

Texts, Emails, and Phone Calls... oh my!

Bethany Graves, IS Auditor

Division of Local Government Audit

CCFO/CMFO Training

11.6.25

TENNESSEE COMPTROLLER OF THE TREASURY



1



Nathan Abbott



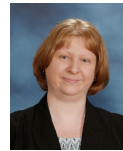
Twyla Pratt



Bethany Graves



Julie Davis-Shelton



Jeni Paladeni



Shania Leonard



Elisha Crowell



Rachel DePriest



Chrisvonta Smith



Barbara Shults

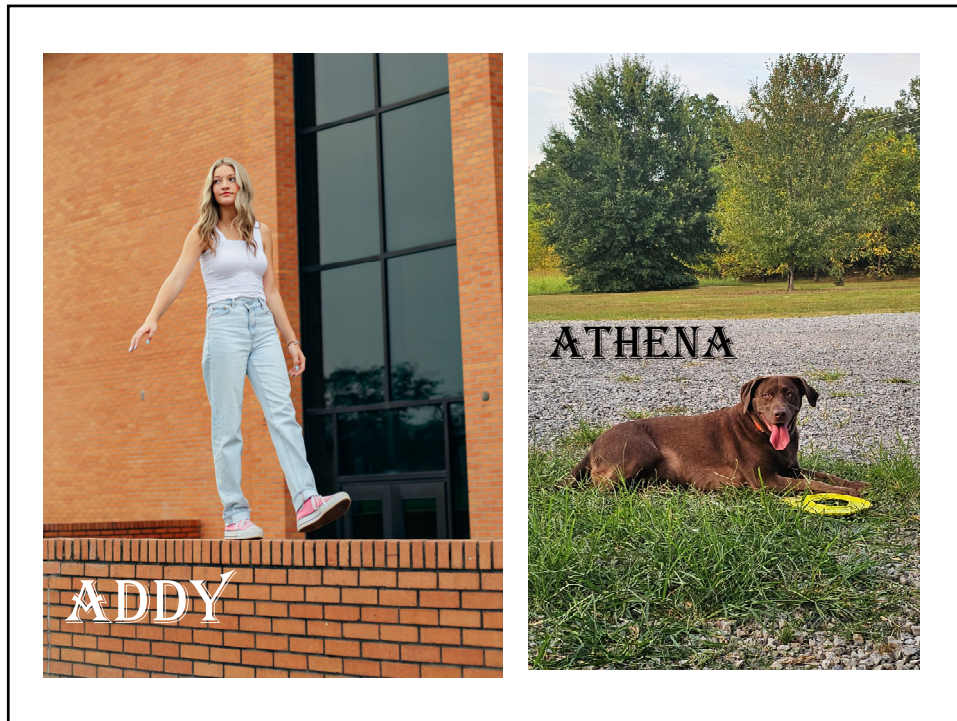


Emma Hayse

TENNESSEE COMPTROLLER OF THE TREASURY



2



3

Disclaimer

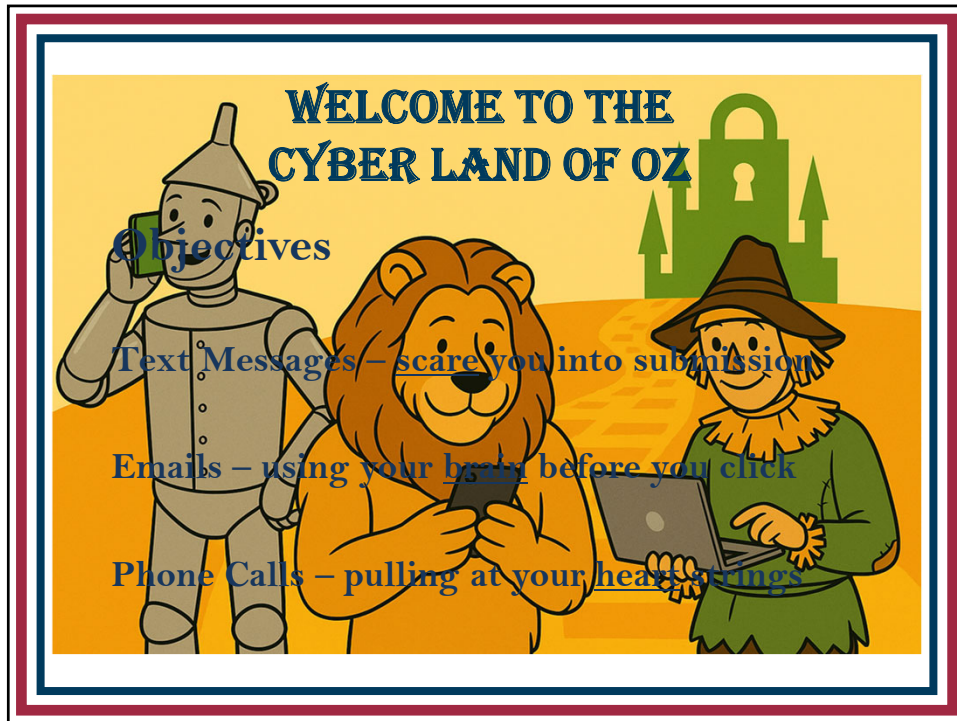
The Opinions expressed during this presentation are my own.

They do not necessarily represent the views of the Tennessee Comptroller of the Treasury, his representatives, or the Tennessee Department of Audit.

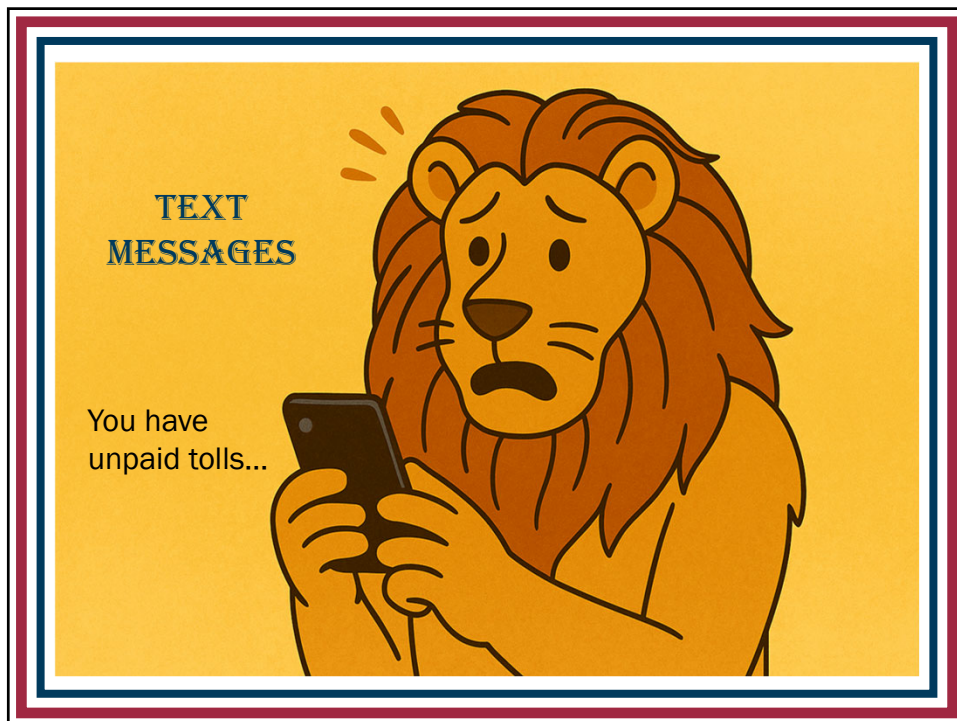
TENNESSEE COMPTROLLER OF THE TREASURY



4



5



6

Text Messages

- 🌐 Smishing
- 🌐 Asking for basic information
- 🌐 Sending links
 - Text messages
 - Social media messages
- 🌐 Higher threat than email

7

Text Messages

- 🌐 US lost approximately \$470 million to smishing attacks in 2024 – 5 times higher than 2020
- 🌐 19.2 billion spam texts were sent in August 2025
- 🌐 Surge in malicious URL texts coming through

8

Text Messages

- Don't let them scare you, have courage and check the source
- Don't click on or respond to messages you don't know
- Use a reputable texting app
- Report spam messages and use spam blocker
 - Forward to 7726 (SPAM)

9

EMAILS



10

Emails

- Common source of communication
- Phishing and Business Email Compromise (BEC)
- Targets anyone at any time and anywhere
- Number 1 method for fraud

11

Emails

- Phishing – wide attack and seeking general information
- BEC – uses artificial intelligence and machine learning to send more specific information
- Think of phishing as getting information about you, BEC is already having information and wanting more

12

Emails

- 🌟 AI and ML have increased the click rate in recent years
- 🌟 Over 1 million phishing attacks in 2025 Q1, 13% rise in Q2
- 🌟 FBI reported \$2.77 billion losses from BEC in 2024
 - Average wire transfer attempt is \$83k

13

Emails

- 🌟 Use your brain, don't click on or respond to messages you don't know or if you weren't expecting something
- 🌟 Verify the sender
 - Hover over the sender to see the full email address
 - Send an email separately to ask, "Was this you?"
 - Call the sender to verify
- 🌟 Report it and communicate with others who may be at risk

14



15

Phone Calls

- ✿ Can't avoid the inevitable
- ✿ 1893 first "phone con" was documented following more widespread access to phone lines
- ✿ 2006 first modern vishing attack fraudsters impersonating banks and getting information
- ✿ Tennessee is ranked 3rd in the US for most unwanted calls
- ✿ Tennessee Attorney General joined forces with other AGs to launch Operation Robocall Roundup

16

Phone Calls

- Most common form of communication
- Generally unreported unlike text and emails
- Rise in AI voice simulation (deepfake) assists in speech patterns and familiarity
- VoIP (voice over IP) makes calls cheaper, easier to spoof numbers, and more difficult to trace

17

Phone Calls

- Grandparent scam – scammers call elderly seniors and pretend to be a grandchild in crisis
- Help desk calls to reset MFA (multifactor authentication)
- Utility shut-off imposters calling for immediate payment or your service will be disconnected
- Hybrid attacks using BEC and phone call verification

18

Phone Calls

- ✳️ **Think smart and don't let them pull at your heart strings**
- ✳️ **Use a call blocker that will block and report calls**
- ✳️ **As always verify the source**
 - **Ask to call back (to a number you know)**
 - **Send an email**
 - **Communicate with others**

19

Common examples

- ✳️ **Text Messages**
 - **Bank/Financial Institution issues – click here to fix your account**
 - **Package undeliverable**
 - **False MFA verification alert**
- ✳️ **Vishing**
 - **Bank/Financial Institution issues – verify your card number and PIN**
 - **Government Agency – unpaid taxes, warrant for arrest**
 - **Grandparent scam – family member in distress**

20

Common examples

✦ Phishing

- Bank/Financial Institution – account update
- Gift card with survey – fill out sensitive information
- Credential verification

✦ BEC

- Bank/Financial Institution – account update
- Unpaid invoice for service
- Update on projects or sensitive topics

21

Tennessee Stats

- ✦ Unwanted calls: 46k+ complaints of robocalls in 2024 which is a decrease from 98k in 2021
- ✦ Reported \$157 million losses last year, imposter scams that started through text, emails, and phone calls
- ✦ Per TCA 8-4-119, state agencies are required to notify COT of any confirmed or suspected data breach or information-system breach within 5 business days of the occurrence. This does not include malware or spyware.

22

THANK YOU FOR VISITING THE CYBER LAND OF OZ

Questions or Comments?

Bethany Graves

Bethany.Graves@cot.tn.gov

615-401-7945

tncot.cc/cyberaware

Cyber.Aware@cot.tn.gov

