UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

Dear UC ANR Colleagues,

Cyberattacks against many organizations are increasing, and more than 90 percent of all breaches start with a malicious email. Although we have the necessary network safeguards in place, we rely on you as an essential first line of defense against attackers. Below are ways we're working together to strengthen our security, along with some reminders about the specific actions you can take to keep cybercriminals out of UC ANR.

Ransomware is increasingly being used by hackers to extort money from companies. Ransomware is a type of malicious software that takes over your computer and prevents you from accessing files until you pay a ransom. Although we maintain controls to help protect our networks and computers from this type of attack, with the quickly-changing attack scenarios, we rely on you to be our first line of defense.

Here are some simple things you can do to help UC ANR avoid a ransomware/malware attack:

Think before you click. The most common way ransomware enters corporate networks is through email. Often, scammers will include malicious links or attachments in emails that look harmless. To avoid this trap, please observe the following email best practices:

- **Do not click on links or attachments from senders that you do not recognize.** Be especially wary of .zip or other compressed or executable file types.
- **Do not provide sensitive personal information (e.g. usernames and passwords) over email.**
- **Watch for email senders that use suspicious or misleading domain names.**

Pay careful attention to the email address. If you can't tell if an email is legitimate or not, please double-check the email id it came from.

When in doubt, do not click on a link. Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

If you suspect ransomware or malware, contact ANRIT at help@ucanr.edu
If your computer is infected with ransomware, you will typically be locked out of all programs and a "ransom screen" will appear. In the unfortunate event that you click a link or attachment that you suspect is malware or ransomware, please notify IT immediately.

Protect yourself from becoming phish bait
There are certain indicators to look for on emails, text messages, or phone calls that can help you uncloak the scam: requests for personal information or passwords, unexpected messages or attachments, and spelling errors.

Phone phishing is the latest ploy being used by cybercriminals to extract information from the unsuspecting. These scams are more insidious than email phishes because most people believe their telephone calls are secure. Phone phishers pose as if they are from a legitimate organization to trick you into revealing your private information. Some UC ANR employees have received phone calls from a

wireless number. The caller states they are with IT and claims a “system update” needs to be run. This is a phishing attempt designed to gain access to our network systems and sensitive information with the intent to commit identity theft or cause financial harm. Note that UC ANR does not communicate system upgrades by phone. Only teams within UC ANR, not an outside entity, manage the function and security of our network systems.

Typical phone phishing scam signs:

- Caller fails to introduce themselves or the organization they are calling from.
- Caller requests sensitive business or personal information (credit card or banking information, Social Security number, address, passwords, etc.).
- Caller requests access to your device or system (for example, through the use of a non-standard application or website).
- Caller creates an unnecessary sense of urgency or uses threatening language.

If you receive one of these calls, hang up without sharing any information and report the incident to help@ucanr.edu

If you think an email or text smells phishy, take action! Use the spam function in Outlook and/or forward suspicious emails to help@ucanr.edu.

Please remain vigilant and remember that as a UC ANR employee you are our first and most important line of defense against cyberattacks. Thanks again for helping to keep our network and our people safe from these cyber threats.

Regards,

Sree Mada
Chief Information Officer