


How to Avoid a Trip to
Hacker's Paradise
Shania Leonard, IS Auditor
Division of Local Government Audit
CCFO/CMFO Training Event
Knoxville, Tennessee
September 4th – 5th, 2025

TENNESSEE COMPTROLLER OF THE TREASURY



1



2



3



4

IS Staff

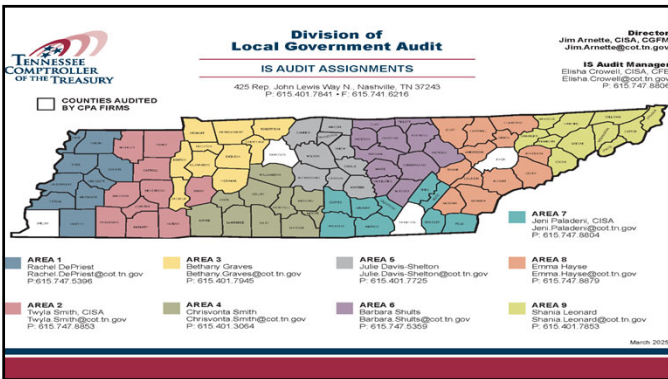




TENNESSEE COMPTROLLER OF THE TREASURY



5



6

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.

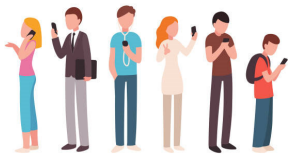
TENNESSEE COMPTROLLER OF THE TREASURY



7

DataReportal – January 2025

- 398 minutes a day
- 6.5 hours a day
- 46.5 hours a week
- 100 days a year
- 17 years of our lives



TENNESSEE COMPTROLLER OF THE TREASURY



8

HACKER'S PARADISE

THE FANTASY ISLAND OF CYBER
DECEPTION, THREATS, AND NIGHTMARES



Hacker's Paradise is NOT Paradise!

9



10

Hacker's Paradise

An environment with poor cybersecurity practices or a lack of awareness.

- Easy Access
- Security Holes
- Stolen Data
- All Systems at Risk

11

Goals of Presentation:
Don't Buy a One-Way
Ticket to Hacker's
Paradise!

- I. Define Cybersecurity
- II. Responsibility
- III. Cyber Deception and Threats
 - I. Social Engineering
 - II. Phishing Attacks
 - III. Business Email Compromise
- IV. Malware & Ransomware
- V. Weak Passwords
- IV. Rules of Protection

12

I. DEFINE CYBERSECURITY

13

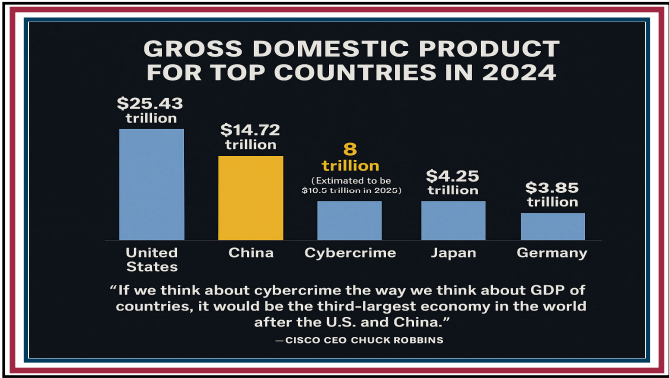
What is
Cybersecurity?



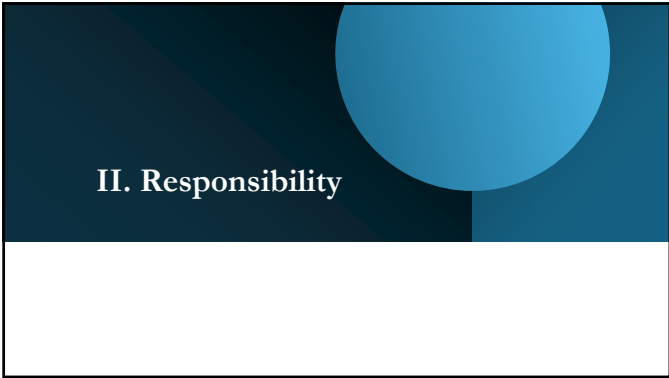
According to CISA.gov:

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.

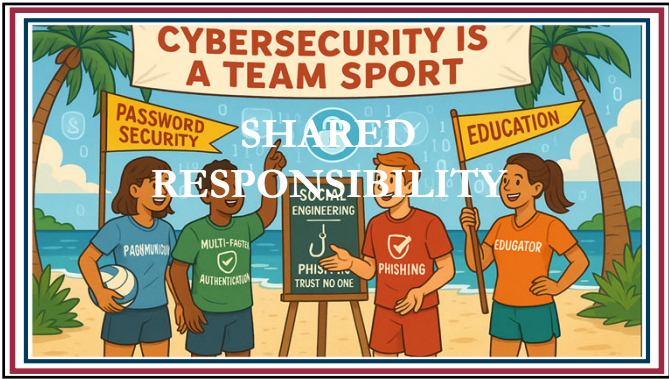
14



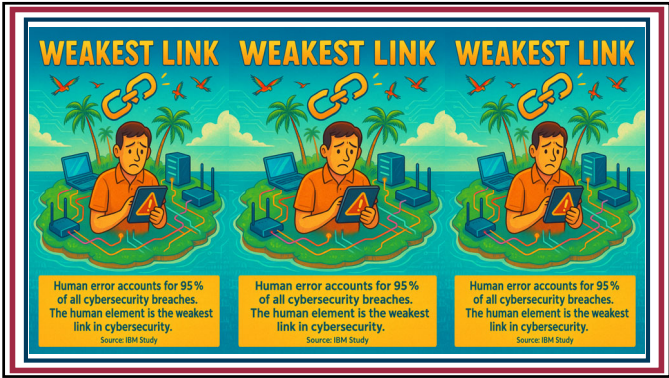
15



16



17



18



19



20



21

SOCIAL ENGINEERING

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

WHY IT WORKS:

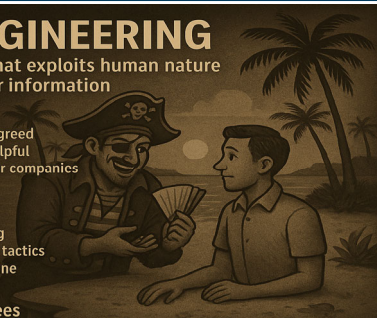
- Plays on emotions like fear or greed
- Exploits our tendency to be helpful
- Impersonates trusted people or companies

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

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



22




23

Social Engineering

takes advantage of human behaviors using psychological manipulation.

The user may respond due to:

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



24



25

Phishing

A technique for attempting to acquire sensitive information such as bank account numbers, through fraudulent solicitation in an email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

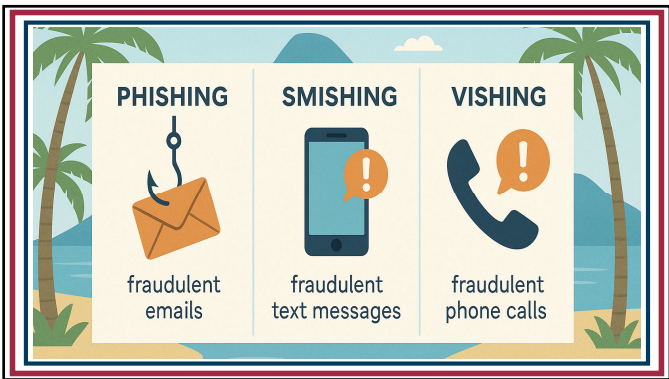
Definition source: csrc.nist.gov



What is Phishing?

What are they Phishing for?

26



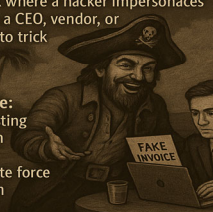
27

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

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

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



Common BEC Red Flags


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

How to Escape the Island Trap

- Train your team
- Use MFA


28

BEC Stats







2022: BEC made up **50%** of all social engineering tactics.

2023: BEC accounted for **99%** of reported email-based threats.

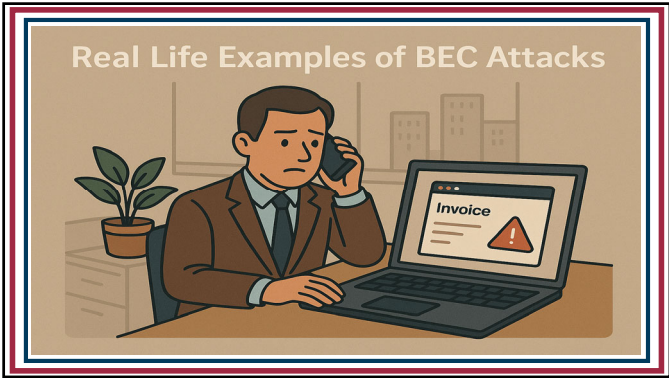


29

TYPES OF BEC ATTACKS


 <p>EXECUTIVE IMPERSONATION</p>	 <p>ATTORNEY IMPERSONATION</p>	 <p>ACCOUNT COMPROMISE</p>	 <p>VENDOR EMAIL COMPROMISE</p>
---	--	--	---

30



31

> On Friday, April 1, 2022, 10:38:55 AM CDT, Donna Craig
> <clerkoffice11@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

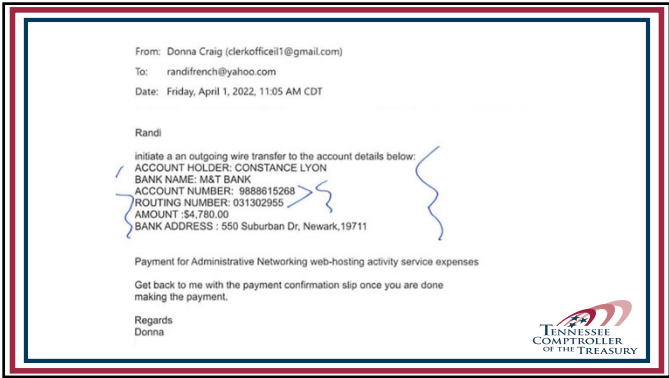


32

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



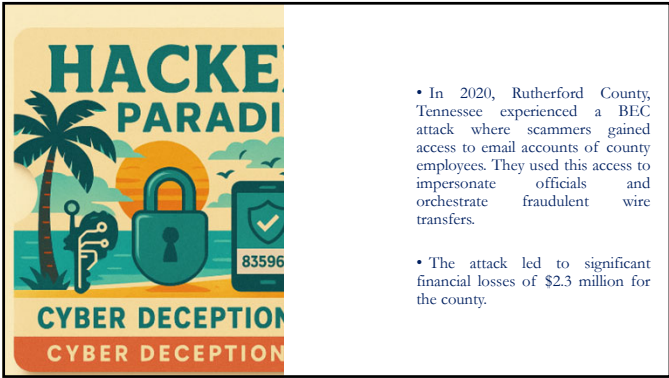
33



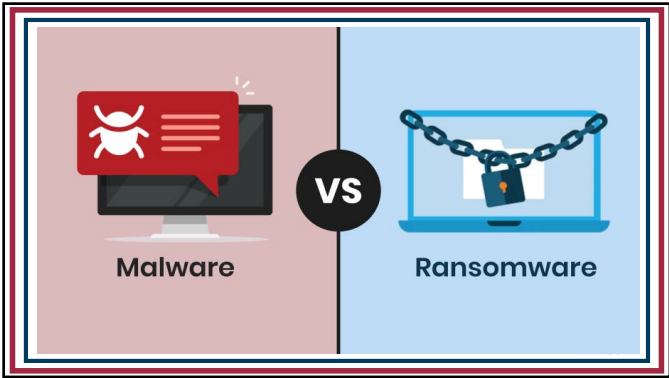
34



35



36



40

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



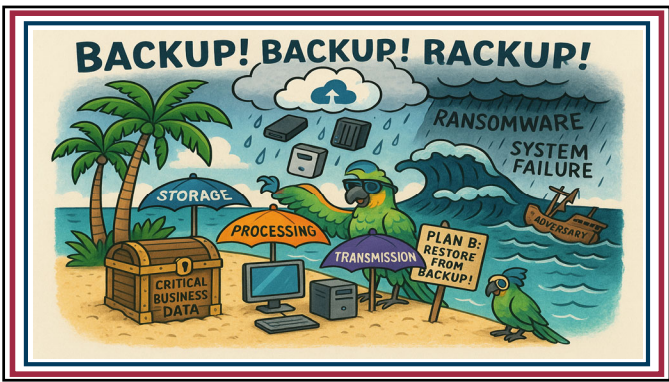
41



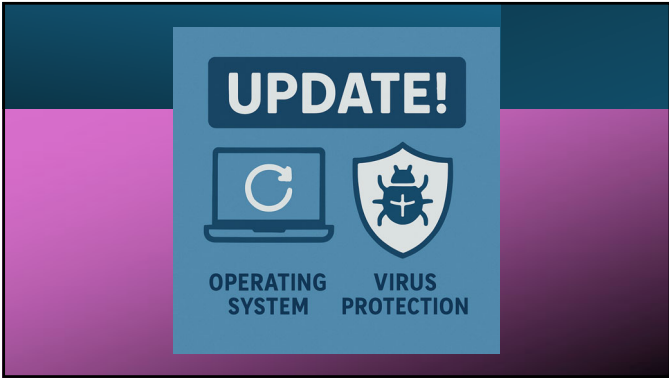
42

IV. Rules of Protection – How do we stay away from Hacker’s Paradise?

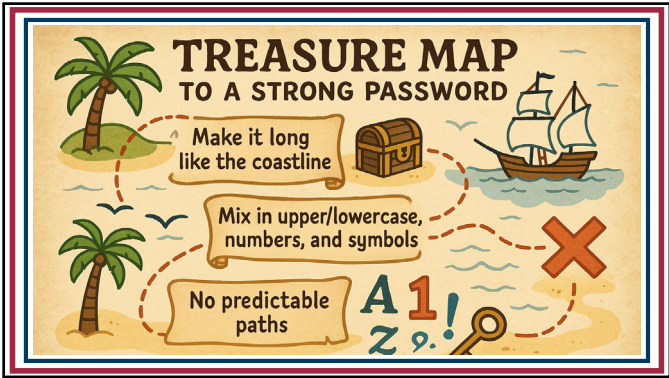
43



44



45



46

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024					
Hardware: 12 x RTX 4090 Password hash: bcrypt					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	27 secs	22 hours	8 months	2 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	36m years	165m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9m years	56bn years
16	119 years	517m years	33m years	566m years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS > Learn more about this at hivesystems.com/password

47



48

MFA

What you know – Password or Pin

What you are – Your Fingerprint, Voice Recognition, or some other biometric, such as Face ID

What you have – Access Badge

MULTI-FACTOR AUTHENTICATION

The diagram illustrates the concept of Multi-Factor Authentication (MFA) using a beach-themed background. It shows three factors being combined: 'WHAT YOU KNOW' (represented by three asterisks ***), 'WHAT YOU ARE' (represented by a fingerprint), and 'WHAT YOU HAVE' (represented by a smartphone). These three factors are added together (+) and then equated (=) to 'ACCESS'.

49

An illustration of a person wearing a hat and sunglasses, sitting at a desk with a computer. The computer screen shows a green checkmark and a shield icon. Above the person is a sign that says 'CYBERSECURITY TRAINING'. To the right of the person are two signs: 'UPDATE VIRUS PROTECTION AND ANTI-MALWARE' and 'BACKUP REGULARLY' with a circular arrow icon.

50

An illustration of a person looking thoughtful, with a speech bubble asking 'WHAT SHOULD I DO IF I CLICKED?'. Below the person, text reads: '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.' The background is a dark purple gradient with white arrows pointing in various directions.

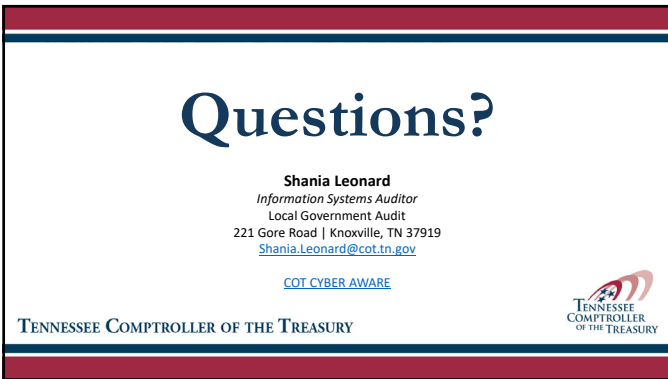
51



52



53



54
