

**CYBER SECURITY
KEYPOINTS
November**

*From the County
Network Security
Cooperative*



Pretexting:

False Identity Tactics

Hackers may impersonate co-workers or authority figures, creating a fake scenario (pretext) to request sensitive data. Verify any such requests via another communication channel before acting on them.



Spear Phishing

Unlike general phishing, spear phishing uses personal information to craft highly targeted attacks. Hackers may know details about your role or recent activities—always verify unexpected messages, even if they seem familiar.



Social Media Reconnaissance

Social engineers gather information from social media profiles to craft attacks. Publicly shared information about your job, hobbies, or friends can be used to manipulate you. Be mindful of what you post online.



Vishing:

Voice-Based Phishing

Hackers may use phone calls (vishing) to trick you into revealing sensitive info, pretending to be your bank or county's IT department. Hang up and call the official number to verify the request.

The County Network Security Cooperative is a collaboration of partners including:



- AND -



Disclaimer: This document reflects current guidance and is subject to change due to the evolving cyber security environment.