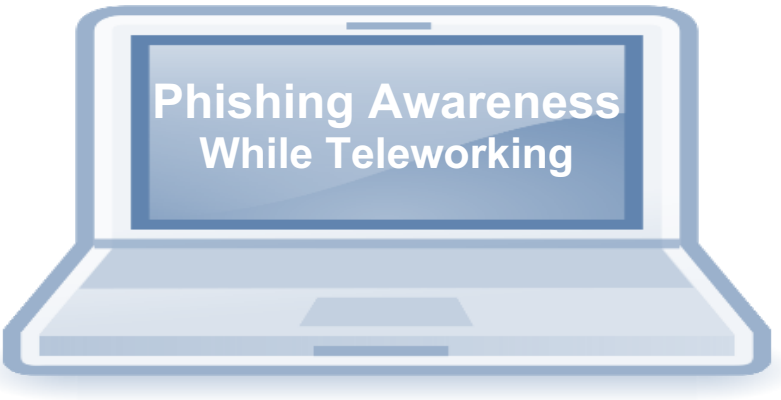
North Carolina Agricultural and Technical University
Information Technology Services Division
Information Security Services



The university is experiencing a rise in phishing attacks as the number of employees teleworking increases. Phishing scams include job offers, impersonations, and tricking employees into making fraudulent purchases. Below are phishing awareness behaviors to teleworking securely.

HOW TO AVOID GETTING PHISHED

- **BEWARE** of unsolicited phone calls, emails, and text messages requesting cash, checks, gift cards, passwords/PINS, credit card numbers, ID numbers (begins with 95), social security numbers, checking account, or any confidential information.
- **BEWARE** of cybercriminals impersonating university administrators, supervisors, and co-workers to trick you into downloading malicious attachments or clicking on links that ask for your passwords or other confidential information.
- **BEWARE** when someone that you know sends you an email that is out of the ordinary.
- If the offer is too good to be true, treat it as a scam.
- **PAUSE** and **THINK** before you **CLICK**.
- **ALWAYS** hover over links with your mouse pointer to display the full URL. If it leads somewhere that doesn't fit with the email, DO NOT CLICK!

REPORTING A SUSPECTED PHISH

1. **DO NOT RESPOND** to the email
2. **FORWARD** the email to **informIT@ncat.edu**
3. **DELETE** the email from your mailbox!

YOU Are KEY To Cybersecurity!