Avoiding Social Engineering & Phishing

Social engineering - human interaction to obtain or compromise information about a person, organization or system.

Phishing - a form of social engineering using email, text messages, voice messages or malicious websites to solicit personal information by posing as a trustworthy organization.

Common indicators of phishing attempts
- Suspicious sender's address
- Generic greetings and signature
- Spoofed hyperlinks and websites
- Suspicious attachments

Avoid being compromised
- Be suspicious of unsolicited phone calls, visits, or email messages requesting personal or organizational information.
- Don't send sensitive information over the internet before checking a website's security…does the address start with "https"?
- If you are unsure whether an email request is legitimate, contact the TCESC tech department (tcesc.techdept@trumbullesc.org)
- Enforce multifactor authentication (MFA).

Below is an example of a phishing email

If you have received a similar email, please don't respond to the email and don't click on any web links.

If you do click on any web links, please do the following immediately…
Reboot your computer to sever any malicious network connections and clear the system's memory
Reset your email password immediately
Email tcesc.techdept@trumbullesc.org for support

For more information, please review the resources below.
https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
https://www.phishing.org/common-phishing-scams