CYBERSECURITY

It's All About You!!!

Jim Arnette, Director
Division of Local Government Audit
Tennessee Comptroller of the Treasury

TENNESSEE COMPTROLLER OF THE TREASURY

1

CYBERSECURITY

How educated are you?

- Do you know how to secure your system?
- Can you recognize cybersecurity threats?
- How would you respond to a cyberattack?

2

CYBERSECURITY

3 Things That Cyber Criminals Want

- Control of your system
- Data
- Money

3

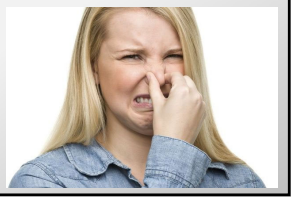
CYBERSECURITY

4

CYBERSECURITY

Cybersecurity Hygiene

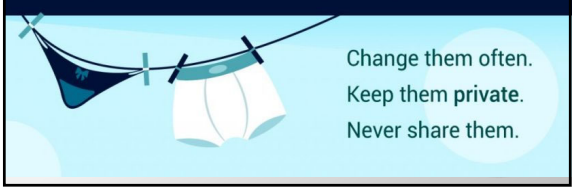
- No training
- Outdated operating systems and virus detection software
- Inadequate system backups
- Weak passwords



5

CYBERSECURITY

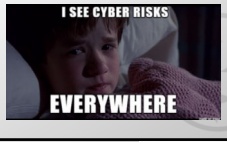
PASSWORDS ARE LIKE
UNDERPANTS



6

CYBERATTACKS

- Hackers attack systems every 39 seconds, on average 2,244 times a day (University of Maryland)
- The average time to identify a breach in 2019 was 206 days (IBM)
- 94% of malware was delivered by e-mail (Verizon)
- The average cost of a ransomware attack on businesses is $133,000 (SafeAtLast)

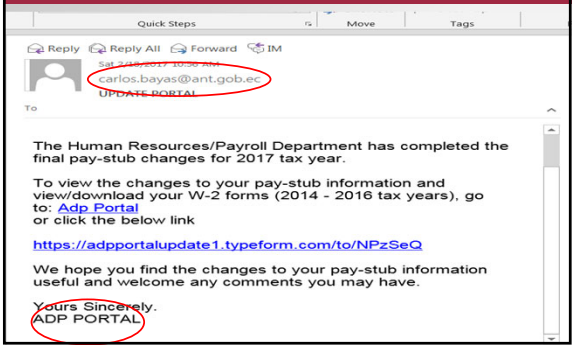


7

CYBERSECURITY

8

PHISHING



9

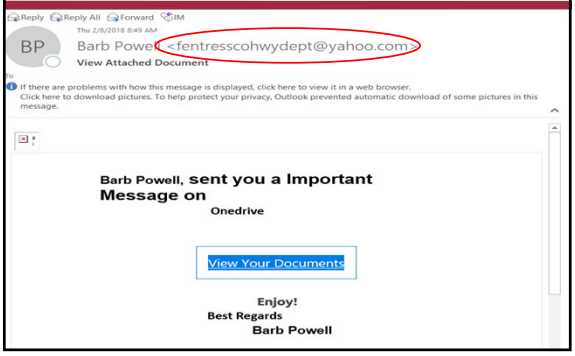
PHISHING

From: Elvira Currie [mailto:Elvira.Currie@tn.gov]
Sent: Tuesday, October 04, 2016 11:04 AM
Subject: Outlook Web

Please this message is important, we are expanding and upgrading all Outlook Web Mailbox immediately. Please CLICK HERE and fill the form completely so we can upgrade and validate your Outlook Web Mailbox. Please if you cannot access the link, send your Username and Password to our staff helpdesk email at citystaff@outlook.com for immediate validation. This message is from System Administrator.

10

PHISHING



11

PHISHING

-----Original Message-----
From: Tammy Steele <multilimpio@multilimpio.com.mx>
To: Dmyers2382 <Dmyers2382@aol.com>
Sent: Tue, Aug 29, 2017 11:07 am
Subject: Invoice number 8662549 second Notification

Good day First Utility District of Tipton County 2275,

Called you a few times without success. Decided to reach you by email. I need to know the status of this invoice below, it's way past due.

http://funfrance.fr/Invoice-266141-reminder/

Yours Truly,
Tammy Steele

12

PHISHING

[redacted]

From: [redacted]oncountytn.gov>
Sent: Thu 04-14-2016 12:26 pm
To: [redacted]oncountytn.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

Sent from my iPhone

13

PHISHING

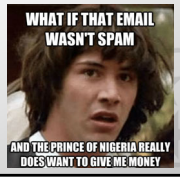
"TRUST BUT VERIFY"

14

PHISHING

What does a phishing e-mail look like?

- Sense of urgency
- Spelling or grammar mistakes
- Personal or unrecognized e-mail addresses
- Requesting highly sensitive or confidential information
- Unfamiliar tone/language
- Too good to be true



15

PHISHING

There are so many scams on the Internet nowadays.

Send me $19.95 and I will tell you how to avoid them!

16

COT - PHISHING

10% CLICK RATE — Percentage of staff that clicked on a simulated phishing link in an email

1% — Division with the lowest phishing rate

LOCAL GOVERNMENT AUDIT

17

RANSOMWARE

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.

18

RANSOMWARE

Types

- Crypto
- Locker
- Leakware

19

RANSOMWARE

20

RANSOMWARE

To pay, or not to pay?

That is the question...

21

RANSOMWARE

22

RANSOMWARE

How is ransomware launched?

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

23

RANSOMWARE

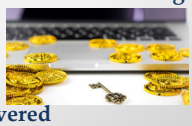
$522

$133,000

24

RANSOMWARE

- County Sheriff
  - Employee clicked on an ad while live-streaming a radio station
  - Files were encrypted
  - Ransom demand = $572
  - Ransom was paid – Data recovered



25

RANSOMWARE

- Municipality
  - Employee attached an infected thumb drive to their computer
  - Files were encrypted
  - Ransom demand = $1,000
  - Ransom not paid
  - Computers reimaged – data restored

26

RANSOMWARE

- Municipality
  - Employee clicked on a link in an e-mail
  - All files were encrypted
  - Ransom demand = $250,000
  - Ransom not paid
  - Backups were infected
  - Hired service to help
  - Lots of staff overtime
  - Manual receipts

27

RANSOMWARE

N.C. county weighs paying cyber hackers $26K ransom for servers held hostage

Doug Stanglin, USA TODAY Published 11:29 a.m. ET Dec. 6, 2017 | Updated 3:34 p.m. ET Dec. 6, 2017

(Photo: MariuszBlach, Getty Images/iStoc)

Officials in North Carolina's Mecklenburg County were in touch with hackers, believed to be from Iran or Ukraine, and planned to decide Wednesday evening whether to pay them $26,000 to win the release of multiple files held hostage on county servers.

County manager Dena Diorio told reporters it could take "days not hours" to restore the computers and bring full service back, regardless of whether the county pays the ransom.

Cyber experts believe the hackers operated from Iran or Ukraine and infected the servers with a new strain of ransomware known as LockCrypt, she said.

An email attachment opened by a county employee Tuesday initiated the attack. The attachment contained a "worm" that began encrypting the county's files. It also contained an email address and instructions on how to pay the ransom.

The ransomware was quickly spotted and isolated, but still affected 48 of the county's 500 servers, Diorio said. The county was "open for business" but many operations had slowed, she added. Because of a backup system, the hack didn't compromise any personal information or delete any data.

Ransomware Defense Book

28

RANSOMWARE

Atlanta's ransomware attack may cost the city $17M

Written by Julie Spitzer | August 06, 2018 | Print | Email

The SamSam ransomware attack that took down the city of Atlanta's computer network in March could cost taxpayers $17 million — up from earlier estimates of $2.7 million, according to a "confidential and privileged" seven-page document reviewed by *The Atlanta Journal-Constitution* and *Channel 2 Action News*.

The latest cost estimate includes about $6 million in existing contracts for security services and software upgrades and $11 million in potential costs associated with the attack, including new desktops, laptops, smartphones and tablets. This would mark one of the U.S.' costliest cyberattacks affecting a local government in 2018, despite city officials declining to pay the ransom demanded by the hackers.

"We are pleased with the progress of the recovery efforts. In addition to responding to the criminal attack against the city of Atlanta, we are using this opportunity to make the city more secure," a city spokesperson told the publications in an email statement. "Unfortunately, in today's world, governments are seeing an increase in cyber attacks … As you already know, the city is insured against cyberattack (sic). We continue to work through that process for the most cost-effective outcome for our residents."

The ransomware incident knocked out services such as warrant issuances, water requests, new inmate processing, court fee payments and online bill-pay programs across multiple city departments. To unlock the city's systems and data, hackers demanded $51,000 in bitcoin, which the city refused to pay. The full extent of the damage is not yet clear, although *AJC* and *Channel 2 Action News* discovered two months ago that years

29

RANSOMWARE

Peace Corps

30

RANSOMWARE

- **Mitigation Strategies**
  - Avoid clicking links on a webpage, in an e-mail, or in a chat message unless you absolutely trust the page or sender
  - Avoid clicking on advertisements on websites
  - Install operating system updates
  - Use a reputable anti-virus software and keep the definitions current
  - Watch where you're going on the Internet
  - Most important of all...BACKUPS!

31

TENNESSEE DATA BREACH LAW

- Section 47-18-2107, *TCA*
- Defines personal information
- Requires notification no later than 45 days with exception
- If required notification exceeds 1,000 individuals, consumer reporting agencies must be notified

32

INSURANCE

33

Information Systems Audits

- Logical access controls (usernames and passwords)
- System backups
- Disaster Recovery Plans
- Virus detection software
- Operating system upgrades and patches

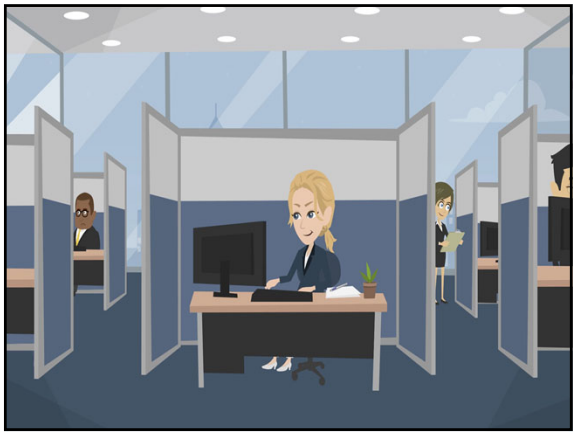
34

Education

- Recognize cybersecurity threats
- Prevent and respond to cyberattacks
- Implement strong system access controls
- Make sure your system is backed up regularly and your backups are clean
- Have a plan for re-imaging computers and restoring data files
- Keep virus detection software current
- Upgrade your operating system

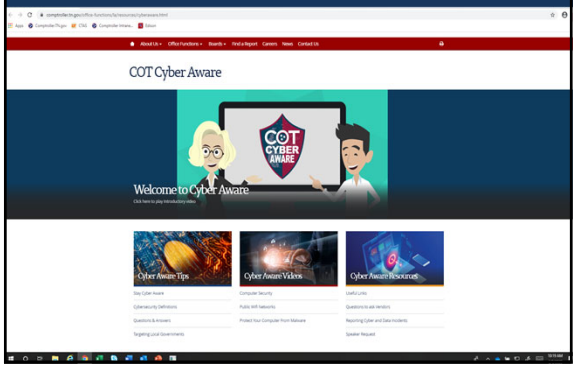
35

36



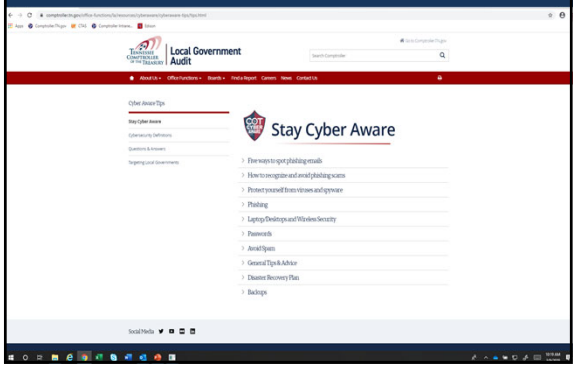
37

TNCOT.CC/CYBERAWARE



38

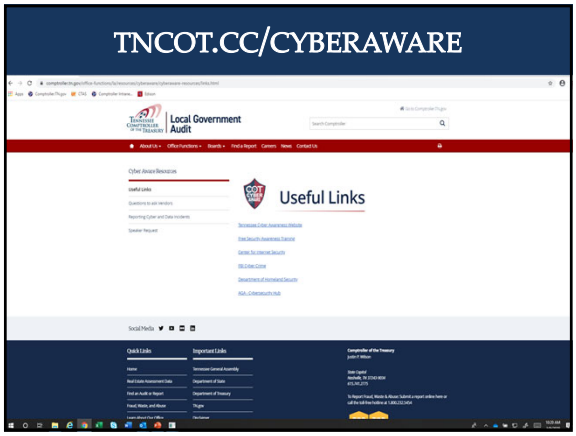
TNCOT.CC/CYBERAWARE



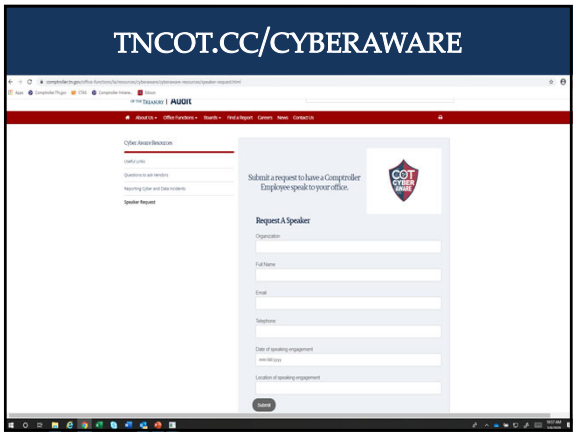
39


TNCOT.CC/CYBERAWARE
Local Government Audit
Computer Security

40


TNCOT.CC/CYBERAWARE
Local Government Audit
Useful Links

41


TNCOT.CC/CYBERAWARE
Request A Speaker

42

CYBERSECURITY

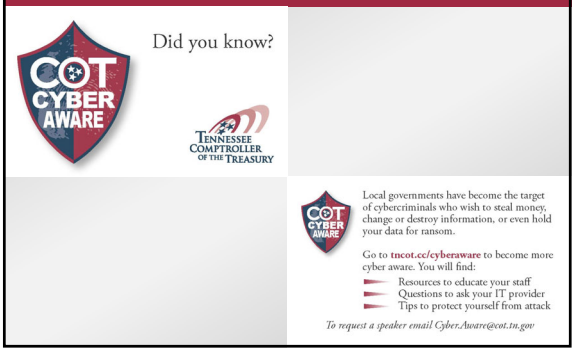
43

BOND RATINGS

- Are local governments in Tennessee fiscally sound?
- Do they have competent financial management staff? (CMFO, CCFO)
- Do they protect their computer systems and their data? (COT Cyber Aware)

44

IN CONCLUSION



45

In Conclusion

Jim Arnette
Director
Division of Local Government Audit
615.401.7841
Jim.Arnette@cot.tn.gov

46