CYBER SECURITY KEYPOINTS

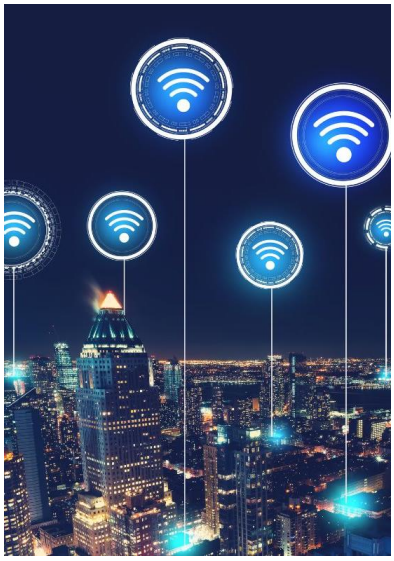
July

From the County Network Security Cooperative

THE RISKS OF PUBLIC WiFi

*A common threat on the wild web is a sneaky thing called adversary-in-the-middle (AiTM) attack, a fancy term for eavesdropping on your data. Picture this: bad guys intercepting and reading everything between your device and a service - a total privacy invasion! And if that's not enough, scammers kick it up a notch with phishing emails, pretending to be your pals, and getting you to spill your private info. Stay sharp, let's outsmart these villains together!

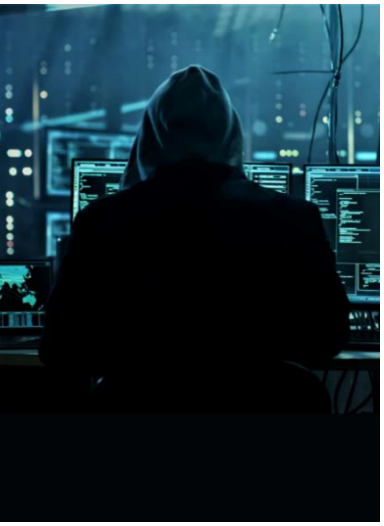
*Let's talk encryption. Encrypted networks send information between the device and the router in a "secret code" requiring a key to see information. Most WiFi routers have encryption turned off by default. Connecting to an unencrypted network is like rolling out the red carpet for scammers to snoop on your web traffic. Public WiFi may be encrypted, but we are not throwing a superhero guarantee on that. Stay cautious as uncertainty can be a playground for potential risks.



PUBLIC WiFi

While the convenience of public WiFi is undeniable, offering free internet access at various locations such as restaurants, hotels, and airports, it is important to recognize the associated risks. These connections, though useful, can expose users to potential cyberattacks. Therefore, it is crucial to adopt safe online practices to protect both personal and business data.

Stay safe out there!



*Another sneaky trick involves attackers who slip malware to your computer through software vulnerabilities, which are security holes in operating systems or software programs. They craft code, exploit weaknesses, and inject malware undetected onto your device.

*WiFi snooping involves cybercriminals using fancy software to eavesdrop on WiFi signals, giving them the power to seize your entire online life. Peep at your web history, snatch login details, and even hijack your online hangouts.

*Malicious hotspots, or rogue access points, masquerade as legit networks with reputable sounding names. For instance, "Sleeptyght Inn" vs the correct "SleepTight Inn." Connect to the wrong one, and your personal info becomes their VIP guest. Don't fall for WiFi illusions.

FOR SAFE USAGE

*Protect that secret identity and avoid sensitive info on public WiFi.
*Use a VPN: a virtual private network adds an extra security cape to the connection.
*Stick to encrypted HTTPS websites for more security.
*Utilize browser extensions such as "HTTPS Everywhere" – a digital superhero cloak for your browsing.
*Turn off automatic connections on your devices.
*Turn off file sharing before accessing public WiFi.
*Use a trusty sidekick like two factor authentication to protect passwords.
*Update like a hero! Up to date Operating Systems are security patches for your digital fortress.
*Remember to log out all services used & make sure your device will "forget the network" – no digital breadcrumbs.
*Use antivirus software – this is like a superhero suit for your device.

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

NEBRASKA ASSOCIATION OF COUNTY OFFICIALS

- AND -

NIRMA
Serving County Government

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