CITY OF BRYAN
The Good Life, Texas Style.™

SAFEGUARDING
THE NATION'S CRITICAL INFRASTRUCTURE

Our daily lives depend on 16 critical infrastructure sectors, which supply food, water, financial services, public health, government services, communications, transportation, and power along with other critical functionality. A disruption to these systems, most of which are operated via the Internet, can result in significant and even catastrophic consequences. Week 4 highlights the roles YOU can play in keeping it safe.

CHAMPION
National Cybersecurity Awareness Month

Did YOU know that the City of Bryan is home to 10 of these?

Commercial Facilities – several large manufacturing facilities are in the city limits

Dams – Lake Bryan

Defense Industrial Base – Several defense contractors are in the B/CS area and TEEX provides many critical training classes.

Emergency Services – Our very own Police and Fire Departments, Brazos County Emergency Communications District (Brazos County 911).

Energy – We have power production, transmission and distribution right here in Brazos County.

Food and Agriculture – Sanderson Farms processing plant and many farms and ranches depend on the city's resources.

Government Facilities – Several federal and state government offices are located in Bryan.

Healthcare and Public Health – CHI St. Joseph hospital and county health offices are in Bryan.

Transportation Systems – The regional TX Department of Transportation (TXDoT) office is in Bryan.

Water and Wastewater Systems – We operate water and wastewater services.

So what can YOU do locally to help protect OUR national critical infrastructure assets?

The Department of Homeland Security (DHS) and the U.S. Cyber Emergency Readiness Team (US-CERT) provides the following tips that YOU can do to help protect OUR critical infrastructure.

Keep a clean machine. Keep the security software, operating system, and web browser on your devices updated. Keeping the software on your devices up to date will prevent attackers from being able to take advantage of known vulnerabilities.

Enable stronger authentication. Always enable stronger authentication for an extra layer of security beyond the password that is available on most major email, social media, and financial accounts.

Stronger authentication (i.e., multi-factor authentication that can use a one-time code texted to a mobile device) helps verify that a user has authorized access to an online account. For more information about authentication, visit the new Lock Down Your Login Campaign.

When in doubt, throw it out. Links in email and online posts are often the way cyber criminals compromise your mobile devices. If it looks suspicious—even if you know the source—it's best to delete or, if appropriate, mark it as "junk email."

Make your passwords long and strong. Use complex passwords with a combination of numbers, symbols, and letters. Use unique passwords for different accounts.

Secure your Wi-Fi network. Your home's wireless router is the gateway entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network and your digital devices by changing the factory-set default password and username.

Safer for me, more secure for all: What you do online affects everyone. Good online habits help the nation's digital community.