TECH LINK

Cybersecurity Tips for a Safer Digital World

By Abby Berry, National Rural Electric Cooperative Association

Did you know the average household with internet access owns about 17 connected devices? That figure covers a wide range of electronics, including smart phones, computers, streaming devices, smart speakers, home assistants and more. Given our increasing reliance on internet-connected technologies, the likelihood of new cyber threats is ever-present.

Maquoketa Valley/MVlink is deeply committed to ensuring our local system is safe and secure. We routinely monitor and manage cyber risks, and we work together with other co-ops to share the latest advancements in cybersecurity measures that make us stronger. But you can help, too.

When we all work together to stay safe online, we lower the risk of cyber threats to our systems, online accounts and sensitive data.

October is National Cybersecurity Month, and while good cyber hygiene should be practiced year-round, we'd like to share a few cybersecurity tips to help you bolster your online safety.

- **Learn how to spot and report phishing attempts.** Phishing occurs when criminals use phony emails, direct messages or other types of digital communications that lure you to click a bad link or download a malicious attachment. If you receive a suspicious email or message that includes urgent language, offers that seem too good to be true, generic greetings, poor grammar or an unusual sender address, it could be a phishing attempt. If you spot one, report it as soon as possible—and don't forget to block the sender. (If you receive a suspicious work email, report it to the appropriate IT contact. Suspicious messages that are delivered to your personal email or social media accounts can also be reported.)

- **Create strong, unique passwords.** When it comes to passwords, remember that length trumps complexity. Strong passwords contain at least 12 characters and include a mix of letters, numbers and symbols. Create unique passwords for each online account you manage and use phrases you can easily remember.

- **Enable multi-factor authentication when available.** Multi-factor authentication (also known as 2-factor authentication) adds an extra layer of security to your online accounts. These extra security steps can include facial recognition, fingerprint access, or one-time codes sent to your email or phone.

- **Update software regularly.** Software and internet-connected devices, including personal computers, smartphones and tablets, should always be current on updates to reduce the risk of infection from ransomware and malware. When possible, configure devices to automatically update or notify you when an update is available.

Let's all do our part to stay cyber smart and create a safer digital world for all. Visit *staysafeonline.org* to learn about additional cybersecurity tips.