UTIA INSTITUTE OF AGRICULTURE
THE UNIVERSITY OF TENNESSEE

IMPORTANT INFORMATION ABOUT SPEAR PHISHING

Spear phishing seems to be a never-ending threat. Please know that your supervisor will not send you an email asking you to buy some gift cards and then ask you to email him/her the codes. Here are the key things to remember:

- Spear phishing attacks are targeted attacks.
- A hacker will troll departmental websites to find who is in charge.
- The hacker will also look at the employees so he knows who to target.
- The hacker then looks at the departmental and employees' social media sites.
- If the hacker is questioned, he will (pretending to be your boss!) ask you personal questions from the information he has seen on the social media sites.
- Even if you do not use social media, you can bet someone, somewhere has innocently posted something that can be garnered by the hacker about you (i.e., departmental site or social media site).
- You will notice that there is no request to click a link.
- Spear phishing is about the hacker getting free money, instead of compromising your computer.
- The message seems urgent and the "supervisor" wants you to respond via email only.
- The original message truly looks like it is from your supervisor's UT email address, but the address is being spoofed.
- If you do click on "Reply," you will notice that the reply-to address changes to <*xxxxx*.utk.edu@gmail.com>.
- If you see this, close the message and delete.
- Never, ever make the requested purchase of gift cards because your supervisor won't ask this!
- Contact me (sandy@tennessee.edu) and/or forward the email with its Internet Headers using these instructions: https://ag.tennessee.edu/security/Documents/ReportPhishing.pdf.