
- The name that appears on your caller ID service may not be the person making the call.
- No government agency, and typically no legitimate private organization, will send an email, fax, or text message to solicit SPI from you.

A service of the Investigators of Kroll – These materials are derived from the research and discovery activities of the Fraud Specialists and Licensed Investigators of Kroll, 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 Cyber Security & Information Assurance.These materials are provided for informational purposes only. MEM-040-2011-12-27