

CYBERSECURITY SAFETY



Cyber threats are real — and growing. Whether you're at home, work, or on the go, simple steps can keep your data safe

Use Strong Passwords

- At least 12 characters
- Use a mix of letters, numbers & symbols
- Avoid names or common words

Enable Multi-Factor Authentication (MFA)

- Add an extra layer of protection to logins
- Keep Software Updated
- Apply patches and updates to apps, operating systems, and browsers

Think Before You Click

- Don't open suspicious links or attachments
- Watch out for phishing emails

Back Up Your Data

- Use secure cloud storage or external drives

Prepare Today. Ready Tomorrow.
northtexasprepares.nctcog.org

COMMON CYBER THREATS

- Phishing: Fake emails, texts, or websites trying to steal info
- Ransomware: Malware that locks your files until you pay
- Identity Theft: Stolen personal info used for fraud
- Social Engineering: Manipulating you into revealing information

CYBER THREATS Q&A

How do I spot a phishing attempt?

- Generic greeting (“Dear User”)
- Urgent or threatening language
- Unusual links or attachments
- Mismatched email addresses

What should I do if I get hacked?

- Change passwords immediately
- Notify your IT department or provider
- Check your financial accounts
- Run antivirus/malware scans