


# Cybersecurity- “Be in the Know!”

Barbara Shults  
Legislative IS Auditor  
*Division of Local Government Audit*

August 22, 2024

TENNESSEE COMPTROLLER OF THE TREASURY



1

---

---

---

---

---

---

---

---

# Meet My People



2

---

---

---

---

---

---

---

---

# About Us



Jason Mumpower

Jim Arnette

THE BOSSES

3

---

---

---

---

---

---

---

---



4

---

---

---

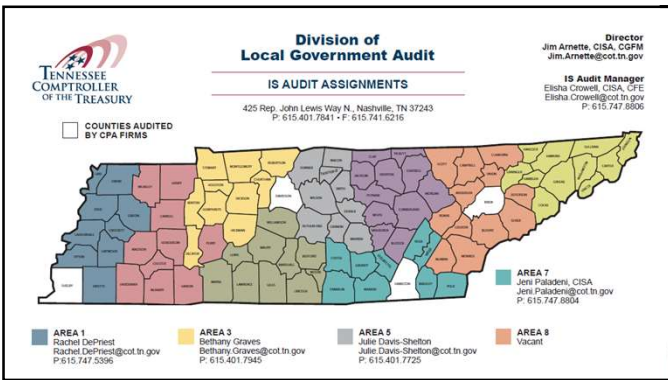
---

---

---

---

---



5

---

---

---

---

---

---

---

---

**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

6

---

---

---

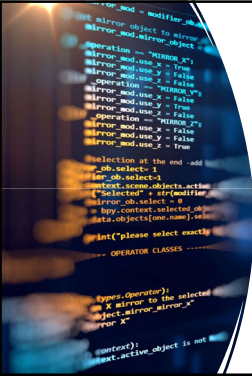
---

---

---

---

---



## Goals of Presentation- Be In the Know!

I. Define cybersecurity

II. Responsibility  
Who is at Risk?

III. Threats  
a. Social Engineering  
b. Business Email Compromise/BEC  
c. Phishing/Spearphishing  
d. Weak Passwords  
e. Ransomware/Malware

IV. Defense  
a. Cybersecurity Training  
b. Create strong Passwords  
c. Multifactor Authentication

IV Conclusion/Questions

7

---

---

---

---

---

---

---


---

## What is Cybersecurity?

According to CISA.gov:

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

TENNESSEE COMPTROLLER OF THE TREASURY

  
TENNESSEE  
COMPTROLLER  
OF THE TREASURY

8

---

---

---

---

---

---

---

---



CIA TRIAD

- Confidentiality
- Integrity
- Availability

TENNESSEE COMPTROLLER OF THE TREASURY

9

---

---

---

---

---

---

---

---



10

---

---

---

---

---

---

---

---



11

---

---

---

---

---

---

---

---



12

---

---

---

---

---

---

---

---

### Who is at Risk of a Cyber-Attack?



TENNESSEE COMPTROLLER OF THE TREASURY

TENNESSEE COMPTROLLER OF THE TREASURY

13

---

---

---

---

---

---

---

---

### 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

TENNESSEE COMPTROLLER OF THE TREASURY

14

---

---

---

---

---

---

---

---

### Everyone is a Target Because: Cybercrimes Are Big Business!



CYBERCRIMES LOSSES WERE \$8 TRILLION GLOBALLY IN 2023- PREDICTED TO HIT \$9.5 TRILLION IN 2024 AND \$10.5 TRILLION BY 2025.

\$10.2 BILLION WAS REPORTED BY FBI AS POTENTIAL LOSSES IN UNITED STATES FOR 2023.

\$1.3 MILLION AVERAGE LOSSES BY BUSINESSES IN 2023

ESTIMATED ONE ATTACK OCCURS EVERY 39 SECONDS IN 2021

\$16.4 BILLION A DAY OR \$160,000 PER SECOND IN DAMAGES RESULTING FROM CYBERATTACKS (ESTIMATED BY CYBERSECURITY VENTURES).

<https://www.usatoday.com/money/blueprint/business/vpn/cybersecurity-statistics/>

TENNESSEE COMPTROLLER OF THE TREASURY

TENNESSEE COMPTROLLER OF THE TREASURY

15

---

---

---

---

---

---

---

---



16

---

---

---

---

---

---

---

---



17

---

---

---

---

---

---

---

---

**Social Engineering-**  
(in the context of information security)  
the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

---

How People Really Get Hacked

<https://languages.oup.com/google-dictionary-en/>

18

---

---

---

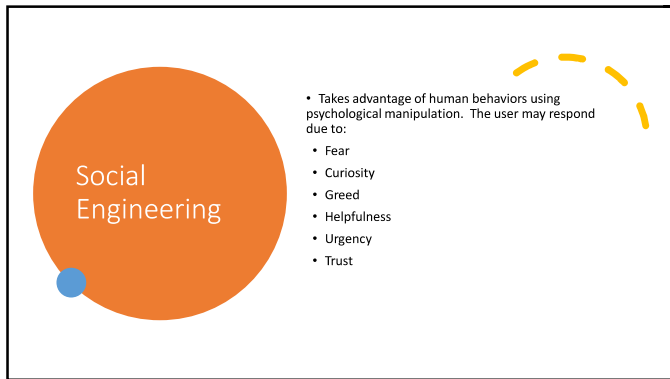
---

---

---

---

---



**Social Engineering**

- Takes advantage of human behaviors using psychological manipulation. The user may respond due to:
- Fear
- Curiosity
- Greed
- Helpfulness
- Urgency
- Trust

19

---

---

---

---

---

---

---

---



**Threats**

TENNESSEE COMPTROLLER OF THE TREASURY

20

---

---

---

---

---

---

---

---



**Cybersecurity Threats**

- Business Email Compromise
- Phishing/Smishing/Vishing
- Malware/Ransomware
- Weak Passwords

21

---

---

---

---

---

---

---

---

Definition:  
Business  
Email  
Compromise

A type of cybercrime in which the attacker uses email to trick someone to share sensitive and confidential information or send funds to them through various means which could include wire transfers, gift cards, or some other means of paying fake invoices.

22

---

---

---

---

---

---

---

---

### STATISTICS-Be In The KNOW!

2023

- FBI reports 21,489 complaints regarding BEC, with adjusted losses over 2.9 billion dollars.
- Phishing and Spoofing 298, 878 complaints, with adjusted losses over 18.7 million dollars.
- Ransomware, 2,825 complaints with adjusted losses over 59.6 million dollars.

To report a cybercrime complaint: [www.ic3.gov](http://www.ic3.gov)

[https://www.ic3.gov/media/PDF/AnnualReport/2023\\_IC3Report.pdf](https://www.ic3.gov/media/PDF/AnnualReport/2023_IC3Report.pdf)

COMPTROLLER OF THE TREASURY

23

---

---

---

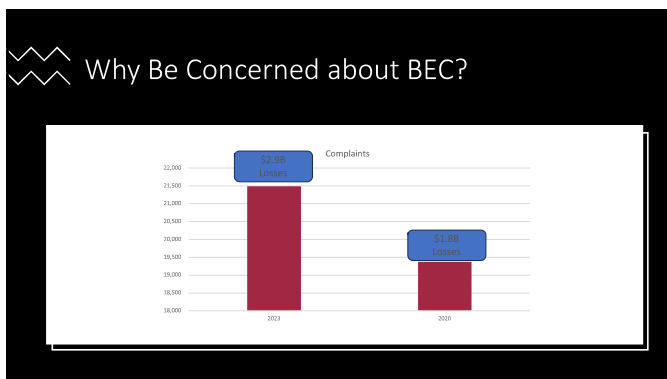
---

---

---

---

---



24

---

---

---

---

---

---

---

---



FBI Knoxville  
Public Affairs Officer Daniel Delbello  
(865) 544-0751

March 7, 2024

**FBI: Scammers Stole \$160 Million From Tennesseans in 2023**

KNOXVILLE, Tenn.—Tennessee residents lost more than \$160 million to internet scammers last year, according to a new report released by the Federal Bureau of Investigation. The report highlights critical vulnerabilities and underscores the imperative for heightened cybersecurity measures in the Volunteer State.

In 2023, Tennessee reported 3161 in the county, with residents aging a total of 8,454 complaints with the FBI's Internet Crime Complaint Center (IC3), reporting losses amounting to \$161,195,009. These figures underscore the devastating impact cybercrime has on individuals and businesses statewide.

"We're noticed a steady stream of cybercrime here in Tennessee. This means we all need to be extra careful and take action to stay safe online," said Joseph Connor, special agent in charge of the FBI's Knoxville Field Office. "Cybercriminals are always coming up with new tricks. Keep your eyes peeled, whether you're a regular person or a big company. So, it's really important for everyone in Tennessee to pay attention and make sure you're protecting ourselves online."

The top cybercrimes reported include fraud, and business-to-business computer (B2C) email scam (phishing) attacks for losses in Tennessee. Particularly alarming is the heightened risk record by individuals over 60, who are most susceptible to falling victim to such cyber scams.

Nationwide, in 2023, the IC3 recorded a staggering 880,418 complaints, indicating a substantial rise in cybercrime activities across the nation. The total losses incurred from these incidents exceeded a staggering \$17.5 billion, underscoring the severity of the cyber threat landscape.

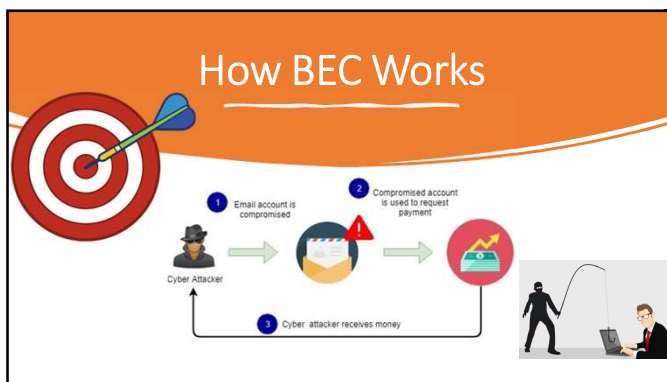
Notably, this figure represents a significant increase compared to the average number of complaints received over the past five years. California, Texas, Florida, New York, and Ohio reported the highest number of victims, while California, Texas, and Florida also topped the list in terms of overall losses.

**Protecting yourself online is crucial. Make sure to use strong, unique passwords for your accounts, and be cautious about clicking on links or opening attachments in e-mails from unfamiliar sources," said Jason Jaramas, supervisory special agent leading the FBI's cybercrime squad in Knoxville. "Keep your computer's software up to date and consider using antivirus software. And most importantly, if something seems suspicious or too good to be true, trust your gut and double-check before sharing personal information or sending money."**

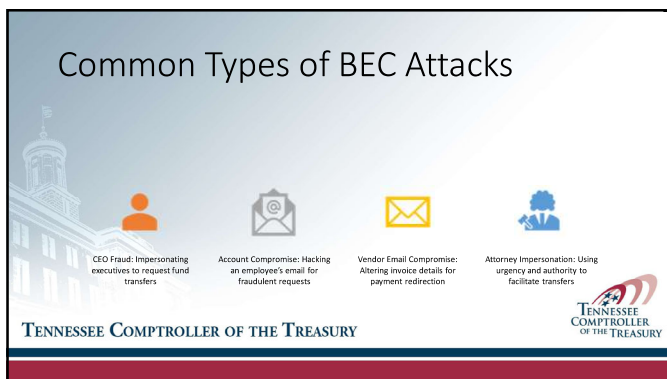
The FBI remains committed to working closely with local law enforcement agencies and community partners to mitigate risks and protect Tennessee residents against cyber attacks. If your business is the victim of a cyber attack, contact your local FBI office immediately for assistance.

For more information on the 2023 Internet Crime Report and resources for cybersecurity, visit the IC3 website at [www.ic3.gov](https://www.ic3.gov).

25

[illegible]

26

[illegible]

27

---

---

---

---

---

---

## Real Life Examples Of BEC

Children's Health Care-Atlanta-\$3.6 million

Eagle Mountain City, Utah-\$1.3 million

Toyota Boshoku Corporation-\$37 million

City of Lexington, KY- \$4 million

28




**Malachi Mullings, Setting**  
 Malachi Mullings Setting a State Medicaid Program in Sandy Springs, GA. He created 20 bank accounts for The Mullings Group LLC from 2019-2021. During this time, he phished a State Medicaid Program and set up Romance Schemes for \$4.5 Million dollars.

**Real-World Examples of BEC**

- Malachi Mullings, 31 Sandy Springs, GA. He created 20 bank accounts for The Mullings Group LLC from 2019-2021. During this time, he phished a State Medicaid Program and set up Romance Schemes for \$4.5 Million dollars.

TENNESSEE COMPTROLLER OF THE TREASURY

29



**Real-World Examples of BEC**

- ETS Contracting, Brooklyn, NY \$240,926 Brianna S. Graves, 30 Kansas City, MO she sent an email to ETS with payment instruction for a company ETS was working with. However, the email had 1 letter different in the domain and it was Fraudulent.

TENNESSEE COMPTROLLER OF THE TREASURY

30



31

---

---

---

---

---

---

---

---

### Real-World Example

> On Friday, April 1, 2022, 10:38:55 AM CDT, Donna Craig  
 > <clerkoffice1@gmail.com> wrote:  
 >  
 > Randi  
 > I'll need you to process a payment for me today via ACH/WIRE  
 > TRANSFER/CHECK MAILING. For the  
 > Administrative networking web-hosting activity expense.  
 >  
 > Get back to me if you can get this done, so i can forward the payment  
 > details to you.  
 >  
 > Regards  
 > Donna

On 4/1/22, Randi French <randifrench@yahoo.com> wrote:  
 > Yes ma'am i sure can :)  
 > Thank you, Randi French Henry County Trustee

32

---

---

---

---

---

---

---

---

From: Donna Craig (clerkoffice1@gmail.com)  
 To: randifrench@yahoo.com  
 Date: Friday, April 1, 2022, 11:05 AM CDT

Randi

Initiate an outgoing wire transfer to the account details below:  
 ACCOUNT HOLDER: CONSTANCE LYON  
 BANK NAME: M&T BANK  
 ACCOUNT NUMBER: 9888615268  
 ROUTING NUMBER: 031302955  
 AMOUNT: \$4,780.00  
 BANK ADDRESS: 550 Suburban Dr, Newark, 19711

Payment for Administrative Networking web-hosting activity service expenses

Get back to me with the payment confirmation slip once you are done making the payment.

Regards  
 Donna

TENNESSEE  
 ATTORNEY GENERAL

TENNESSEE  
 ATTORNEY GENERAL

33

---

---

---

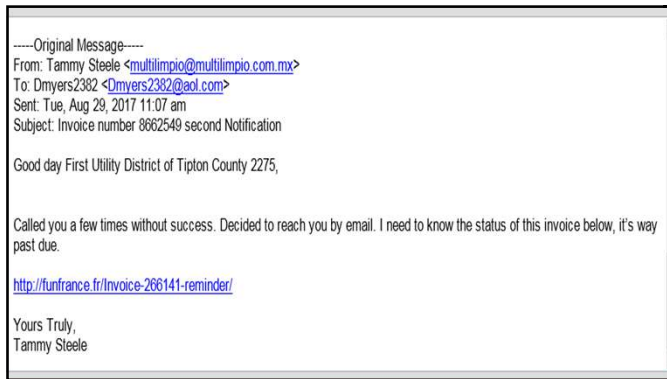
---

---

---

---

---



34

---

---

---

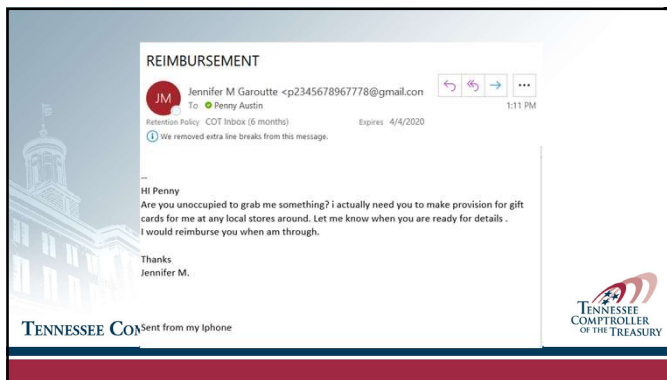
---

---

---

---

---



35

---

---

---

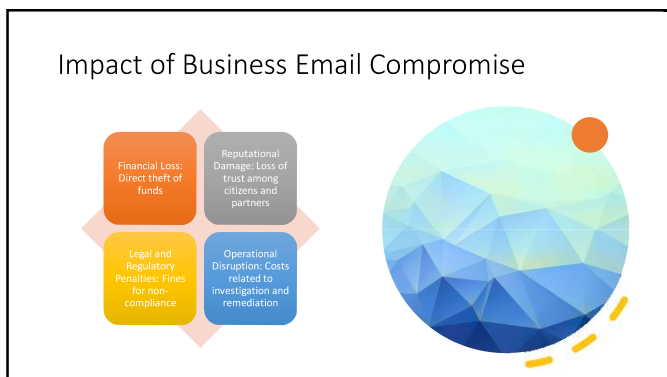
---

---

---

---

---



36

---

---

---

---

---

---

---

---



37

---

---

---

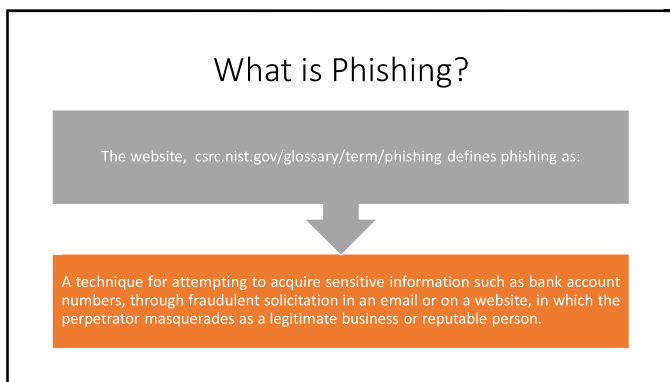
---

---

---

---

---



38

---

---

---

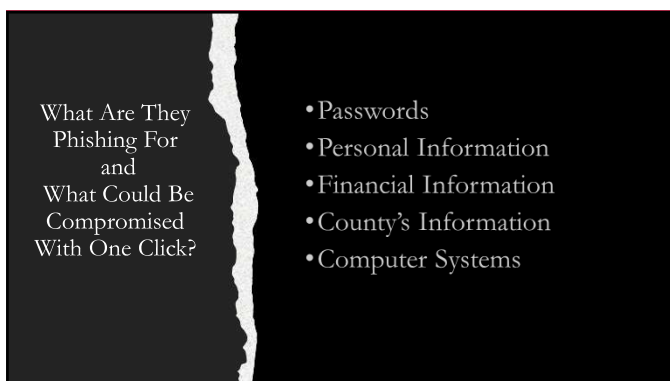
---

---

---

---

---



39

---

---

---

---

---

---

---

---



40

---

---

---

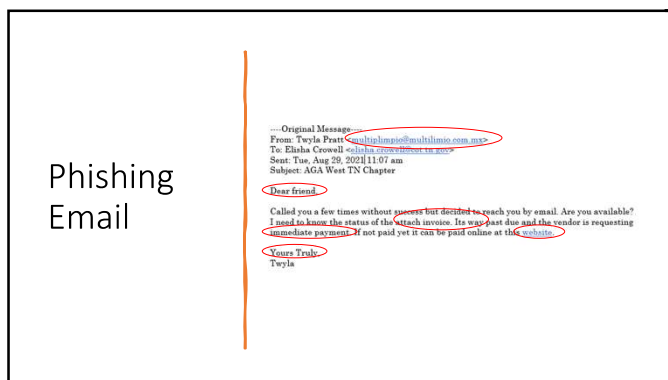
---

---

---

---

---



41

---

---

---

---

---

---

---

---



42

---

---

---

---

---

---

---

---



43

---

---

---


---

---

---

---

---

 Password Complexity

- Avoid using widely known information.
- The longer, the better.
- Create a passphrase which consists of multiple words and is at least 14 characters long.

44

---

---

---


---

---

---

---

---

 Passwords – Dos and Don'ts

<u>DOS</u>	<u>DON'T</u>
Use different passwords for all accounts	Don't use widely known information
Change passwords regularly	Don't write down and "hide" your password
Create strong, memorable passwords	Don't save passwords in browsers

45

---

---

---

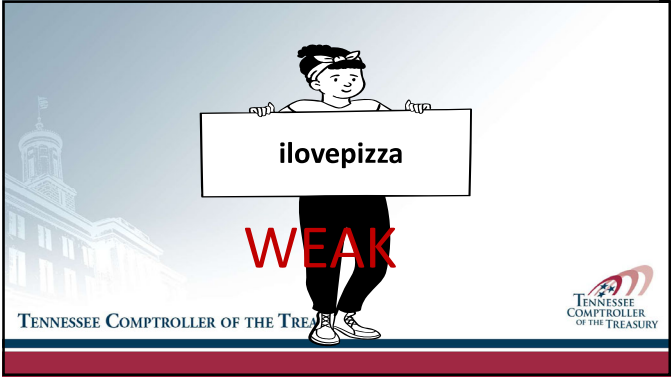
---

---

---

---

---



46

---

---

---

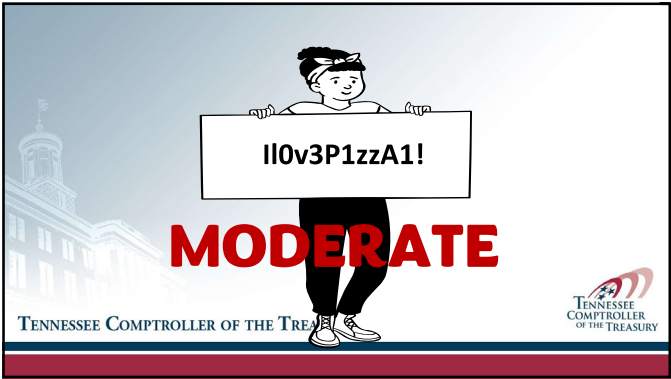
---

---

---

---

---



47

---

---

---

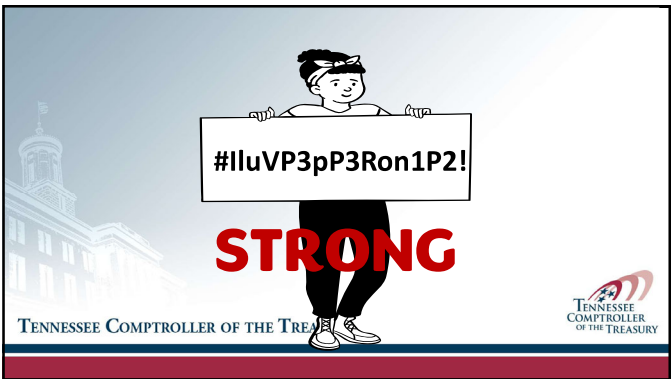
---

---

---

---

---



48

---

---

---

---

---

---

---

---



## How to Prevent Cybersecurity Threats like BEC!

- Multi-factor authentication



49

---

---

---

---

---

---

---

---

## What Do I Do If I Suspect I Have Responded to a Threat like BEC or Phishing?



Don't Panic



Report it immediately to management.



Follow your organizations cyber policy/cyber-attack plan.



If needed, management should seek guidance from IT or software vendors.



50

---

---

---

---

---

---

---

---



## 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.

51

---

---

---

---


---


---


---


---

### 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



•Click  
•Click  
•Click

52

---

---

---


---


---

---

---

---





STOP and THINK  
before  
You CLICK

53

---

---

---

---

---

---


---


---

**BACKUP! BACKUP! BACKUP!**

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

54

---

---

---

---

---

---

---

---



55

---

---

---

---

---

---

---



56

---

---

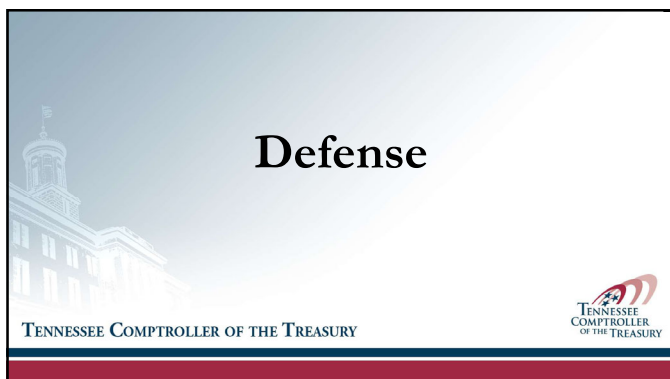
---

---

---

---

---



57

---

---

---

---

---

---

---

## Education

### Security Awareness Training



58

---

---

---

---

---

---

---

---



59

---

---

---

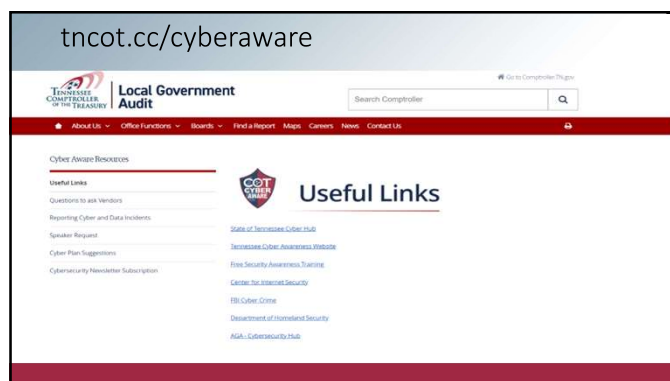
---

---

---

---

---



60

---

---

---

---

---

---

---

---



61

---

---

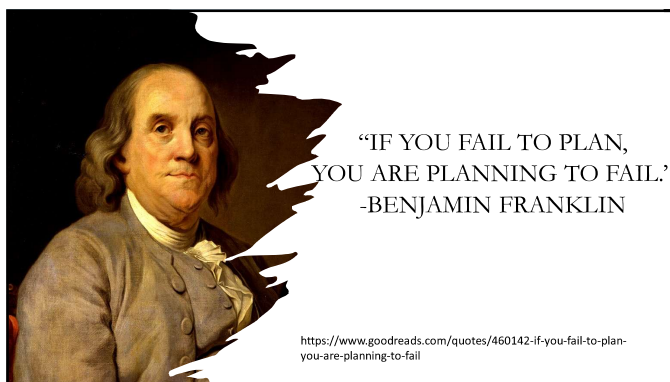
---

---

---

---

---



62

---

---

---

---

---

---

---



63

---

---

---

---

---

---

---

[illegible]

---

---

---

---

---

---

---

---

---

---

---

---

## Best Defense-Recap

- Cybersecurity Awareness Training
- Create Strong Passwords and change regularly.
- Do not share your passwords.
- Use MFA (Multifactor Authentication)
- Develop a Cybersecurity Plan
- Understand Your Office's Cybersecurity Posture
- Know what your sensitive data is and where it is stored.
- Use antivirus software and anti-malware software on computers to detect malicious software.
- Update your operating system
- Backup Regularly
- Most importantly, be a good team member. Be mindful, think before you click. Communicate to appropriate level of management if something seems off or if you think you may have clicked on something.

67

---

---

---

---

---

---

---

---

## CIA TRIAD

- Confidentiality
- Integrity
- Availability



68

---

---

---

---

---

---

---

---

## Best Defense-Overlap

### How Do We Maintain Confidentiality of Our Data and Networks?

- Employee Training
- Know what your sensitive information is and where it is stored.
- Restricting access to least privileged users.
- Strong Password Protection Or Multi-factor Authentication.
- Logging Out of the Application when away from workstations and locking the workstation. To lock select Ctrl+Alt+Delete.
- Password protected screen savers or sleep settings that activate within 30 minutes or less of inactivity.

### How Do we Maintain Integrity of our Data and Networks?

- Employee Training
- Physical Security
- Backup and Recovery Procedures and Plans
- Least privileged user access
- Data Validation and Verification
- Audit Trails and logs.

### How Do We Protect Availability of our Data and Networks?

- Employee Training
- Update and Patch
- Backup Data Daily.
- Redundancy of backups/ store off-site weekly.
- Inventory your data.
- Implement and follow Record Retention Policies.
- Proper Disposal of data and records.
- Monitoring

69

---

---

---


---

---

---


---

---



# Conclusion

TENNESSEE COMPTROLLER OF THE TREASURY



70

---

---

---


---

---

---

---

---



**“Be In The Know!”  
That  
Makes You A Winner!**

---

**Go Vols!**

71

---

---

---

---

---

---

---


---



# Questions?

Barbara Shults  
[Barbara.Shults@cot.tn.gov](mailto:Barbara.Shults@cot.tn.gov)  
 615-747-5359  
[tn.cot.cc/cyberaware](http://tn.cot.cc/cyberaware)

TENNESSEE COMPTROLLER OF THE TREASURY



72

---

---

---

---

---

---

---

---