CORPORATE SUPPORT SERVICES

Volume 22 | Quarterly Newsletter | October- December 2025

Building a Cyber Strong America

Cybersecurity Awareness Month (October) is an international initiative that highlights essential actions to reduce cybersecurity risks. This year's theme is **Building a Cyber Strong America**, highlighting the need to strengthen the country's infrastructure against cyber threats, ensuring resilience and security.

Cybersecurity is more than an IT issue—it's a public safety and economic security priority. Many organizations are part of the nation's **critical infrastructure**, from local utilities and transportation systems to hospitals, schools and public safety agencies; and many small and medium size businesses play an important role in critical infrastructure, who might be suppliers, contractors, vendors, manufacturers, or another role that helps keep critical infrastructure operating.

When these systems are disrupted, the impact is immediate and far-reaching. Protecting them starts with each person's daily actions online.

The **Cybersecurity and Infrastructure Security Agency** (CISA), the federal lead for the campaign, provides resources for organizations to help educate employees and other organizations that are connected in some way. Cybersecurity Awareness Month is supported by corporations, government agencies, businesses, tribes, non-profits and professionals committed to cybersecurity education and protecting our communities.

The campaign builds on past efforts, empowers everyone to take core steps to protect against online threats, and offers additional ways to help keep the nation's critical infrastructure secure against cyber threats. This year, there are additional recommendations for small/medium business and state, local, tribal, and territorial government organizations that own, operate, or support critical infrastructure. We live in a highly connected world, with more sensitive information online than ever before. This convenience comes with risks. All organizations that are part of the nation's critical infrastructure and supply chain have an important role in cybersecurity.

Here are some tips that are mentioned.

As you can see these are steps and training Summit provides throughout the year to help educate and prepare our employees about Cyber threats. I included these so you will see that we are on the right path to protect ourselves, our families and our business. If these topics remind you of the training you have received then take pride in yourselves and know that you are doing your part to help. Keep up the good work and keep those questions and concerns coming. It takes a village to raise a family. Here at Summit, we should consider ourselves as part of a family and this family is on it.

1. **Teach Employees to Avoid Phishing**: Phishing tricks employees into opening malicious attachments or sharing sensitive information. Train staff to recognize and report suspicious activity.

2. **Require Strong Passwords**: Strong passwords are a simple but powerful way to block criminals from accessing your accounts through guessing or automated attacks. Make them mandatory for all users.

3. **Require Multifactor Authentication (MFA)**: MFA—also known as 2-factor authentication—adds an extra layer of security beyond passwords. Require it to make accounts significantly more secure. Use phishing resistant MFA where available.

4. **Update Business Software**: Outdated software can contain exploitable flaws. Promptly install security updates and patches to keep your systems protected.

If you have any questions, please contact Caty Savage, FSO, at (850) 312-9356 or csavage@summittech.us