UTIA INSTITUTE OF AGRICULTURE
THE UNIVERSITY OF TENNESSEE

WORKING SECURELY FROM HOME

This seems to be a very opportune time to remind everyone about how to work securely from home.

1. **You**: First and foremost, technology alone cannot fully protect you; you are the best defense. Attackers know the easiest way to get what they want is to target you, not your computer, by tricking you into giving up sensitive information, such as passwords or data, by pretending to be a supervisor (think recent spear phishing attacks!), among other methods. Even when working from home or working while traveling, be suspicious if you are asked for information over the phone or in an email. Don't act until you have assessed the situation. Call the person or send them a new email to verify the request. Common sense will avert most attacks.

2. **Home Network**: Almost every home network starts with a wireless (Wi-Fi) network. This is what enables all your devices to connect to the Internet. Most home WiFi networks are controlled by your Internet router or a separate, dedicated wireless access point. Do the following:

    - Change the default administrator password to your Internet router or wireless access point, whichever is controlling your WiFi network. The admin account is what allows you to configure the network settings.

    - Ensure only people you trust can connect to your WiFi network. Do this by enabling strong security. Never use an open network, as it has no security at all. If given a choice, choose WPA2 or WPA3, as they are the strongest WiFi security. By enabling strong security, a password is required for anyone trying to connect to your home network, and once connected their online activities are encrypted.

    - Ensure the password used to connect to your wireless network is a strong password and that it is different from the admin password.

    If you aren't sure how to do these things, ask your Internet Service Provider, check the documentation that came with your Internet router or wireless access point, or check the ISP's website.

3. **VPN:** As mentioned in my January email, policy requires the use of a VPN when connecting to the UT network when at home or traveling. Most UT apps that require the use of the VPN won't let you in without being connected to the VPN first (e.g., IRIS). It is still a best practice to log into the VPN first so you are protecting data in the apps that

have not been added to the other VPN-requiring apps. You can get Pulse Secure here: https://webapps.utk.edu/oit/softwaredistribution/.

4. **Passwords**: When a site asks you to create a password, create a strong and unique passphrase (e.g., iL0veTheNYY@nkees!) instead. The more characters a passphrase has, the stronger it is. Using a unique passphrase means using a different one for each online account. If one passphrase is compromised, all of your other accounts are still safe. And please enable two-factor authentication whenever possible.

5. **Updates**: Make sure each of your Institute-owned **and** personally-owned IT assets are running the latest version of its software. The easiest IT assets to compromise are the ones with vulnerabilities because they aren't being updated. By ensuring your all devices are installing new updates promptly, you make it much harder for someone to hack you. To stay current, simply enable automatic updating whenever possible.

6. **Children / Guests**: Make sure your family and friends understand they cannot use Institute-owned IT assets assigned to you. Someone else could accidentally erase or modify data, or infect the IT asset. Please remember that you, an Institute employee, is responsible for that asset and the data on it.

As always, if you ever have doubts, questions, concerns, or comments, please don't hesitate to let me know!

Sandy Lindsey, CISO
sandy@tennessee.edu