


Cybersecurity 101

Nathan Abbott
Local Government Audit

10.06.2021

TENNESSEE COMPTROLLER OF THE TREASURY




1

Why is it so important?

- It is estimated that 2/3 of successful cyber attacks resulted from poor employee practices.


TENNESSEE COMPTROLLER OF THE TREASURY



2


Headlines

- City pays ransom to Hackers
- Credit agency pays millions in data breach settlement
- Retail customer data stolen

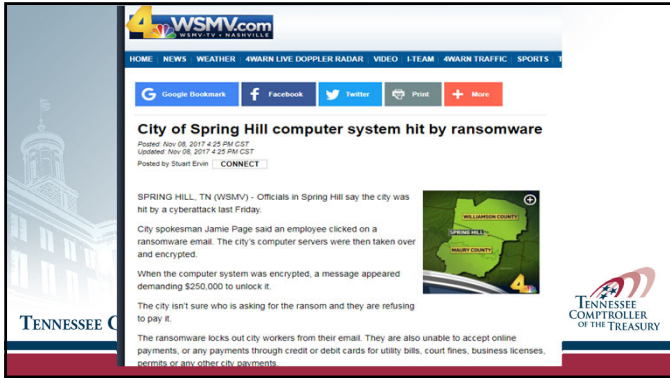


This Photo by Unknown Author is licensed under CC BY-NC

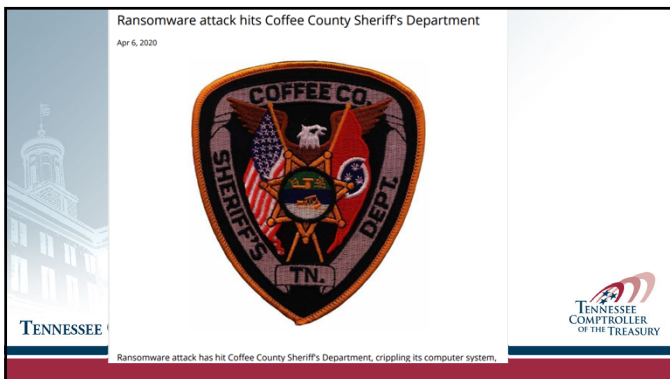
TENNESSEE COMPTROLLER OF THE TREASURY



3







N.H. town's money likely lost

Officials in Peterborough, New Hampshire, said yesterday the government of the 7,000-person town lost \$2.3 million to an email fraud scheme, and that recovering the money is doubtful. Criminals likely operating from a foreign country impersonated both a school district and a local construction firm to trick the town's finance department into making multiple payments to phony accounts. Officials said they do not believe the transactions can be reversed, and are unlikely to be covered by the town's general liability policy.

TENNESSEE COMPTROLLER OF THE TREASURY



7

Cybersecurity 101



Cyber responsibilities



Cyber culture



Cyber risks

TENNESSEE COMPTROLLER OF THE TREASURY



8

Cyber Responsibilities

Develop Cybersecurity Policies and Procedures

- User access privileges
- Data backup
- Software Inventory
- Hardware support and maintenance



This Website by Unknown Author is licensed under CC BY-NC-ND

TENNESSEE COMPTROLLER OF THE TREASURY



9

User access privileges

Your staff are the users: Developing security awareness and vigilance amongst all users.

Your staff must have continuously to grow the skills to practice and maintain cyber readiness.

- Not sharing passwords
- Changing passwords




TENNESSEE COMPTROLLER OF THE TREASURY

10

Data Backups

Your data is what business is built on: Make backups and avoid the loss of information critical to operations.

Even the best security measures can be circumvented with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted. Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.




TENNESSEE COMPTROLLER OF THE TREASURY

11

System Inventory

Your systems are what make you operational: Protect critical assets and applications.

Information is the life-blood of any organization; it is often the most valuable of a business' intangible assets. Know where this information resides, know what network assets store and process that information, and build security into and around these assets.



TENNESSEE COMPTROLLER OF THE TREASURY

12

Cyber Culture

Starts with Yourself

- As a leader you want to drive cybersecurity strategy, investment and culture.

Once you are aware of and understand cyber risks to your organization, you will comprehend why cybersecurity must have a major role in your organization's operational resilience strategy. Your investment allows actions and activities that build and sustain a culture of cybersecurity.







TENNESSEE COMPTROLLER OF THE TREASURY



13

Cyber Risk

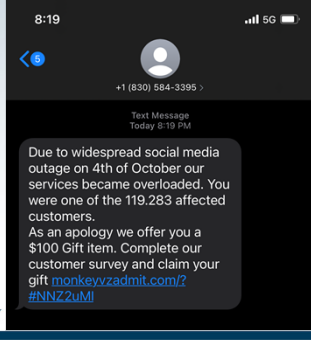
-  Phishing – Email is great isn't it?
-  Vishing and Smishing – Phishing but voice calls and text messages.
-  Social Media attacks – Friend or family member suddenly stuck in a foreign country and needs money?
-  Malware/Ransomware – You don't need those tax records, do you?

TENNESSEE COMPTROLLER OF THE TREASURY



14

SMISHING




TENNESSEE COMPTROLLER OF THE TREASURY

15

Smishing

- Use of text messages as a phishing vector has become more popular because it is effective. Text messages have a 98% open rate, and 90% of messages are opened in the first three minutes, [according to Proofpoint](#). Further, the success rate — as measured by the proportion of users that click through to an attacker's page — is eight times that of email phishing.

TENNESSEE COMPTROLLER OF THE TREASURY



16

Phishing

3.4 Billion fake emails a day!

TENNESSEE COMPTROLLER OF THE TREASURY



17

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

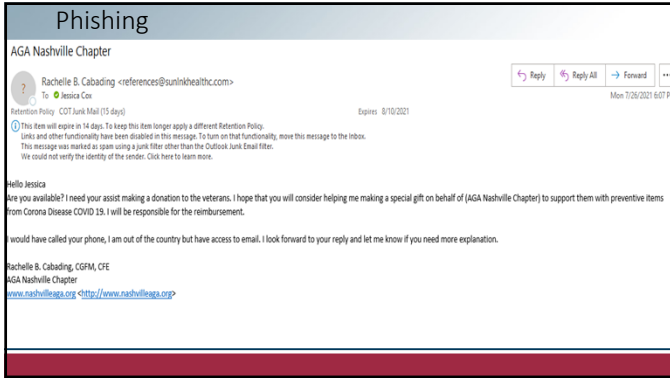
Good day First Utility District of Tipton County 2275,

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.

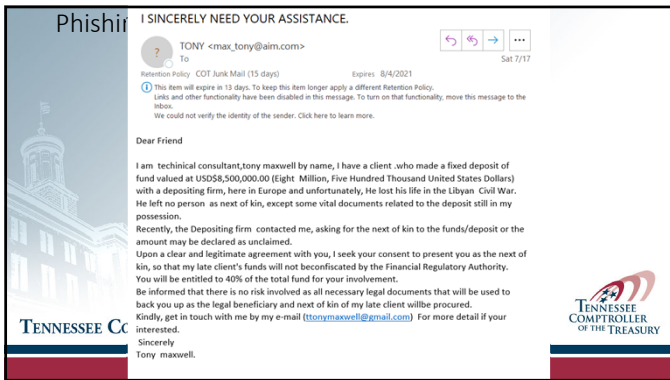
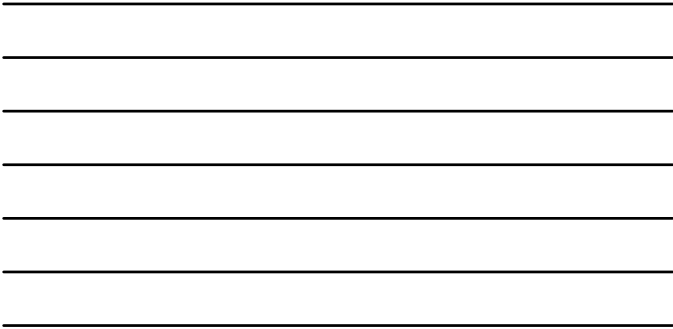
<http://funfrance.fr/Invoice-266141-reminder/>

Yours Truly,
 Tammy Steele

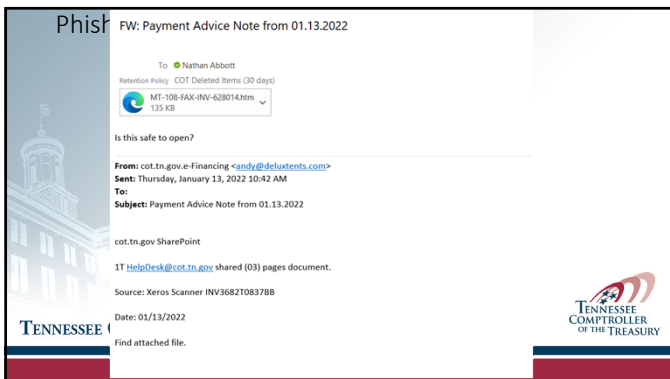
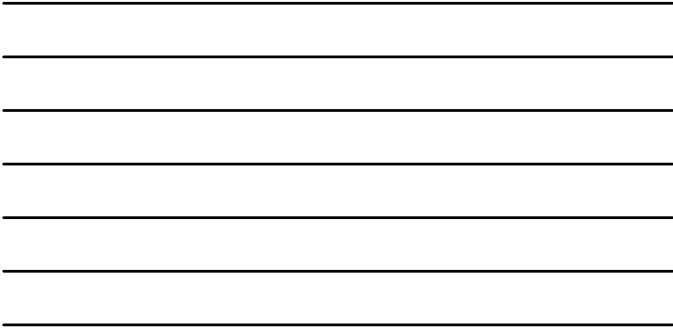
18



19



20




21



5 Ways to spot a Phishing Email

1. The email asks you to confirm personal information
2. The web and email addresses do not look genuine
3. It's poorly written
4. There's a suspicious attachment
5. The message is designed to make you panic

TENNESSEE COMPTROLLER OF THE TREASURY



22

Arrest in 'Ransom Your Employer' Email Scheme

November 22, 2021 30 Comments

In August, KrebsOnSecurity warned that scammers were contacting people and asking them to unleash ransomware inside their employer's network, in exchange for a percentage of any ransom amount paid by the victim company. This week, authorities in Nigeria arrested a suspect in connection with the scheme – a young man who said he was trying to save up money to help fund a new social network.

From: sajid@bpovision.com ☆
 Subject: Partnership Affiliate Offer 8/12/21, 12:03 PM
 To: undisclosed-recipients; ☆


if you can install & launch our Demonware Ransomware in any computer/company main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com


Telegram : madalin8888

TENNESSEE COMPTROLLER OF THE TREASURY




23


Essential elements




Yourself




Your Staff



Your Systems




Your Surroundings



Your Data

TENNESSEE COMPTROLLER OF THE TREASURY



24

Starting Point

- Employ a backup solution that automatically and continuously backs up critical data and system configurations.
- Enable automatic updates whenever possible. Replace unsupported operating systems, applications, and hardware. Test and deploy patches quickly.
- 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.

Backup Data Patch & Update Management Multi-Factor Authentication

TENNESSEE COMPTROLLER OF THE TREASURY

25

tncot.cc/cyberaware

Local Government Audit

COT Cyber Aware

Introducing COT Cyber Aware

Welcome to Cyber Aware

TENNESSEE COMPTROLLER OF THE TREASURY

26

tncot.cc/cyberaware

Cyber Aware Tips Cyber Aware Videos Cyber Aware Resources

Stay Cyber Aware Computer Security Useful Links

Cybersecurity Definitions Public Wi-Fi Networks Questions to ask vendors

Questions & Answers Protect Your Computer From Malware Reporting Cyber and Data Incidents

Targeting Local Governments Speaker Request

Working Remotely

TENNESSEE COMPTROLLER OF THE TREASURY

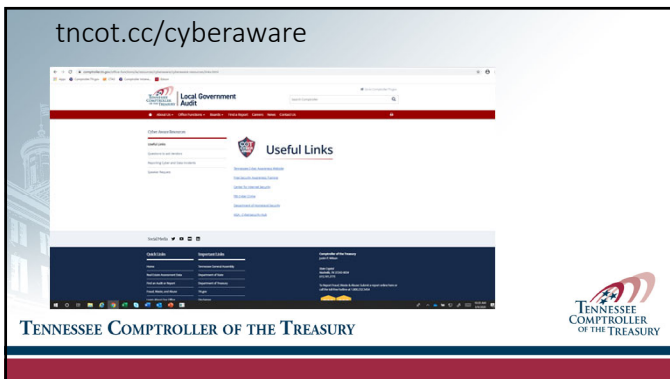
27



28



29



30

Questions

Nathan Abbott
Nathan.Abbott@cot.tn.gov
615-401-7842

tncot.cc/cyberaware



TENNESSEE COMPTROLLER OF THE TREASURY
