

Cybersecurity 101

Twyla Smith
Local Government Audit

9.14.2023

TENNESSEE COMPTROLLER OF THE TREASURY



1

To Join Poll

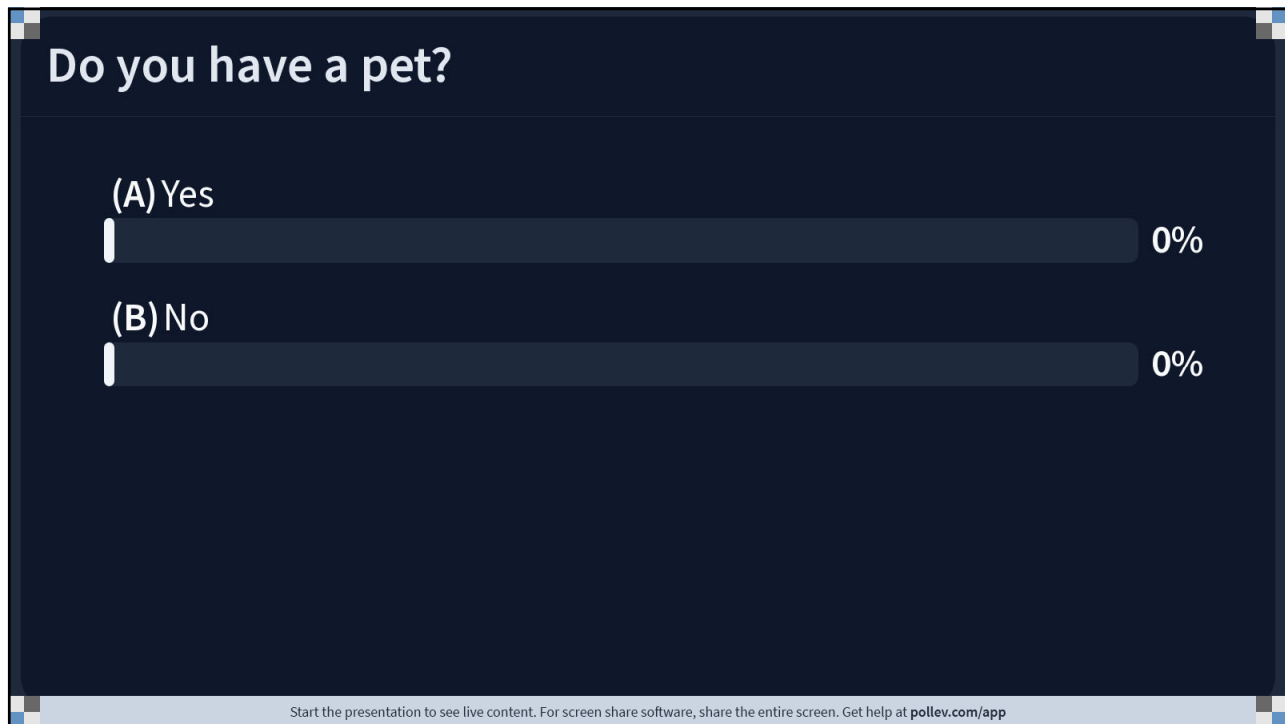


- Text: **TNCOT964** to **22333** once to join
- Website:
tncot.cc/poll

TENNESSEE COMPTROLLER OF THE TREASURY



2



3



4

What is the name of your pet?

Nobody has responded yet.
Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

5



6

What is the name of your spouse?

Nobody has responded yet.
Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app



7

Cybersecurity 101


Twyla Smith
Local Government Audit

9.14.2023

TENNESSEE COMPTROLLER OF THE TREASURY




8



CYBERSECURITY

Cybersecurity is not an IT problem; it is everyone's Job

TENNESSEE COMPTROLLER OF THE TREASURY



9



Cyber Security Awareness

ANGELO BREWING

10

Why is cybersecurity training important?

- Human error accounts for 52% of the root causes of security breaches
- How to protect ourselves against:
 - Social Engineering
 - Phishing
 - Ransomware
 - Weak Passwords

TENNESSEE COMPTROLLER OF THE TREASURY



11

How people think they get hacked



TENNESSEE COMPTROLLER OF THE TREASURY



12


How they really get hacked

TENNESSEE COMPTROLLER OF THE TREASURY



13

TENNESSEE COMPTROLLER OF THE TREASURY



14

Social Engineering Protection

- Be suspicious of unsolicited contact from individuals seeking internal organizational data or personal information.
- Do not provide personal information or passwords over email or on the phone.
- Do not provide information about your organization.
- Verify a request's authenticity by contacting the company or individual directly.
- Install and maintain anti-virus software, firewalls, and email filters.

TENNESSEE COMPTROLLER OF THE TREASURY



15



16

Phishing

3.4 Billion fake emails a day!

TENNESSEE COMPTROLLER OF THE TREASURY



17

Phishing Red Flags

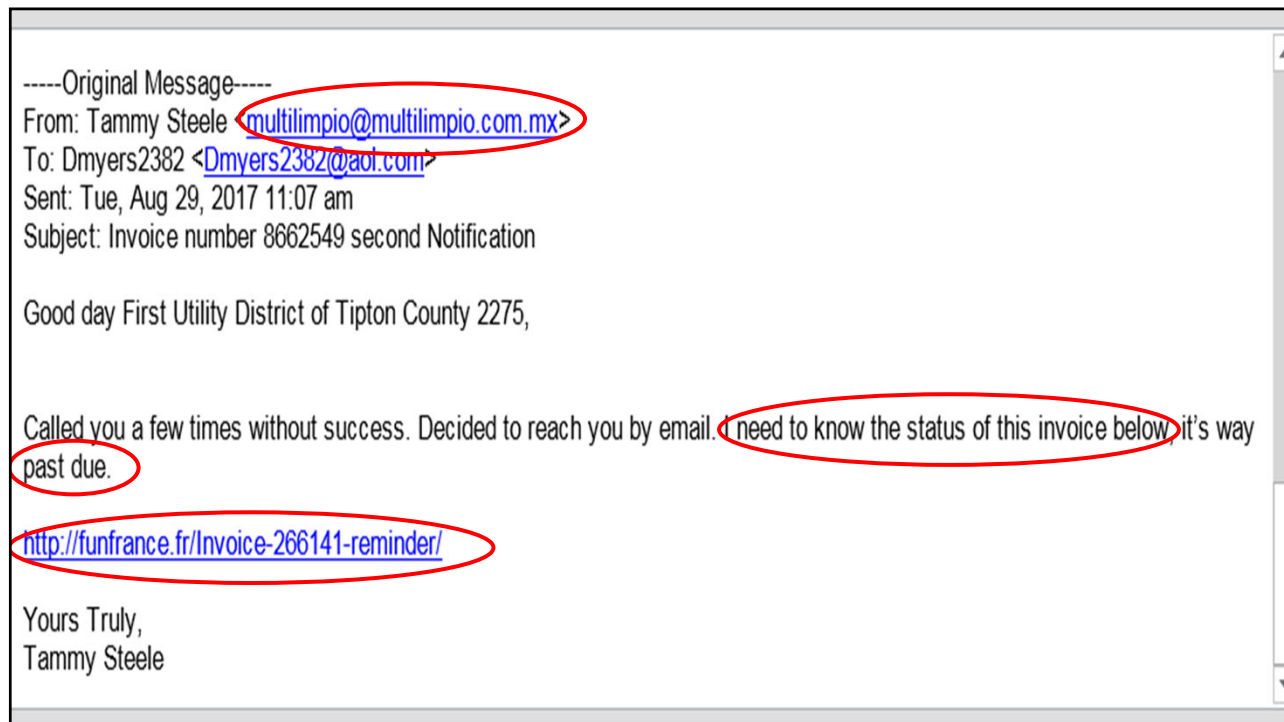
- Sense of urgency
- Spelling or grammar mistakes
- Unrecognized email addresses
- Fictitious Website Links
- Unfamiliar tone or language
- Request for sensitive information



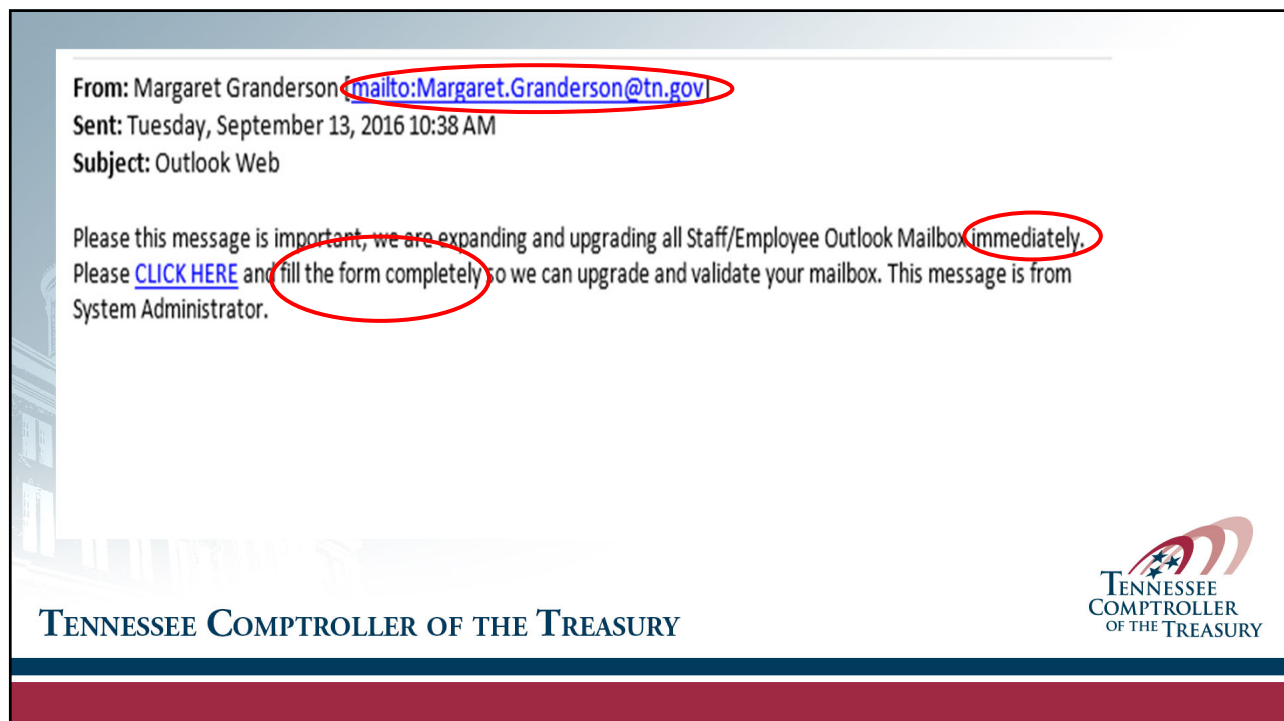
TENNESSEE COMPTROLLER OF THE TREASURY



18



19



20

From: [REDACTED]@soncountytn.gov>
Sent: Thu 04-14-2016 12:26 pm
To: [REDACTED]@soncountytn.gov>
Subject: RE: Question
Modified: Thu 04-14-2016 01:08 pm

Here is the wire information let me know when its done. You can take it from the **General Funding Account**. **It has to go out today.** Send me the confirmation as soon you are done.

BANK NAME: CHASE BANK
 BANK ACCOUNT NUMBER: 803383350
 BANK ROUTIN: 021000021
 BUSINESS NAME: RECIA-SIZEMORE
 BENEFICIARY ADDRESS: 47 W 91ST PLACE ,LOS ANGELES,CA 90044
 BANK ADDRESS: 1027 W 91ST PLACE ,LOS ANGELES,CA 90044
 AMOUNT: \$38,650


T Sent from my iPhone RY


21

Phishing

Other Common Themes

- Requests for payroll information
- Requests to change bank account/ routing numbers
- Requests to update accounts that are expiring



TENNESSEE COMPTROLLER OF THE TREASURY


22

Ransomware

- What is it?
 - A malicious software that is a form of high-tech extortion where the software hijacks computer systems and holds them hostage until their victims pay a ransom.



TENNESSEE COMPTROLLER OF THE TREASURY



23

How Is Ransomware Launched?

- Visiting an unsafe, suspicious, or fake website
- Opening an email or email attachment from someone you may or may not know and were not expecting
- Clicking on a malicious or bad link in an email, on Facebook, Twitter, and other social media posts (like articles, videos, ads), and even instant messenger chats

TENNESSEE COMPTROLLER OF THE TREASURY



24

Types of Ransomware

- Crypto Ransomware
 - Data and files are encrypted rendering applications, Word files, spreadsheets, PDF documents, etc. inaccessible.
- Locker Ransomware
 - Locks the operating system making the computer inaccessible altogether.
- Pay up or risk losing the data forever

TENNESSEE COMPTROLLER OF THE TREASURY



25

Am I really at risk?

TENNESSEE COMPTROLLER OF THE TREASURY



26



Phishing scam puts 1,937 Tipton County Schools employees at risk

*Published: Wednesday, January 25th 2017, 7:02 am EST
Updated: Thursday, January 26th 2017, 1:18 am EST*

By Amelia Carlson CONNECT
By Janice Broach CONNECT



TIPTON COUNTY, TN (WMC) - A phishing scam received by a Tipton County employee has placed 1,937 Tipton County School Board employees at risk of identity theft after their private information was given to a hacker.

According to the police report, a phishing email was sent to an employee Monday requesting all 2016 employee tax forms and sensitive information. The email appeared to be from Tipton County Director of Schools Dr. William Bibb, so the employee complied with the request—sending sensitive and personal information about all 1,937 Tipton County Schools employees to a stranger.

After a short time, the employee realized it was not a legitimate email from Dr. Bibb. That's when the employee contacted law enforcement.

Information contained in the tax forms included the employees name, address, phone number, date of birth, and social security number.

Employees affected by the breach are now concerned about potential identity theft.

Additional Links

Tipton County Schools employees' W-2 forms accidentally sent to hackers

TENNESSEE COMPTROLLER OF THE TREASURY



27



Dickson Sheriff's Office pays ransom to cyber criminals

Chris Gadd, cgadd@dicksonherald.com 2:34 p.m. CT Nov. 11, 2014



The story seems made for TV.

A law enforcement agency's data system is hacked by a cyber criminal who holds the sensitive information for ransom until certain demands are met.

Except in recent developments at the Dickson County Sheriff's Office, that scenario is all too real. The alleged criminal, who used the name "Nimrod Gruber," extorted \$572 from the county by locking up sensitive data with "ransomware" known nationally as "CryptoWall."

"Our computer system was attacked from an outside source," said Sheriff Jeff Bledsoe to county commissioners last week.

In recent days, sheriff's office staff was listening to Dickson radio station WDKN's online radio stream, according to Bledsoe, when the "ransomware" infected the department's report management system.

When "cryptowall" struck, staff were notified by on-screen messages they had a certain amount of time to pay or the data would not be unlocked. The software company used by

BEACHBODY

3-DAY REFRESH KIT WITH CHOC VEGAN...



TENNESSEE COMPTROLLER OF THE TREASURY



28

4 WSMV.com
WSMV-TV • NASHVILLE

HOME NEWS WEATHER 4WARN LIVE DOPPLER RADAR VIDEO I-TEAM 4WARN TRAFFIC SPORTS

Google Bookmark Facebook Twitter Print More

City of Spring Hill computer system hit by ransomware

*Posted: Nov 08, 2017 4:25 PM CST
Updated: Nov 08, 2017 4:25 PM CST*
Posted by Stuart Ervin CONNECT

SPRING HILL, TN (WSMV) - Officials in Spring Hill say the city was hit by a cyberattack last Friday.

City spokesman Jamie Page said an employee clicked on a ransomware email. The city's computer servers were then taken over and encrypted.

When the computer system was encrypted, a message appeared demanding \$250,000 to unlock it.

The city isn't sure who is asking for the ransom and they are refusing to pay it.

The ransomware locks out city workers from their email. They are also unable to accept online payments, or any payments through credit or debit cards for utility bills, court fines, business licenses, permits or any other city payments.

TENNESSEE COMPTROLLER OF THE TREASURY

29

What Do They Have in Common?

- City of Knoxville
- Knoxville Police & Fire Department
- Lawrence County Sheriff's Office
- Coffee County Sheriff's Office
- Spring Hill City & 911
- Henry County 911
- Murfreesboro Police & Fire Department
- Montgomery County Government
- City of Collierville
- Sevier County
- City of Springfield
- Anderson County
- Pellissippi State Community College
- Maury County Public School District
- Jefferson County Schools

TENNESSEE COMPTROLLER OF THE TREASURY

30

Security Awareness Training

Educate users about cyber threats

- Social Engineering
- Phishing Attacks
- Ransomware
- Malicious Websites



TENNESSEE COMPTROLLER OF THE TREASURY



31

Passwords and Multi-Factor Authentication

- Strong, protected passwords
- Avoid using widely known information
- Passphrase with upper- and lower-case letters, numbers and symbols
- Change passwords at least every 90 days
- Require multi-factor authentication (MFA) for accessing your systems whenever possible. MFA should be required of all users, but start with privileged, administrative, and remote access users.

TENNESSEE COMPTROLLER OF THE TREASURY



32

Major U.S. gasoline pipeline hit by cyberattack

The map shows the Colonial Pipeline route starting in Houston, Texas, and extending eastward through Louisiana, Mississippi, Alabama, Georgia, South Carolina, North Carolina, Virginia, Maryland, Delaware, New Jersey, and Pennsylvania to Linden, Pennsylvania. The pipeline is highlighted in red. State abbreviations are labeled: TX, LA, MS, AL, GA, SC, NC, VA, MD, DE, NJ, PA. The Gulf of Mexico and Atlantic Ocean are also labeled. A scale bar indicates 400 km.

TENNESSEE COMPTROLLER OF THE TREASURY

33

Operating Systems and Anti-Virus Updates

**Update!
Update!
Update!**

The image shows a laptop with a blue screen displaying a progress bar and the text "UPDATE...".

TENNESSEE COMPTROLLER OF THE TREASURY

34

Backup! Backup! Backup!



TENNESSEE COMPTROLLER OF THE TREASURY



35

Cybersecurity Posture

- Data Inventory
- Backup Configuration
- Software Updates
- Cyber Insurance
- Other Measures



TENNESSEE COMPTROLLER OF THE TREASURY



36

Contingency Planning

Address steps to take in the event of a cyber attack

- Immediate Response
- Vendor/IT contacts
- Section 47-18-2107, TCA



TENNESSEE COMPTROLLER OF THE TREASURY



37

Questions?

Twyla Smith

Twyla.Smith@cot.tn.gov

615-747-8853

Tncot.cc/cyberaware

TENNESSEE COMPTROLLER OF THE TREASURY



38