CYBER SECURITY KEYPOINTS
February

From the County Network Security Cooperative

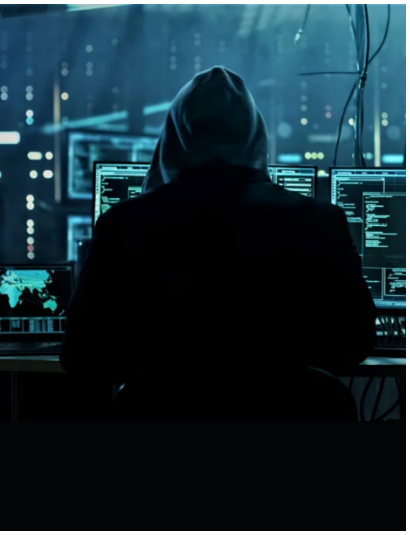
RANDOM DRIVES

NEVER plug in a piece of removable media found in the wild! Let's be frank, do you lock your car? Using a strange removable drive is like handing over your keys to a criminal. Welcoming them to wreak havoc in your virtual world. It's just asking for trouble!

Even random drives found in the office should not be assumed safe—especially if found in a well-traveled space of the building—as there is always the potential that it was left maliciously to gain access to devices and networks. Even if the owner is not a hacker it could contain malware, viruses, or other unintentional downloads that could compromise security.

REMOVABLE MEDIA

What is removable media you might ask? Well, we've all probably seen a version or two, most likely even used one, but perhaps weren't aware that something so small and innocent looking could be potentially lethal to an organization's security. Portable devices such as a USB drive (or flash drive, or dongle, or stick, or thumb drive or whatever one chooses to call it), an external hard drive (for computer back-ups), CDs, DVDs, or SD cards are all removable media.



WHAT TO DO

Files on removable media can be accessed without putting networks, accounts, and devices at risk. If you come across a stray at work, you should hand it over to the IT department. Not at work? Proceed with caution and don't let curiosity get the best of you!

Here's how you can reduce risk:

**Use a data blocker: little connectors used as a line of protection between the device & USB drive.*

**Use an "air-gapped" computer (this is "nerd talk" for a device not connected to the internet).*

***Do nothing:** Are you uncomfortable with more advanced cyber security protocols? Then don't mess with the device. If it is worth anything to the owner, they will come looking for it.*

BEST PRACTICES

*Install anti-malware/anti-virus software on computers.

*Disable auto-run and autoplay features.

*Password-protect your removable media & devices.

*Remove all sensitive material from removable media once data is transferred.

*Use encryption.

The most effective protocol is employee security awareness training. Educate on the importance of data security and provide resources to handle removable media properly. Organizations that follow these practices are better positioned to defend against threats.

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.