

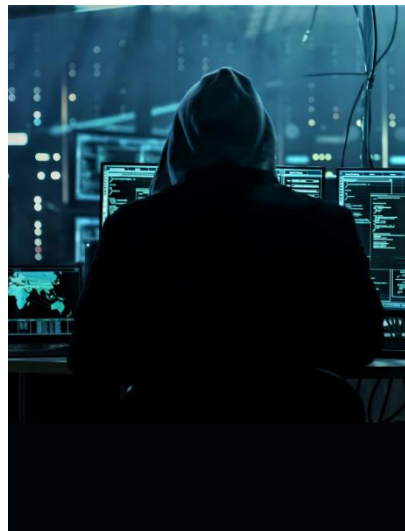
CYBER SECURITY KEYPOINTS October

From the County
Network Security
Cooperative



Beware of Public Wi-Fi for Sensitive Tasks

When using public Wi-Fi, avoid accessing sensitive accounts or sharing personal information. Hackers can easily intercept data over unsecured connections. Use a Virtual Private Network (VPN) to keep your internet activity secure.



Check for HTTPS on Web sites

When entering sensitive information online, always ensure the website starts with **https://**. This means the site is encrypted, protecting your data from being intercepted by hackers.



Verify Unexpected Password Reset Requests

If you receive an email prompting you to reset your password for an account you didn't request, be cautious. Social engineers might be trying to gain access. Always initiate password resets directly from the website, not through email links.

Fake Security Alerts

Beware of urgent "security alerts" claiming that your account has been compromised. These phishing emails often direct you to fake login pages to steal your credentials. Always visit websites directly rather than clicking on links in emails.

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.