


# “Hackers Paradise,” The Fantasy Island of Cyber Deception, Threats, and Nightmares

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

May 9, 2025

TENNESSEE COMPTROLLER OF THE TREASURY



1

---

---

---

---

---

---

---

---



## Meet My People

2

---

---

---

---

---

---

---

---

## About Us



Jason Mumpower      Jim Arnette

**THE BOSSES**

3

---

---

---

---

---

---

---

---



Nathan Abbott

Eliza Crowell

Taylor Smith

Rachel DeFries

Bethany Graves

Christovita Smith

Jami Paladini

Barbara Shults

Emma Hayne

Shania Leonard

Julie Davis-Shelton

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-  
Don't be a tourist in "Hacker's Paradise."  
"Hacker's Paradise is Not Paradise!"

- I. Define and Compare Hacker's Paradise/Fantasy Island
- II. Define Cybersecurity
- III. Responsibility
  - Who is at Risk?
- III. Cyber Threats/Nightmares
  - a. Social Engineering
  - b. Phishing/Smishing/Vishing.
  - c. Business Email Compromise-BEC
  - d. Ransomware/Malware
  - d. Weak Passwords
- .IV. Rules of Protection
  - a. Cybersecurity Training
  - b. Create Strong Passwords
  - c. Multifactor Authentication
- V. Conclusion/Questions

---

---

---

---

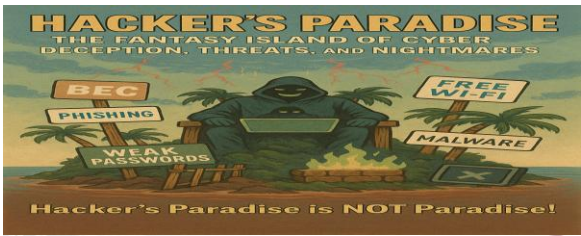
---

---

---

---

7



TENNESSEE COMPTROLLER OF THE TREASURY



---

---

---

---

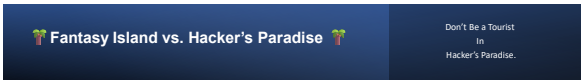
---

---

---

---

8



Feature  
Welcome Message  
Main Attraction  
Guests  
Hotel Wi-Fi  
Key Souvenirs  
Tour Guides  
Entertainment  
Theme Nights  
Hidden Traps  
Natural Disasters  
Exit Plan

**Fantasy Island**  
"Your dreams come true here."  
Magical wish fulfillment.  
Tourists looking for fantasy experiences.  
Just convenient.  
Photos, memories.  
Charming and helpful.  
Adventure, romance, and mystery.  
Masquerade Ball.  
Cursed relics or strange island magic.  
Sudden tropical storms.  
Return flight home.

**Hacker's Paradise**  
"Your worst digital nightmares start here."  
Exploiting your digital desires (free Wi-Fi, too-good-to-be-true deals).  
Hackers, scammers, cybercriminals looking for low-hanging fruit.  
Public and unsecured—ripe for **man-in-the-middle attacks**.  
Use **credentials, bank logins, sensitive emails**.  
Social engineers posing as tech support, HR, or even friends.  
Phishing emails, vishing calls, smishing texts all disguised as urgent or enticing.  
**BEC Attacks** (Business Email Compromise) where hackers pretend to be your boss.  
**Weak passwords, unpatched IoT devices, and default router settings**.  
**Ransomware attacks** that lock up your files and demand Bitcoin.  
No easy way out without **backups, cyber hygiene, and incident response plans**.

---

---

---

---

---

---

---

---

9

## "Hacker's Paradise"

**NOT A VACATION HAVEN**  
Paradise is **NOT** Paradise!  
Don't be a tourist.

**It is an environment with poor cybersecurity practices or a lack of awareness.**

- Hackers can enjoy easy access.
- Security holes are like open beach bars.
- Every system is a potential treasure chest.
- The only waves are waves of data being stolen.



10

---

---

---

---

---

---

---

---

## WHAT DO THESE HAVE IN COMMON?

City of Knoxville  
Knoxville Police & Fire Department  
Coffee County Sheriff's Office  
Spring Hill City & 911  
Maury County 911  
Murfreesboro Police & Fire Department  
Rutherford County

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

11

---

---

---

---

---

---

---

---

## I. DEFINE CYBERSECURITY

TENNESSEE COMPTROLLER OF THE TREASURY



12

---

---

---

---

---

---

---

---

## 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



13

---

---

---

---

---

---

---

---



14

---

---

---

---

---

---

---

---

## II. RESPONSIBILITY

TENNESSEE COMPTROLLER OF THE TREASURY



15

---

---

---

---

---

---

---

---



**SHARED RESPONSIBILITY** KEEP THE ISLAND SAFE!!!

16

---

---

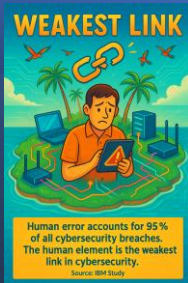
---

---

---

---

---



17

---

---

---

---

---

---

---



18

---

---

---

---

---

---

---



19

---

---

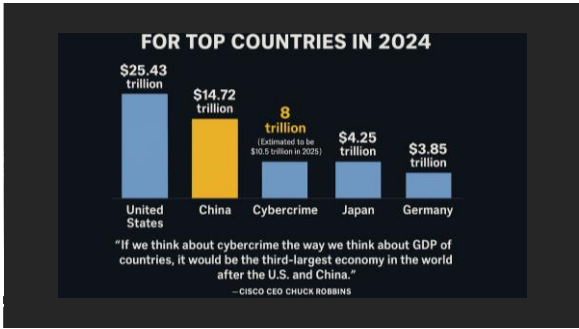
---

---

---

---

---



20

---

---

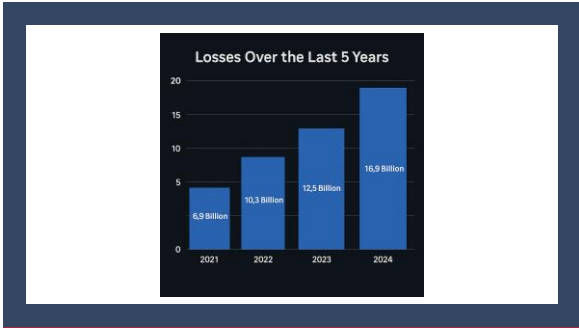
---

---

---

---

---



21

---

---

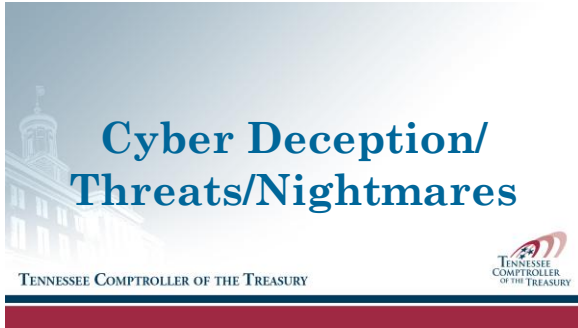
---

---

---

---

---



22

---

---

---

---

---

---

---

---



23

---

---

---

---

---

---

---

---

## SOCIAL ENGINEERING

A type of cyber attack that exploits human nature to manipulate people for information

**WHY IT WORKS:**

- Plays on emotions like fear or greed
- Exploits our tendency to be helpful
- Impersonates trusted people or companies

**DEFENSES:**

- Be wary of unusual requests
- Verify identities before sharing
- Don't give in to high-pressure tactics
- Limit personal info shared online
- Educate and train employees

Educate and train employees

**How People Really Get Hacked!**

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

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

24

---

---

---

---

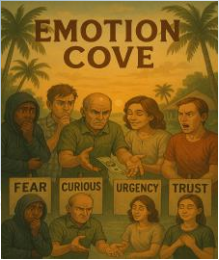
---

---

---


---





Social Engineering takes advantage of human behaviors using psychological manipulation. The user may respond due to:

- Fear
- Curiosity
- Greed
- Helpfulness
- Urgency
- Trust



TENNESSEE COMPTROLLER OF THE TREASURY

---

---

---

---


---

---

---

---

25



TENNESSEE COMPTROLLER OF THE TREASURY



---

---

---

---

---


---

---

---

26

PHISHING  
AND  
BUSINESS EMAIL COMPROMISE



TENNESSEE COMPTROLLER OF THE TREASURY

---

---

---

---

---

---

---

---

27



What is Phishing  
and  
What are they Phishing For?

28

---

---

---

---

---

---

---

---



29

---

---

---

---

---

---

---

---

Phishing  
Email

---Original Message  
From: Terla Pao [terla.pao@pacbell.net](mailto:terla.pao@pacbell.net)  
To: Eliza Crowell [eliza.crowell@pacbell.net](mailto:eliza.crowell@pacbell.net)  
Sent: Tue, Apr 29, 2024 11:07 am  
Subject: AGA West TN Chapter  
  
Dear friend,  
Called you a few times without answer but wanted to reach you by email. Are you available?  
I need to know the status of the attach invoice. Its was just due and the vendor is requesting  
immediate payment. If not paid yet it can be paid online at the website.  
Love Terla  
Terla

30

---

---

---

---

---

---

---

---

**Definition: Business Email Compromise**

A type of cybercrime in which the attacker uses email to trick someone into sharing sensitive and confidential information or sending funds to them through various means, including wire transfers, gift cards, or other means of paying fake invoices. It is an exploitation of our email by impersonating a trusted party.

**BEC: THE SMOOTH-TALKING PIRATE OF HACKER'S PARADISE**

**What is BEC?** Business Email Compromise is a type of cyberattack where a hacker impersonates a trusted figure—like a CEO, vendor, or coworker—via email to trick employees.

**Common BEC Red Flags**

- Are you available? emails
- Spoofed domains
- Urgent financial requests

**Why it's a Favorite in Hacker's Paradise:**

- Fake bosses requesting wire transfers from a 1st bar
- No malware or brute force
- Just pure deception

**How to Escape the Island Trap**

- Train your team
- Use MFA

TENNESSEE COMPTROLLER OF THE TREASURY

31

---

---

---

---

---

---

---

---

**Phishing vs. BEC**

The illustration shows a fisherman in a hat and floral shirt casting a net full of email icons into the water. In the background, a pirate with a beard and a target on his chest stands on a beach, holding a spear. A small boat with a person inside is visible in the water.

TENNESSEE COMPTROLLER OF THE TREASURY

32

---

---

---

---

---

---

---

---

**In 2022 BEC accounted for 50 percent of social engineering tactics**

**In 2023 BEC accounted for 99 percent of reported email-based threats**

TENNESSEE COMPTROLLER OF THE TREASURY

33

---

---

---

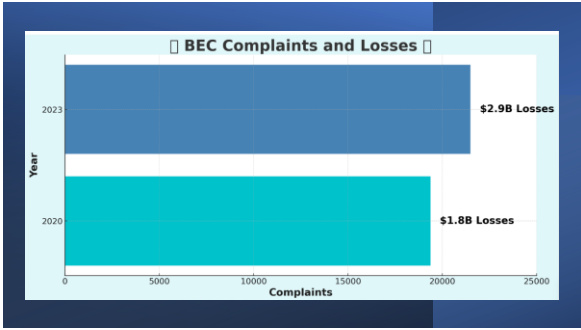
---

---

---

---

---



34

---

---

---

---

---

---

---



35

---

---

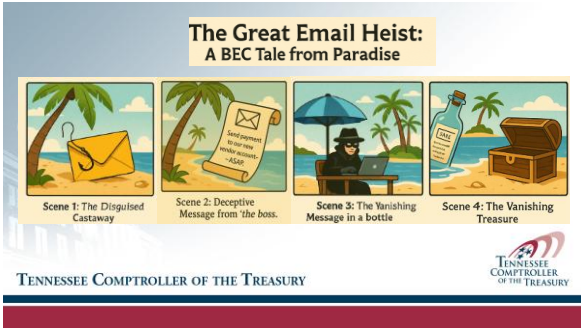
---

---

---

---

---



36

---

---

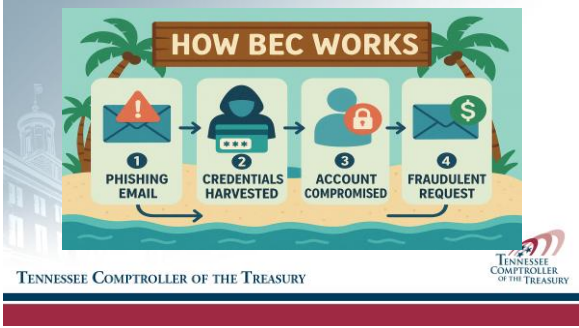
---

---

---

---

---



37

---

---

---

---

---

---

---

---



38

---

---

---

---

---

---

---

---

### BEC Attacks

In 2018, the city of Atlanta, Georgia experienced a ransomware attack that severely disrupted municipal services. The ransomware encrypted critical files across the city's network, forcing systems offline and leading to significant recovery efforts. The attack, which did not involve a ransom payment, resulted in an estimated financial loss of around \$17 million due to recovery costs and operational downtime.

TENNESSEE COMPTROLLER OF THE TREASURY

39

---

---

---

---

---

---

---

---

## BEC Attacks



Atlanta-Children's Hospital -CFO was impersonated convinces the A/P dept. to switch bank on file and send \$3.6 million dollars.

TENNESSEE COMPTROLLER OF THE TREASURY



40

---

---

---

---

---

---

---

---

## BEC Attacks



Eagle Mountain City, Utah- Vendor emails that appeared to be legitimate were sent to the city. Instructions were changed on the ACH payment, and \$1.13 million dollars were sent to a fraudulent account. Account compromise for vendor and a VEC for the city.

TENNESSEE COMPTROLLER OF THE TREASURY



41

---

---

---

---

---

---

---

---

## BEC Attacks



Toyota-3<sup>rd</sup> party hacker posed as a business partner-Subsidiary emails were sent to the accounting dept. asking them to send funds to a specific bank account or that production would be stopped. This was an account compromise of the business partner and a VEC compromise for Toyota.

TENNESSEE COMPTROLLER OF THE TREASURY



42

---

---

---

---

---

---

---

---

# BEC Attacks



City of Lexington, KY-hacker claims to be from Community Action Council which is a local housing group. They asked to update their account information. 4 million dollars was sent.

TENNESSEE COMPTROLLER OF THE TREASURY



43

---

---

---

---

---

---

---

---

# BEC Attacks



In 2020, Rutherford County in Tennessee experienced a BEC attack where scammers gained access to email accounts of county employees. They used this access to impersonate officials and orchestrate fraudulent wire transfers. The attack led to significant financial losses of \$2.3 millions for the county.

TENNESSEE COMPTROLLER OF THE TREASURY



44

---

---

---

---

---

---

---

---

# BEC Attacks



In 2021, the City of Jackson experienced a BEC attack where attackers managed to intercept and alter email communications related to a financial transaction. As a result, they redirected funds intended for a legitimate payment into their own accounts.

The city of Jackson suffered a loss of approximately \$1.5 million due to this attack.

TENNESSEE COMPTROLLER OF THE TREASURY



45

---

---

---

---

---

---

---

---

## BEC Attacks



In 2019, the City of Memphis in Tennessee experienced a BEC attack where attackers targeted the city's finance department by compromising email accounts and using them to impersonate officials. This led to fraudulent wire transfers, resulting in approximately \$3.2 million in losses.

TENNESSEE COMPTROLLER OF THE TREASURY



46



47

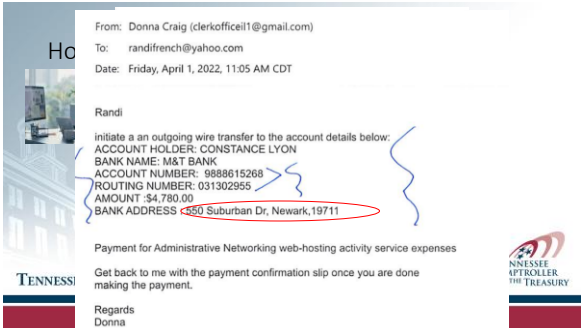
## Real-World Example

> On Friday, April 1, 2022, 10:38:55 AM CDT, Donna Craig  
 > <[clerk@mccl1@gmail.com](mailto:clerk@mccl1@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](mailto:randifrench@yahoo.com)> wrote:  
 > Yes ma'am I sure can :)  
 > Thank you, Randi French, Henry County Trustee

48





49

---

---

---

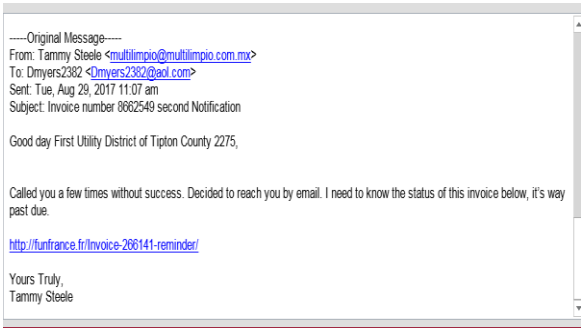
---

---

---

---

---



50

---

---

---

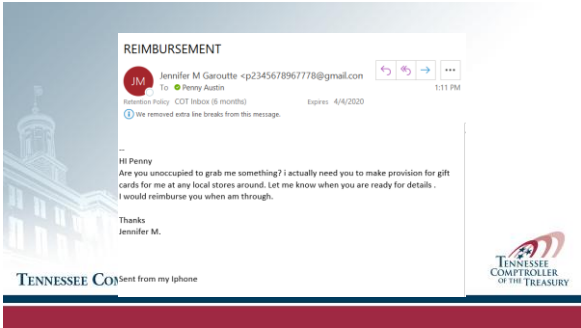
---

---

---

---

---



51

---

---

---

---

---

---

---

---



52

---

---

---

---

---

---

---

---

**FBI Knoxville**  
Public Affairs Officer Daniel DeLuca  
(615) 544-6752

March 7, 2024

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

KNOXVILLE, TN—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 ranked 31st in the country, with residents lodging a total of 8,484 complaints with the FBI's Internet Crime Complaint Center (IC3), reporting losses amounting to \$161,195,000. These figures underscore the devastating impact cybercrime has on individuals and businesses statewide.

"We've 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 Caruso, special agent in charge of the FBI's Knoxville field office. "Cybercriminals are always coming up with new tricks to scam people, 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 we're protecting ourselves online."

Scam, support scams, investment fraud, and business email compromise (BEC) emerged as the leading categories for losses in Tennessee. Particularly alarming is the heightened risk faced by individuals over 60, who are most susceptible to falling victim to these cyber scams.

Notably, in 2023, the IC3 recorded a staggering 885,419 complaints, indicating a substantial rise in cybercrime activity across the nation. The total losses incurred from these incidents amounted to a staggering \$12.5 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 financial 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 emails from unfamiliar sources. Don't share sensitive information, especially your social security number, with anyone online. 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 Tennesseans against cyber threats. 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).

53

---

---

---

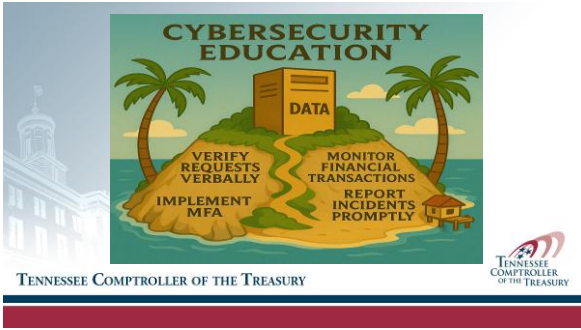
---

---

---

---

---



54

---

---

---

---

---

---

---

---

## Ransomware and Malware

TENNESSEE COMPTROLLER OF THE TREASURY



55

---

---

---

---

---

---

---

---

### Ransomware/Malware Defined

Malware is malicious software.

Ransomware is a type of malicious software that is a form of high-tech extortion where the malicious software hijacks computer systems and holds them hostage until the victim pays a ransom.



56

---

---

---

---

---

---

---

---

## RANSOMWARE AND MALWARE CLICK! CLICK!



- fake and unsafe websites.
- unsuspected emails and attachments.
- bad links in email or social media ads, videos, articles, and Messenger

TENNESSEE COMPTROLLER OF THE TREASURY



57

---

---

---

---

---

---

---

---



58

---

---

---

---

---

---

---



59

---

---

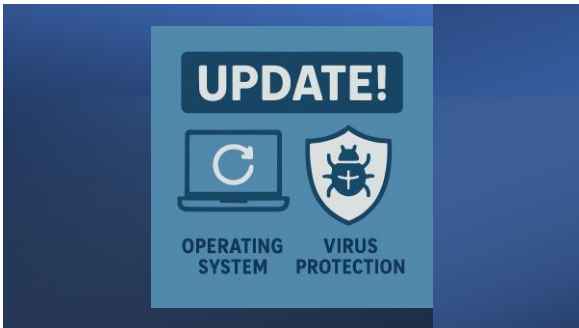
---

---

---

---

---



60

---

---

---

---

---

---

---


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

**WHAT SHOULD I DO IF I CLICKED?**

Don't panic. Follow your organization's cyber-policy and cyber-attack plan.

Report to management immediately. If needed, management should seek guidance from software and IT vendors.

TENNESSEE COMPTROLLER OF THE TREASURY



61

---

---

---

---

---


---

---

---

How Do We Stay Away From “Hacker’s Paradise?”

TENNESSEE COMPTROLLER OF THE TREASURY



62

---

---

---

---

---


---

---

---

STRONG PASSWORDS  
AND  
MULTI-FACTOR  
AUTHENTICATION

TENNESSEE COMPTROLLER OF THE TREASURY



63

---

---

---

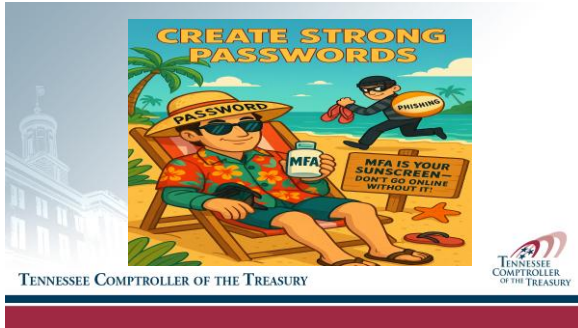
---

---

---

---

---



64

---

---

---

---

---

---

---

---



65

---

---

---

---

---

---

---

---



66

---

---

---

---

---

---

---

---



67

---

---

---

---

---

---

---



68

---

---

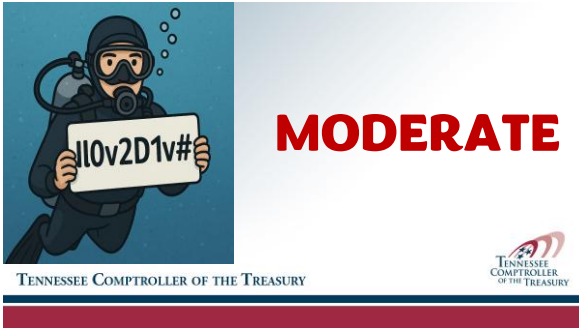
---

---

---

---

---



69

---

---

---

---

---

---

---



**STRONG**

TENNESSEE COMPTROLLER OF THE TREASURY



70

---

---

---


---

---


---

---

---



TENNESSEE COMPTROLLER OF THE TREASURY



71

---

---

---

---

---

---

---

---

**Other Important Protection Rules**

TENNESSEE COMPTROLLER OF THE TREASURY



72

---

---

---

---

---

---

---

---



Education

Security Awareness Training



---

---

---

---

---

---

---

73



---

---

---

---

---

---

---

74



---

---

---

---

---

---

---

75



76

---

---

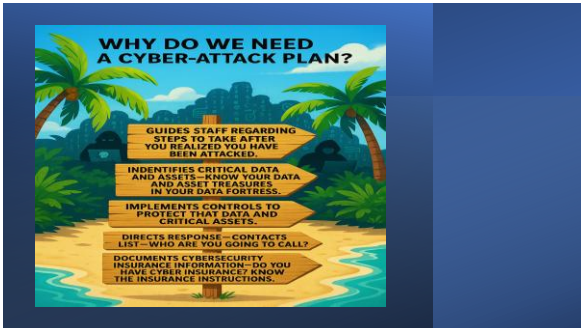
---

---

---

---

---



77

---

---

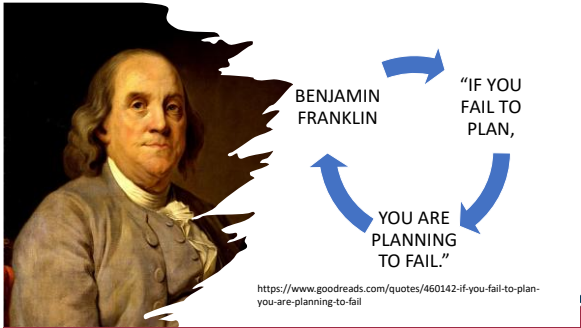
---

---

---

---

---



78

---

---

---

---

---

---

---



# Conclusion

TENNESSEE COMPTROLLER OF THE TREASURY

  
TENNESSEE  
COMPTROLLER  
OF THE TREASURY

79

---

---

---

---

---

---

---



80

---

---


---

---

---

---

---



## Data Island Safety Measures

TENNESSEE COMPTROLLER OF THE TREASURY

  
TENNESSEE  
COMPTROLLER  
OF THE TREASURY

81

---

---

---

---

---

---

---



• **Stay Safe with These Island Rules:**

1. **Education-Participate** in Cybersecurity Trainings often.
2. **Create Strong Passwords**  
Use passphrases or complex combinations — change them often.
3. **Never Share Your Passwords**  
Not even with your "Captain."
4. **Use MFA (Multi-Factor Authentication)**  
Two ways to unlock the treasure.
5. **Develop a Cybersecurity Plan**  
Every island needs a map.
6. **Know Your Sensitive Data and understand your cybersecurity posture.**  
What's the treasure, and where is it buried?
7. **Install Antivirus & Anti-Malware Software**  
Watch for sneaky creatures in the sand.
8. **Keep Operating Systems Updated**  
Patch those daily beach holes.
9. **Backup Regularly**  
Keep a lifeboat ready offshore.
10. **Run Phishing Simulations**  
Practice spotting the fake bait.
11. **Be a Good Crew Member**  
Stay alert, think before you click, and report anything suspicious.

---

---

---

---

---

---

---

---

82

### What to Do If There Is a Cybersecurity Attack

|  |   |
|--|---|
| <b>1. Detect and Identify</b><br>Monitor for suspicious activity | <b>4. Eradicate the Threat</b><br>Remove malware and access     |
| <b>2. Contain the Threat</b><br>Isolate affected systems         | <b>5. Recover Operations</b><br>Restore from clean backups      |
| <b>3. Assess the Damage</b><br>Investigate the scope and impact  | <b>6. Review and Learn</b><br>Analyze the incident and response |

TENNESSEE COMPTROLLER OF THE TREASURY

---

---

---

---

---

---

---

---

83

## tncot.cc/cyberaware

**Local Government Audit**

Search Comptroller

[About Us](#) [Office Functions](#) [Boards](#) [Media Report](#) [Maps](#) [Careers](#) [News](#) [Contact Us](#)

**Cyber Aware Resources**  
**Useful Links**  
[Questions to ask Vendors](#)  
[Reporting Cyber and Data Incidents](#)  
[Speaker Request](#)  
[Cyber Plan Suggestions](#)  
[Cybersecurity Newsletter Subscription](#)

**Useful Links**  
[State of Tennessee Cyber Hub](#)  
[Tennessee Cyber Awareness Website](#)  
[Info Security Awareness Training](#)  
[Center for Internet Security](#)  
[FBI Cyber Crime](#)  
[Department of Homeland Security](#)  
[NSA Cybersecurity Hub](#)

---

---

---

---

---

---

---

---

84

Map Out the Island



The map is titled "ISLAND SECURITY MAP" and shows a green island with various security-related locations. Labels include: Island, Mainland Mountain, Training Tower, CIA Trid Temple, Cybersecurity Monkey, Communication Encoder, Backlog Beach, Password Point, and Password Point. A compass rose is in the bottom left corner.

TENNESSEE COMPTROLLER OF THE TREASURY



85

---

---

---

---

---


---

---

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



86

---

---

---

---

---

---

---