HINSHAW

Alerts

Avoiding Social Engineering Scams

October 16, 2018
Cyber Alert

Download a PDF of the Alert

Risk Management Question: October is cyber security awareness month. What steps are you taking to avoid common Internet scams?

The Issue: Hackers and their exploits are growing more sophisticated by the day. Avoiding their scams is becoming even more difficult. In 2017, 1.4 billion user names and passwords were accessed on the dark web via an electronically searchable database. Any hacker can purchase malware and phishing tools on the dark web.

Risk Management Solution: Be diligent in combating the ever-evolving threats. KnowBe4 has created a great one-page infographic describing 22 Social Engineering Red Flags that you should be on the lookout for: https://cdn2.hubspot.net/hubfs/241394/Knowbe4-May2015-PDF/SocialEngineeringRedFlags.pdf?t=1539009732279

Here are some ways you can recognize online threats in your email inbox:

1. Never click on a link or attachment in an email from someone you don't know or with whom you have never done business.
2. Don't open attachments or click on links you were not expecting to receive even from a known sender. Call the sender at a trusted number and confirm he or she sent it.
3. Carefully review the sender's email address and confirm that it is accurate and does a spoofed email address or domain extension. Hackers love to replace the letter "m" with the letters "n" and "r". Do you ordinarily communicate with that sender or know the sender personally, or have a business relationship with the sender? Take special care if the email's subject matter is not related to your practice areas or job responsibilities. If the email was sent from someone in your organization, assess if the subject matter or the text of the email seems unusual or out of character.
4. Review all of the email recipients. Were you carbon copied on an email without knowing all the other recipients? Ask yourself why? Identify the other recipients, especially if it seems to be an unusual group, before you send any reply.
5. Never click on any hyperlinks in an email if the hyperlink is misspelled or if it is the only information contained in the email. Also, check the hyperlink in the text by hovering over the hyperlink with your mouse to ensure it will send you to the advertised link.

Attorneys

Lauren N. Kus

Steven M. Puiszis

Service Areas

Cyber Security for Law Firms

Law Firm Cyber Alerts

Lawyers for the Profession®

6. Did you receive the email at an unusual time? If so, don't open it. Call the sender and confirm he or she sent it.
7. Is the email's subject irrelevant, unusual, or a reply to something you did not initiate? If so, don't open it.
8. Don't open dangerous file types, such as .exe that will try to run a script on your computer.
9. Do you feel uncomfortable? Trust your gut, and don't open the email.
10. If you ever click on something and a dialog box opens and you are asked to supply additional information, click on something else to open the attachment or enable a later software version, stop. Immediately close out of the email and ask to have a computer scan performed on your machine.

These same rules apply to text messages received on your phone. Remember, always think before you click.