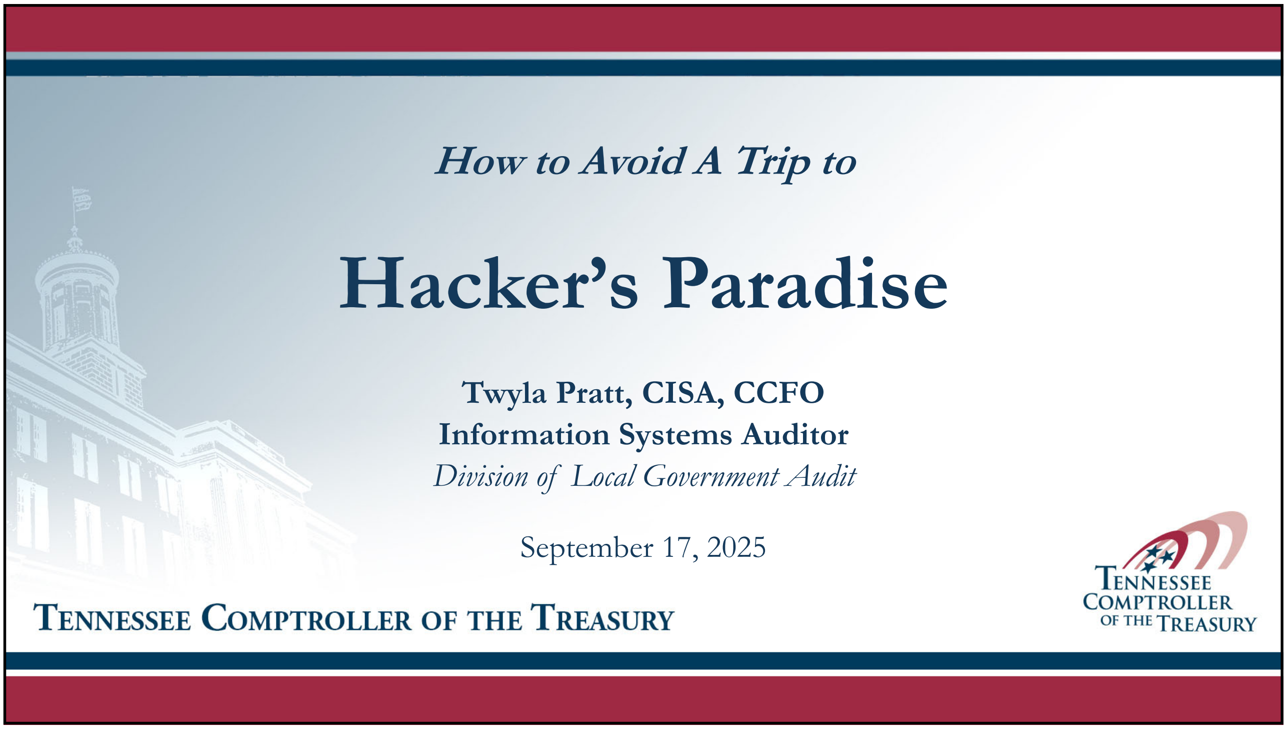


How to Avoid A Trip to

Hacker's Paradise

Twyla Pratt, CISA, CCFO
Information Systems Auditor
Division of Local Government Audit

September 17, 2025

Tennessee Comptroller of the Treasury

1

2

3

About Us

Jason Mumpower
Comptroller

Jim Arnette
Director

Tennessee Comptroller of the Treasury

4

Nathan Abbott

Elisha Crowell

Twyla Pratt

Rachel DePriest

Bethany Graves

Chrisvonta Smith

Julie Davis-Shelton

Barbara Shults

Jeni Paladeni

Emma Hayse

Shania Leonard

5

Tennessee Comptroller of the Treasury

Division of Local Government Audit

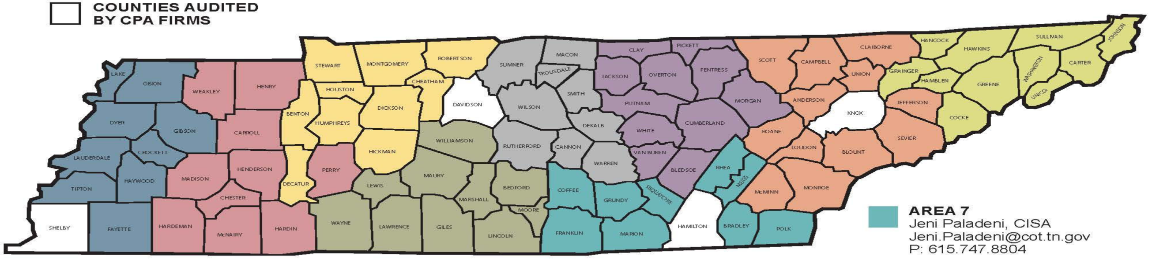
IS AUDIT ASSIGNMENTS

425 Rep. John Lewis Way N., Nashville, TN 37243
P: 615.401.7841 • F: 615.741.6216

Director
Jim Arnette, CISA, CGFM
Jim.Arnette@cot.tn.gov

IS Audit Manager
Elisha Crowell, CISA, CFE
Elisha.Crowell@cot.tn.gov
P: 615.747.8806

□ **COUNTIES AUDITED BY CPA FIRMS**



■ **AREA 7**
Jeni Paladeni, CISA
Jeni.Paladeni@cot.tn.gov
P: 615.747.8804

■ **AREA 1**
Rachel DePriest
Rachel.DePriest@cot.tn.gov
P:615.747.5396

■ **AREA 2**
Twyla Pratt, CISA
Twyla.Pratt@cot.tn.gov
P: 615.747.8853

■ **AREA 3**
Bethany Graves
Bethany.Graves@cot.tn.gov
P: 615.401.7945

■ **AREA 4**
Chrisvonta Smith
Chrisvonta.Smith@cot.tn.gov
P: 615.401.3064

■ **AREA 5**
Julie Davis-Shelton
Julie.Davis-Shelton@cot.tn.gov
P: 615.401.7725

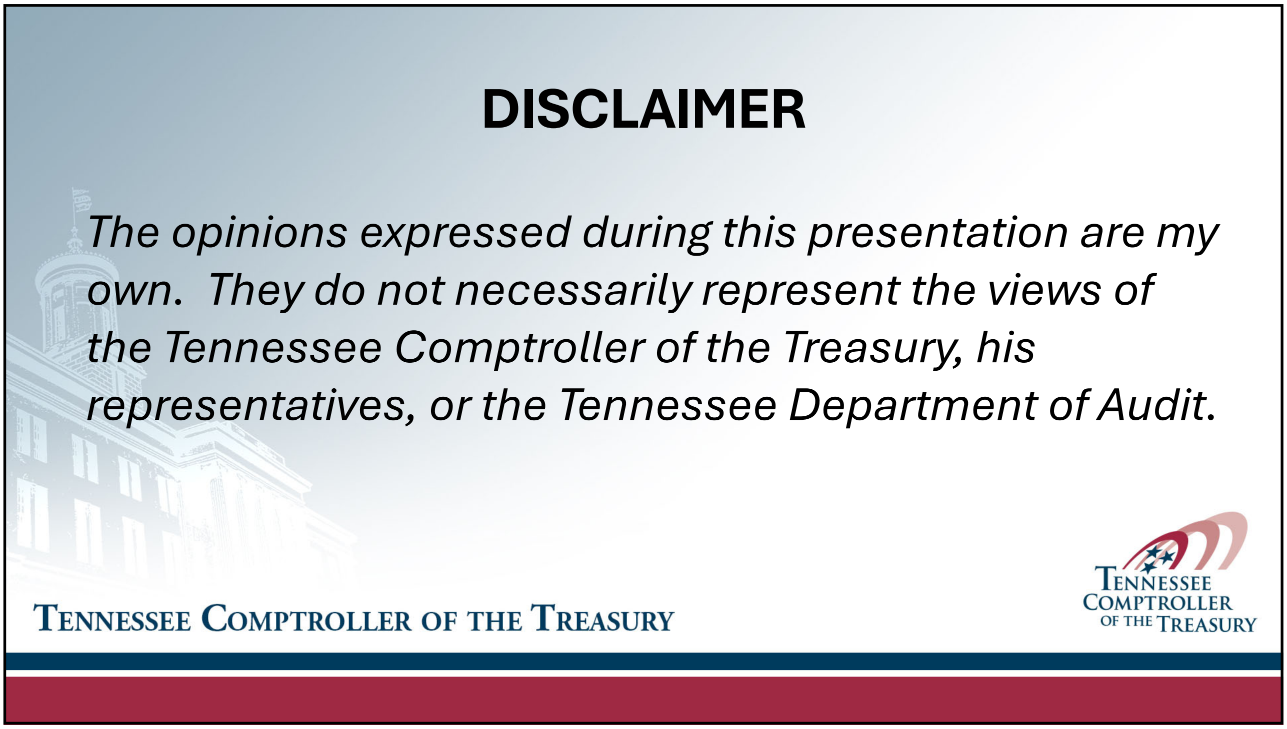
■ **AREA 6**
Barbara Shults
Barbara.Shults@cot.tn.gov
P: 615.747.5359

■ **AREA 8**
Emma Hayse
Emma.Hayse@cot.tn.gov
P: 615.747.8879

■ **AREA 9**
Shania Leonard
Shania.Leonard@cot.tn.gov
P: 615.401.7853

March 2025

6



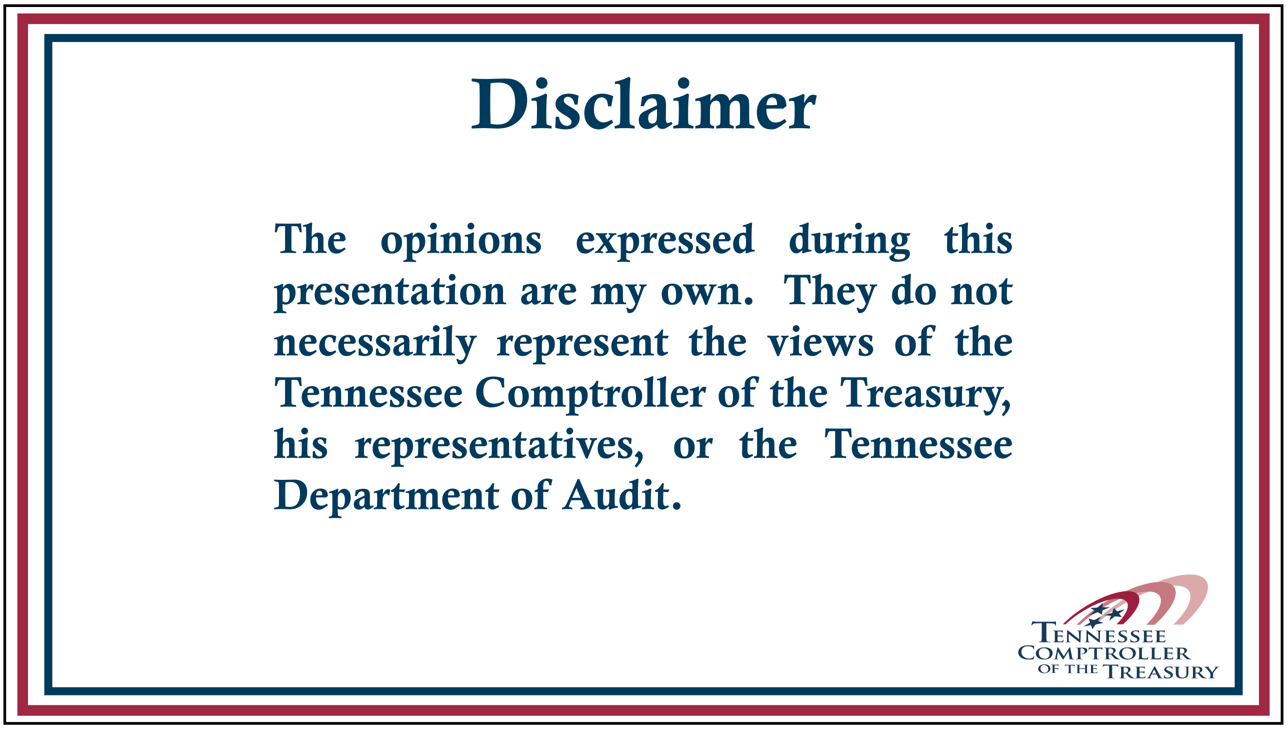
DISCLAIMER

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

Tennessee Comptroller of the Treasury

7



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.

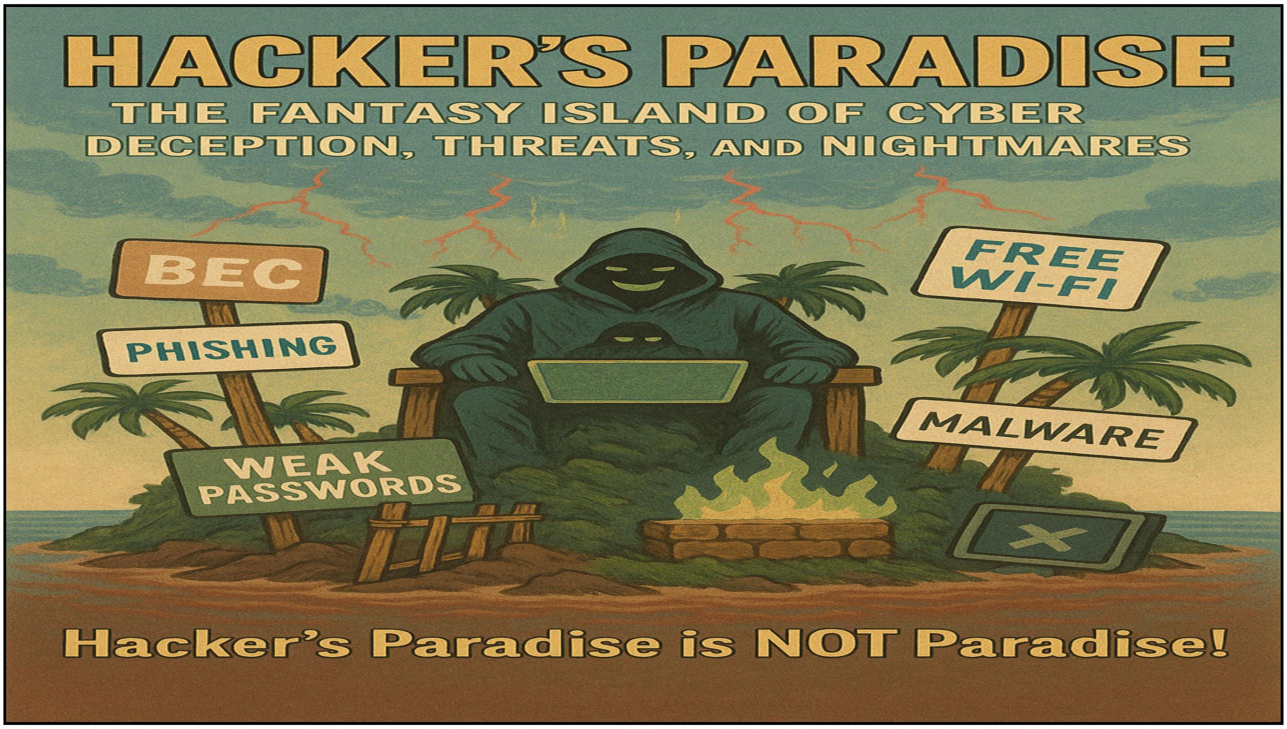
Tennessee Comptroller of the Treasury

8

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

9


HACKER'S PARADISE
THE FANTASY ISLAND OF CYBER DECEPTION, THREATS, AND NIGHTMARES
BEC
PHISHING
WEAK PASSWORDS
FREE WI-FI
MALWARE
Hacker's Paradise is NOT Paradise!

10

11

“Hacker’s Paradise”

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.

FREE Wi-Fi
PHISHING EMAILS
WEAK PASSWORDS
MALWARE
SOCIAL ENGINEERING
IOT's
RANSOMWARE
BEC

12

Goals of Presentation: Don't buy a one-way ticket to Hacker's Paradise!

```
rror_mod = modifier_ob.
t mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
= bpy.context.selected_obj
ata.objects[one.name].sel

int("please select exactly

- OPERATOR CLASSES ----

types.Operator):
X mirror to the selected
ject.mirror_mirror_x"
ror X"

context):
ext.active_object is not
```

I. Define Cybersecurity

II. Responsibility

III. Cyber Deception and Threats

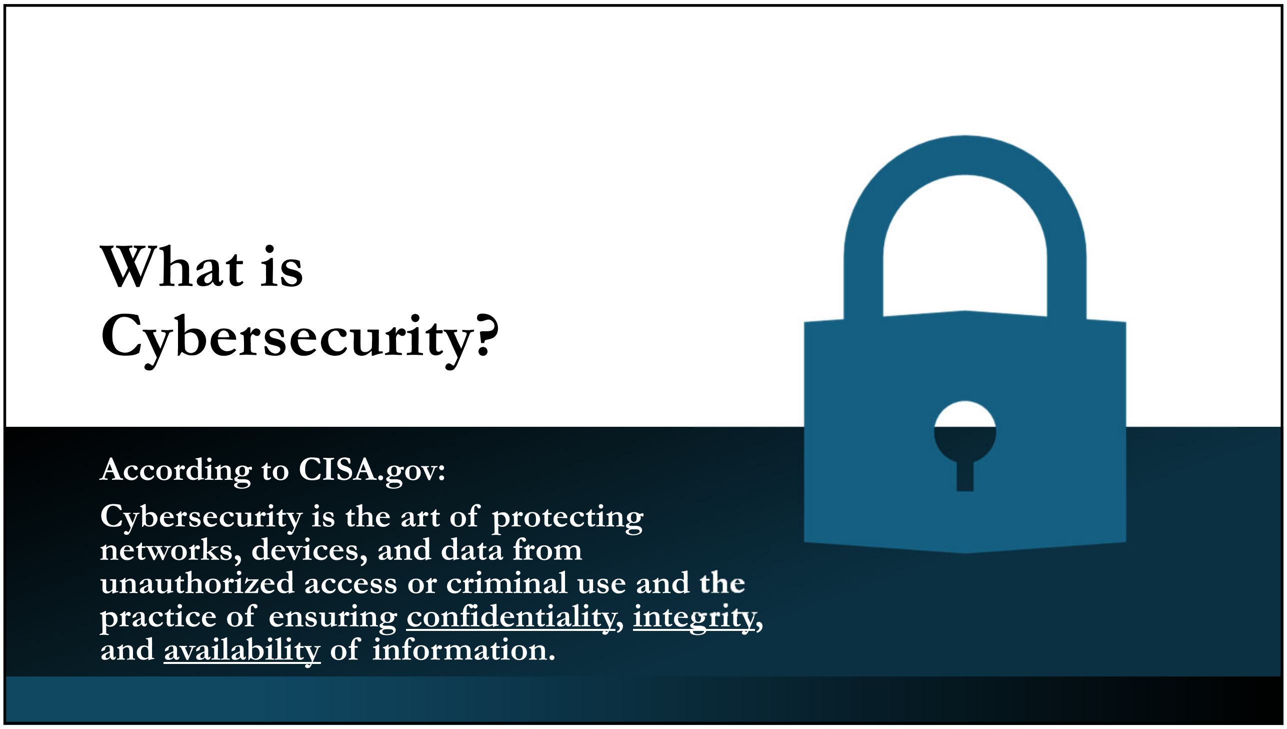
  I. Social Engineering
  II. Phishing Attacks
  III. Business Email Compromise
  IV. Malware & Ransomware
  V. Weak Passwords

IV. Rules of Protection

13

I. DEFINE CYBERSECURITY

14

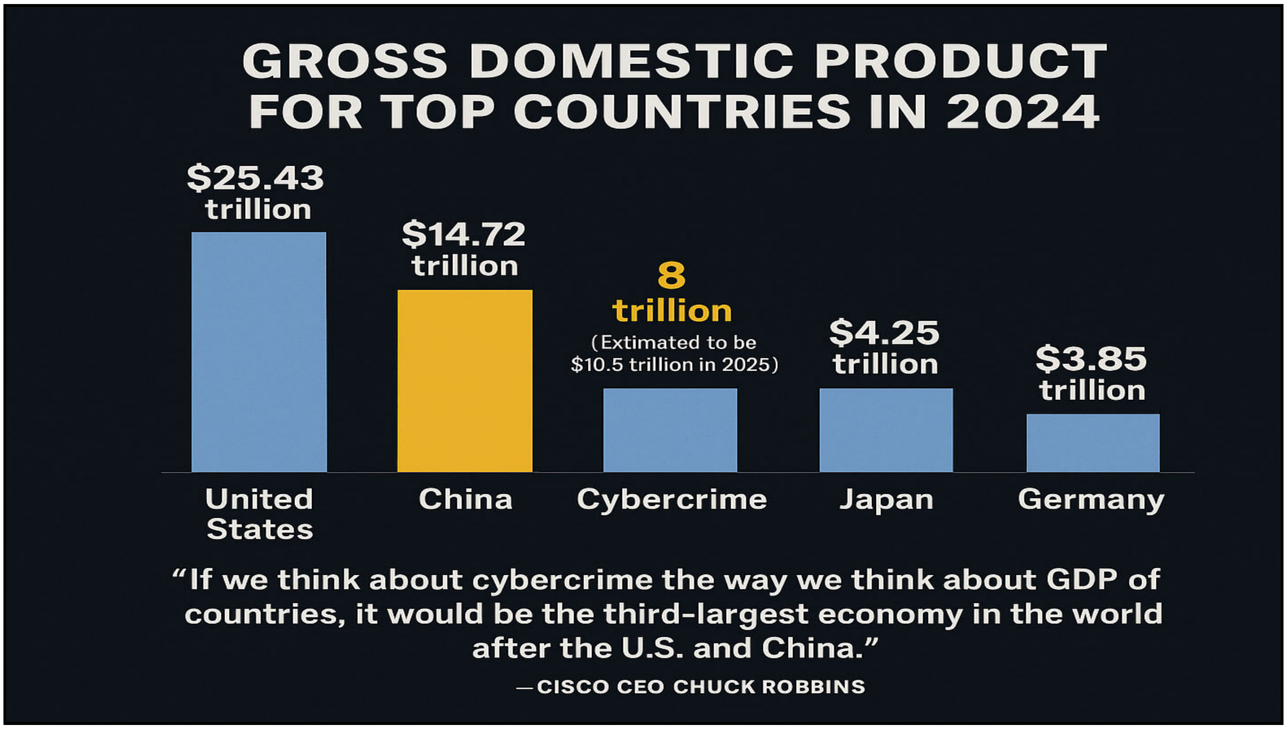


What is Cybersecurity?

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.

15



GROSS DOMESTIC PRODUCT FOR TOP COUNTRIES IN 2024

"If we think about cybercrime the way we think about GDP of countries, it would be the third-largest economy in the world after the U.S. and China."

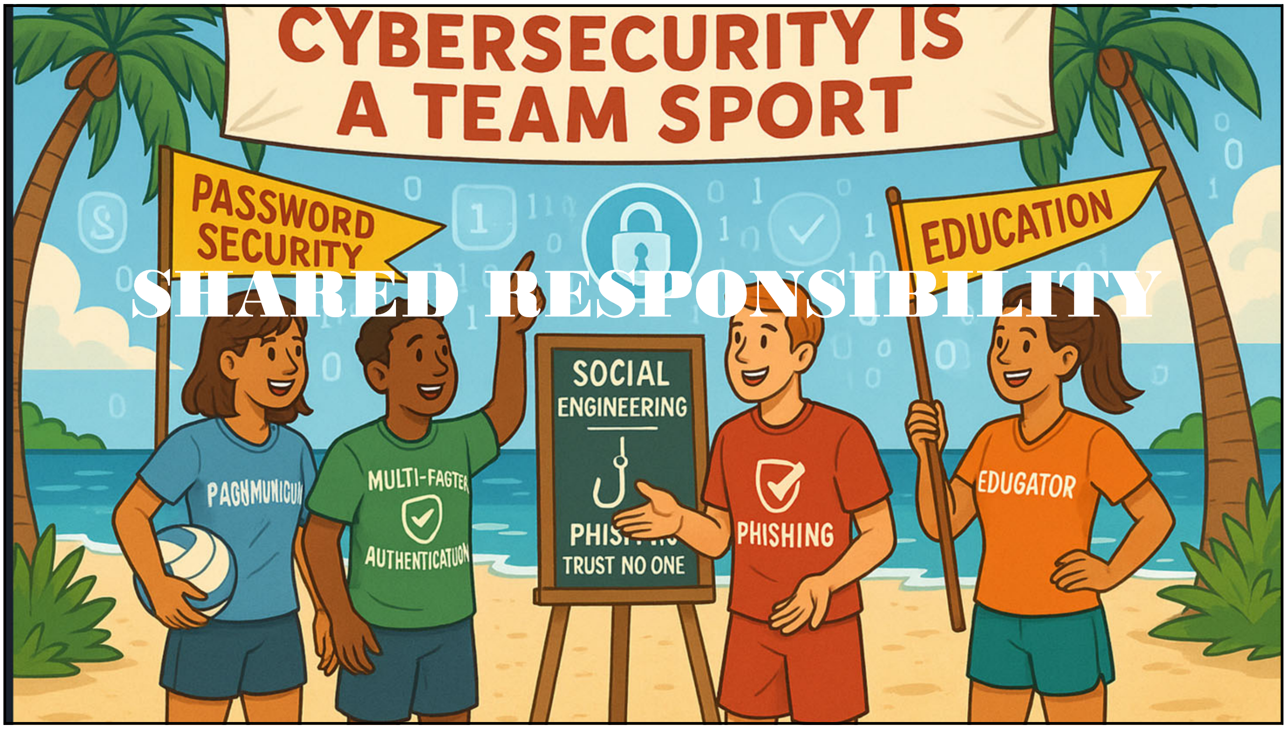
—CISCO CEO CHUCK ROBBINS

16

II. Responsibility

17

SHARED RESPONSIBILITY



18

Human error accounts for 95% of all cybersecurity breaches. The human element is the weakest link in cybersecurity.

Source: IBM Study

19

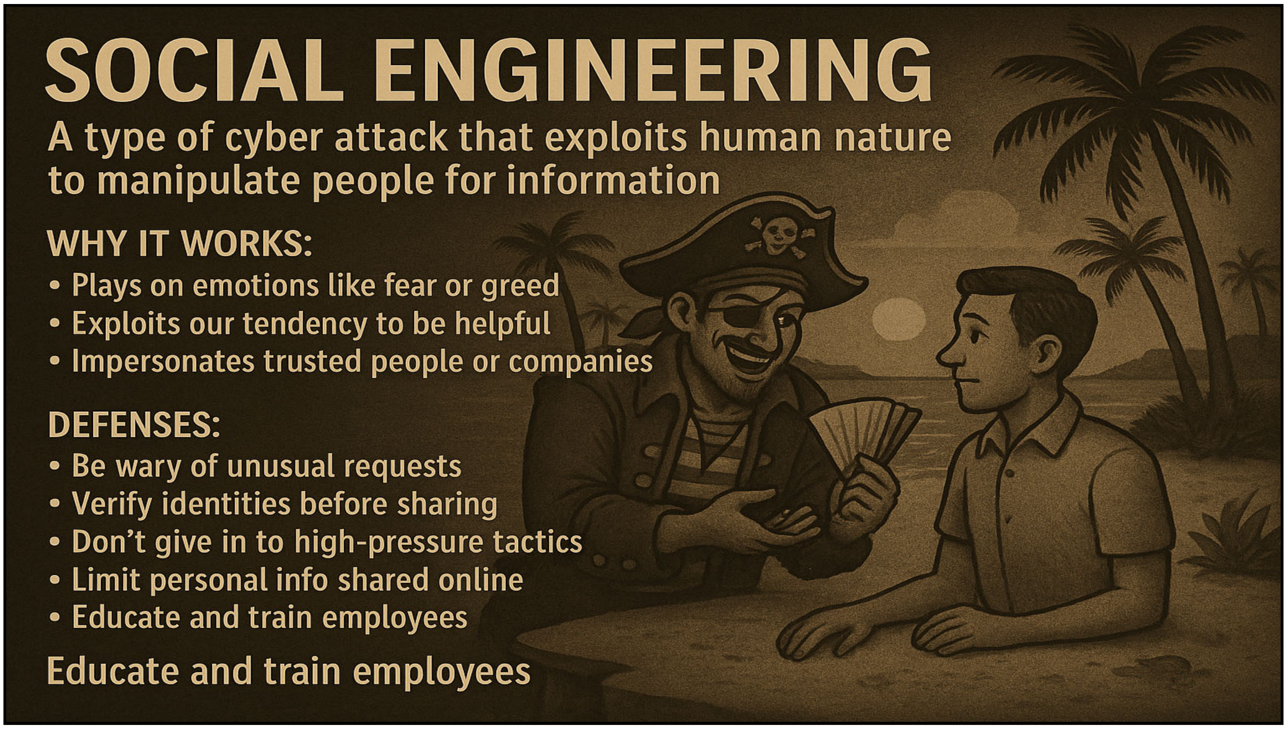
20

III. Cyber Deception and Threats

21

How people think they get hacked

22



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

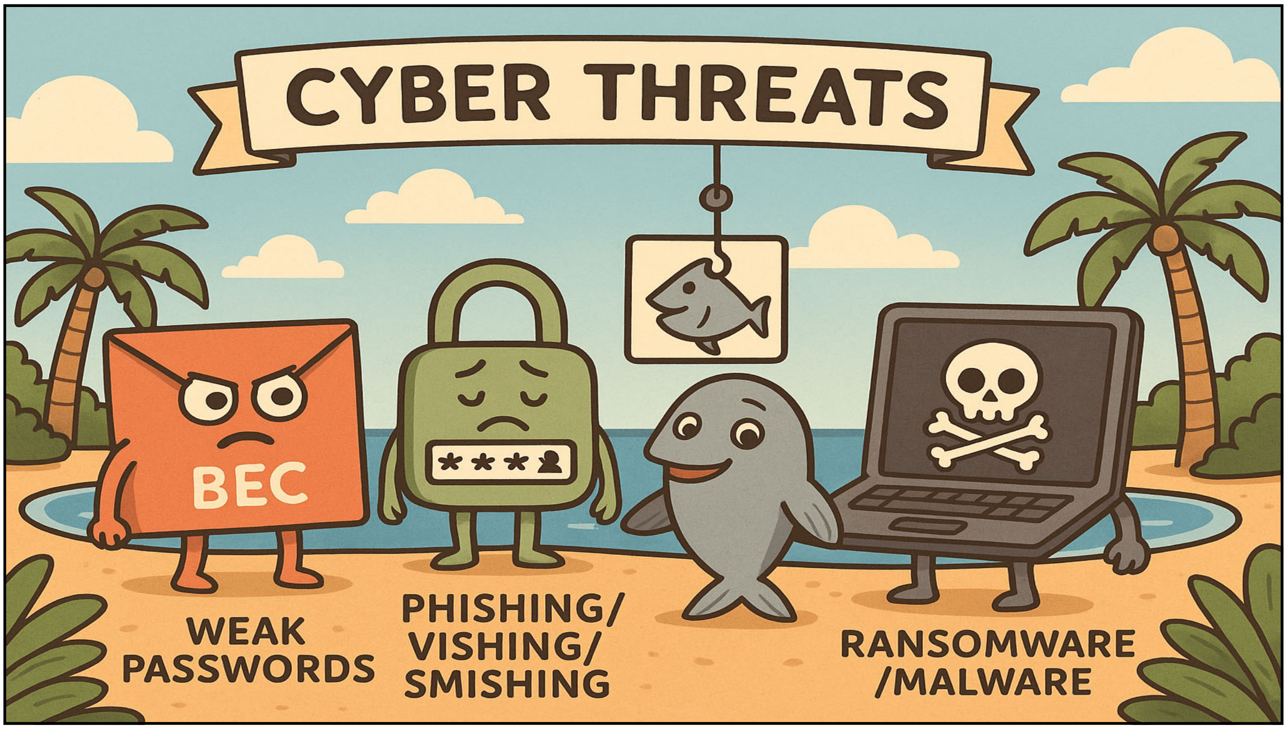
23

24

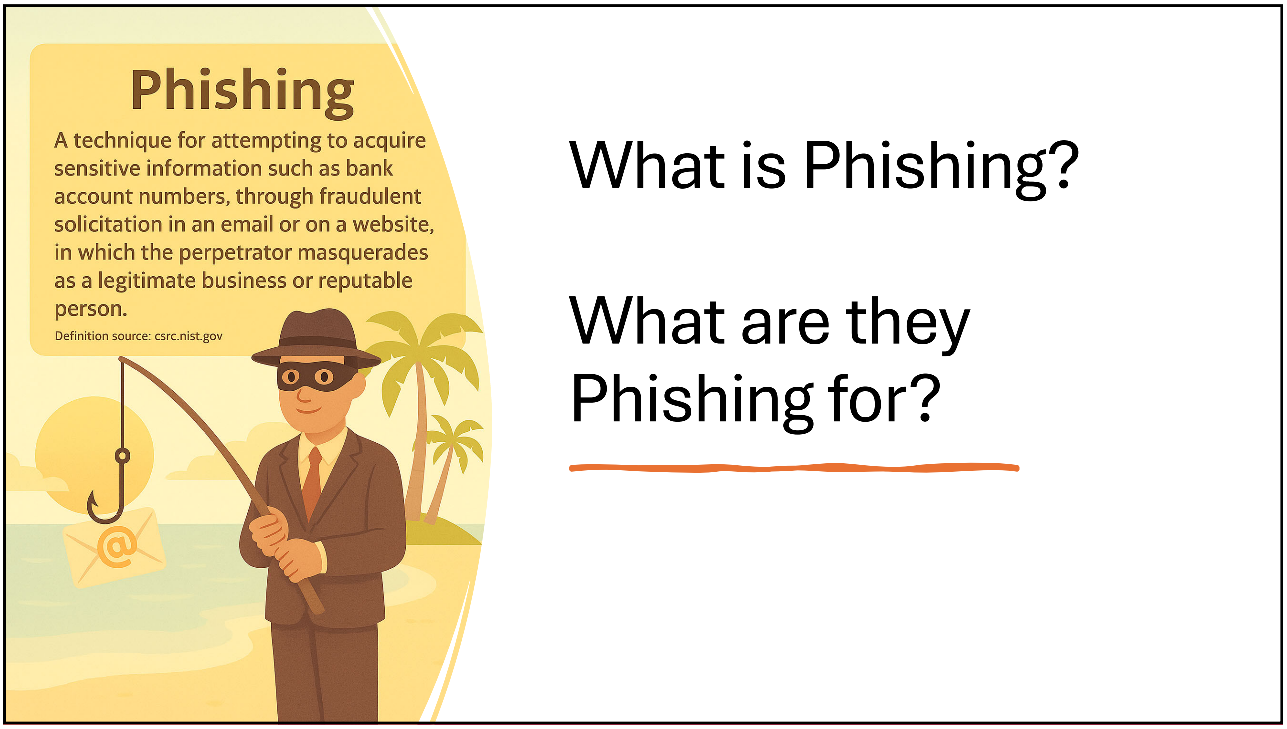
Social Engineering takes advantage of human behaviors using psychological manipulation. The user may respond due to:

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

25



26



Phishing

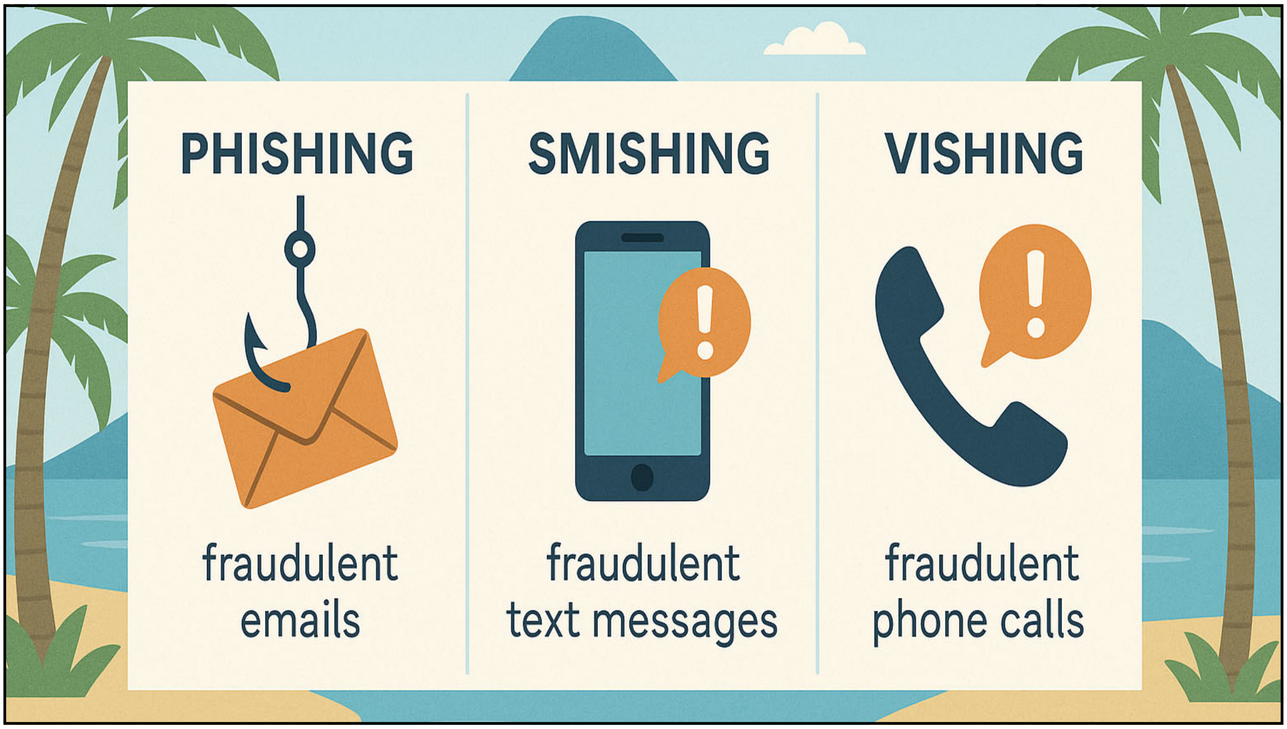
A technique for attempting to acquire sensitive information such as bank account numbers, through fraudulent solicitation in an email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

Definition source: csrc.nist.gov

What is Phishing?

What are they Phishing for?

27



PHISHING

fraudulent emails

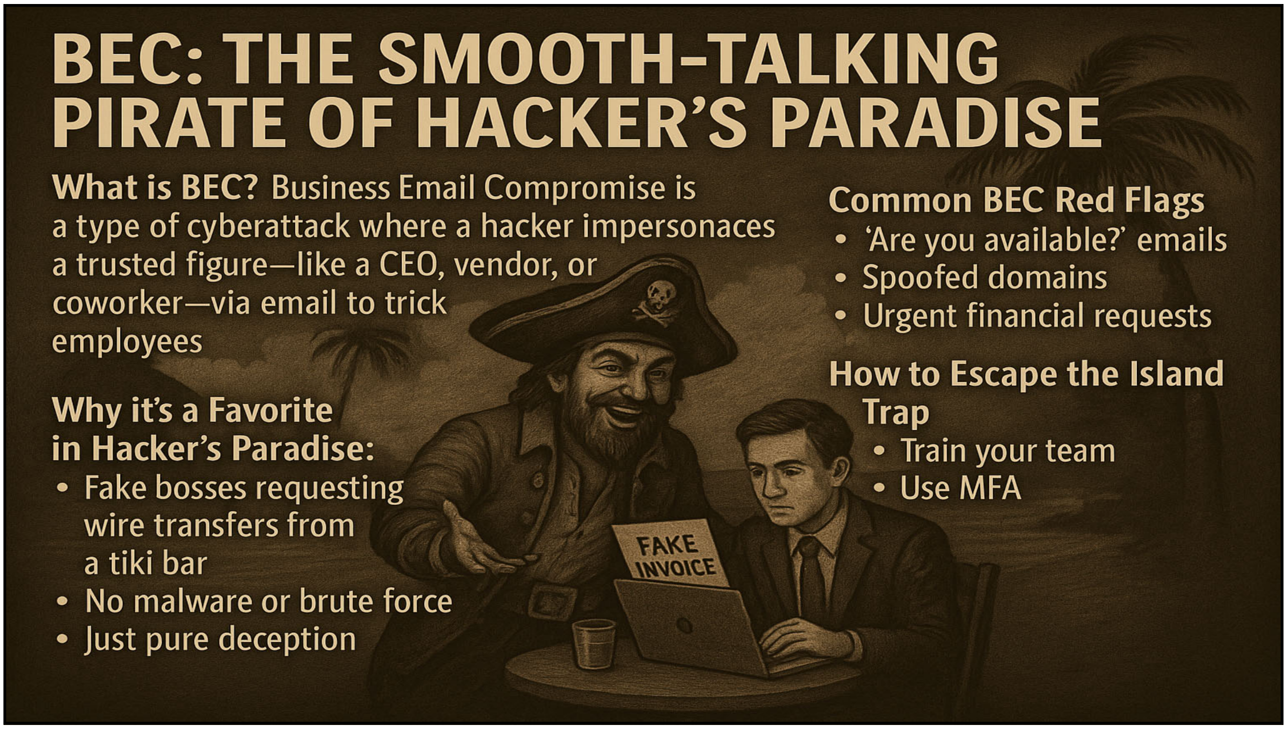
SMISHING

fraudulent text messages

VISHING

fraudulent phone calls

28



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

What is BEC? Business Email Compromise is a type of cyberattack where a hacker impersonaces 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

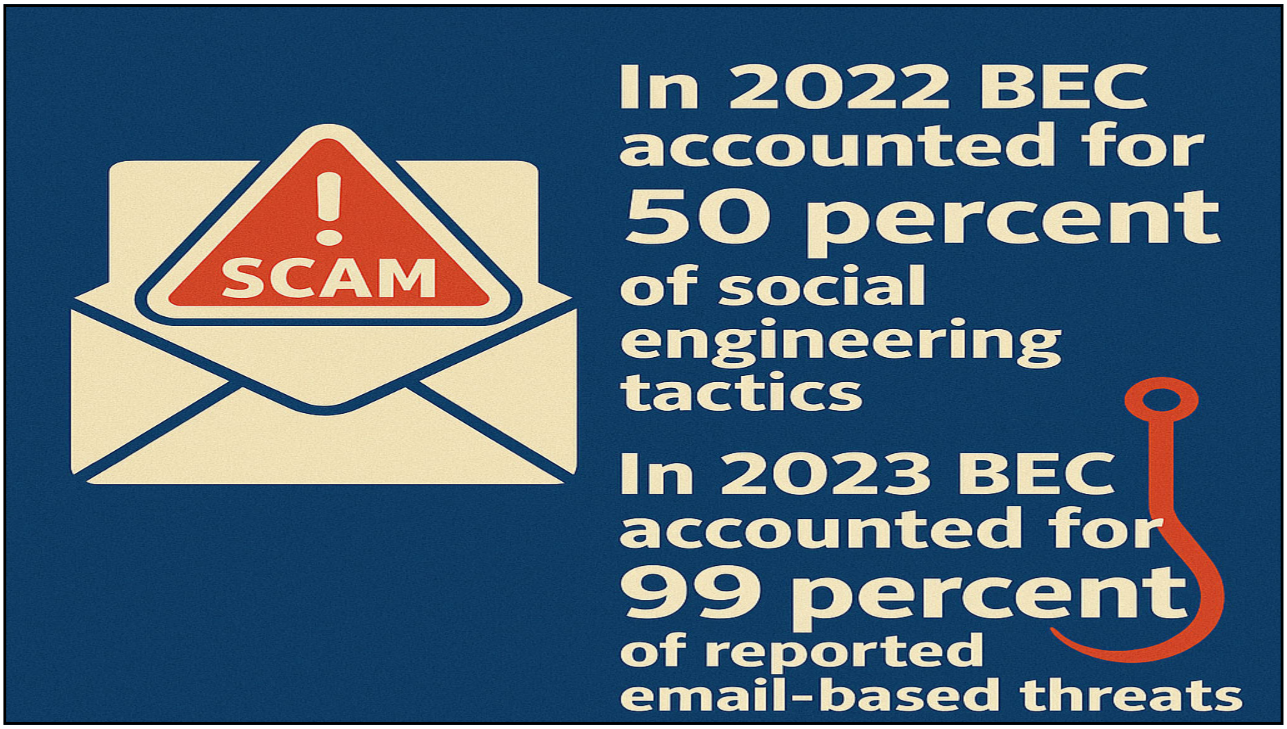
Common BEC Red Flags

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

How to Escape the Island Trap

- Train your team
- Use MFA

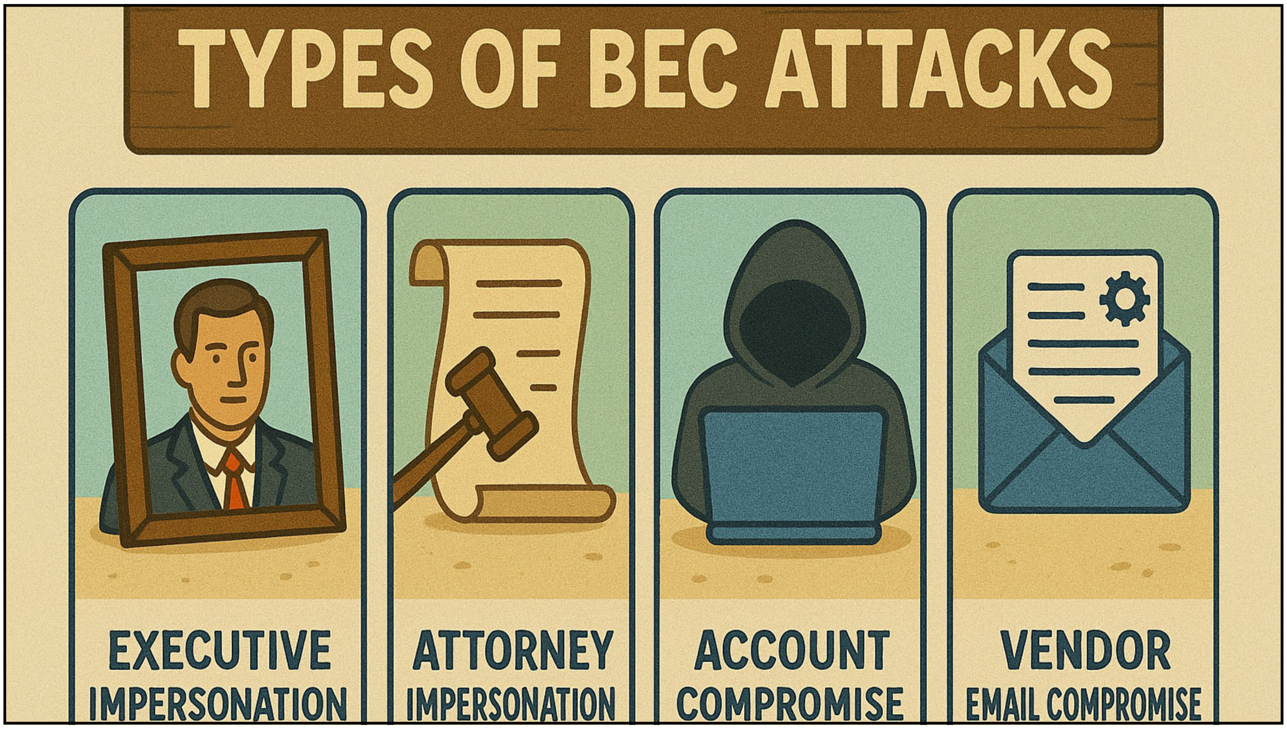
29



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

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

30



TYPES OF BEC ATTACKS

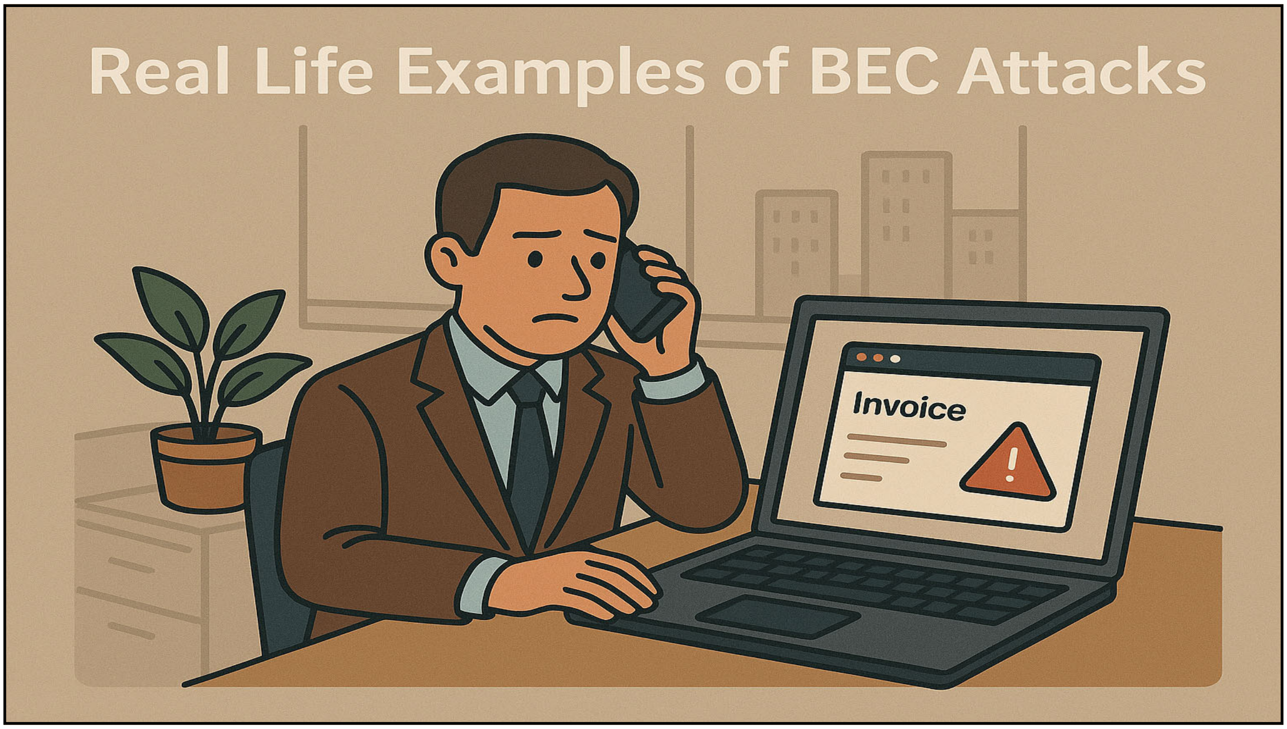
EXECUTIVE IMPERSONATION

ATTORNEY IMPERSONATION

ACCOUNT COMPROMISE

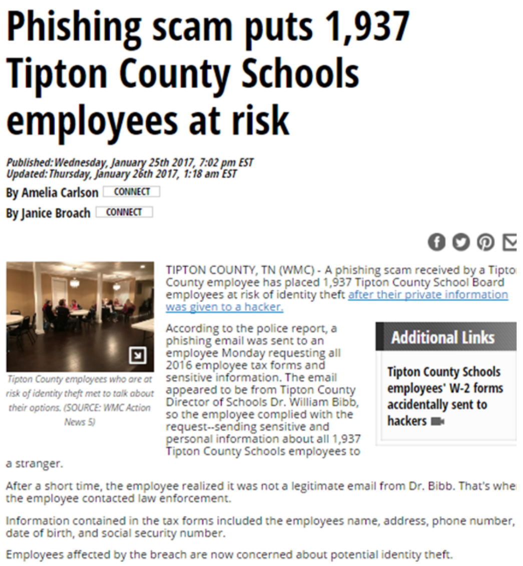
VENDOR EMAIL COMPROMISE

31



Real Life Examples of BEC Attacks

32



Phishing scam puts 1,937 Tipton County Schools employees at risk

Published: Wednesday, January 25th 2017, 7:02 pm EST
Updated: Thursday, January 26th 2017, 1:18 am EST

By Amelia Carlson CONNECT

By Janice Broach CONNECT

Tipton County employees who are at risk of identity theft met to talk about their options. (SOURCE: WMC Action News 5)

TIPTON COUNTY, TN (WMC) - A phishing scam received by a Tipto County employee has placed 1,937 Tipton County School Board employees at risk of identity theft after their private information was given to a hacker.

According to the police report, a phishing email was sent to an employee Monday requesting all 2016 employee tax forms and sensitive information. The email appeared to be from Tipton County Director of Schools Dr. William Bibb, so the employee complied with the request--sending sensitive and personal information about all 1,937 Tipton County Schools employees to a stranger.

Additional Links

Tipton County Schools employees' W-2 forms accidentally sent to hackers

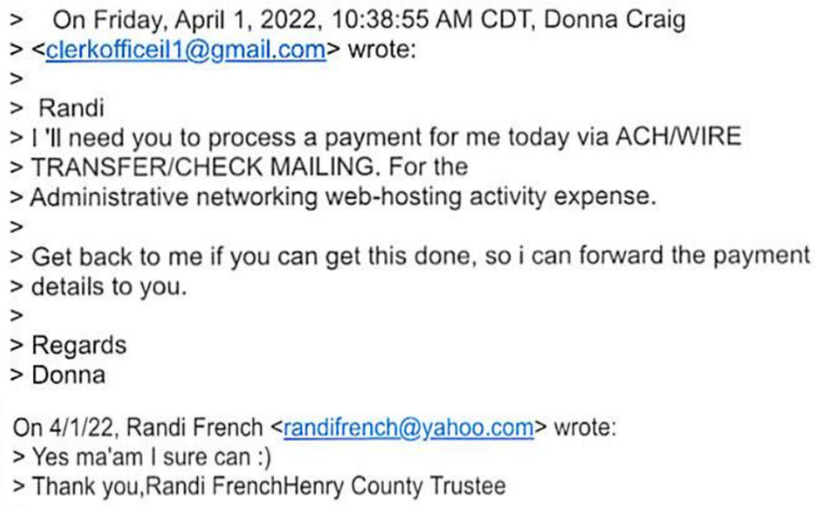
After a short time, the employee realized it was not a legitimate email from Dr. Bibb. That's whe the employee contacted law enforcement.

Information contained in the tax forms included the employees name, address, phone number, date of birth, and social security number.

Employees affected by the breach are now concerned about potential identity theft.

33

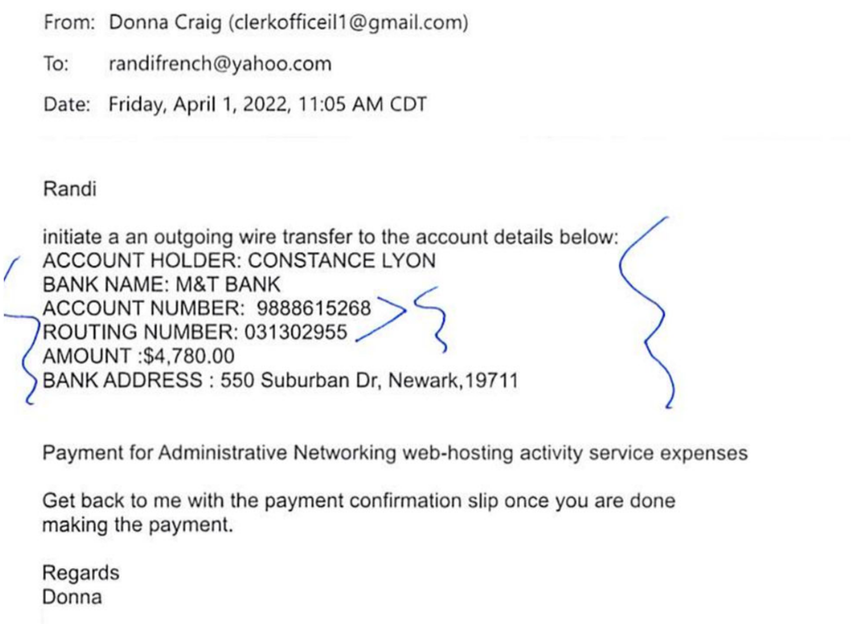
Real-World Example



> On Friday, April 1, 2022, 10:38:55 AM CDT, Donna Craig
> <clerkofficeil1@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 FrenchHenry County Trustee

34



From: Donna Craig (clerkofficeil1@gmail.com)

To: randifrench@yahoo.com

Date: Friday, April 1, 2022, 11:05 AM CDT

Randi

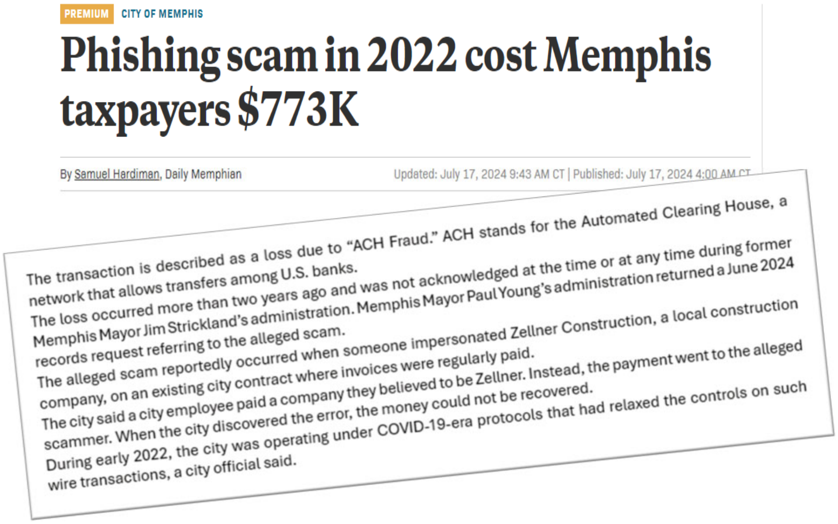
initiate a an outgoing wire transfer to the account details below:
ACCOUNT HOLDER: CONSTANCE LYON
BANK NAME: M&T BANK
ACCOUNT NUMBER: 9888615268
ROUTING NUMBER: 031302955
AMOUNT :$4,780.00
BANK ADDRESS : 550 Suburban Dr, Newark,19711

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

35



PREMIUM CITY OF MEMPHIS

Phishing scam in 2022 cost Memphis taxpayers $773K

By Samuel Hardiman, Daily Memphian

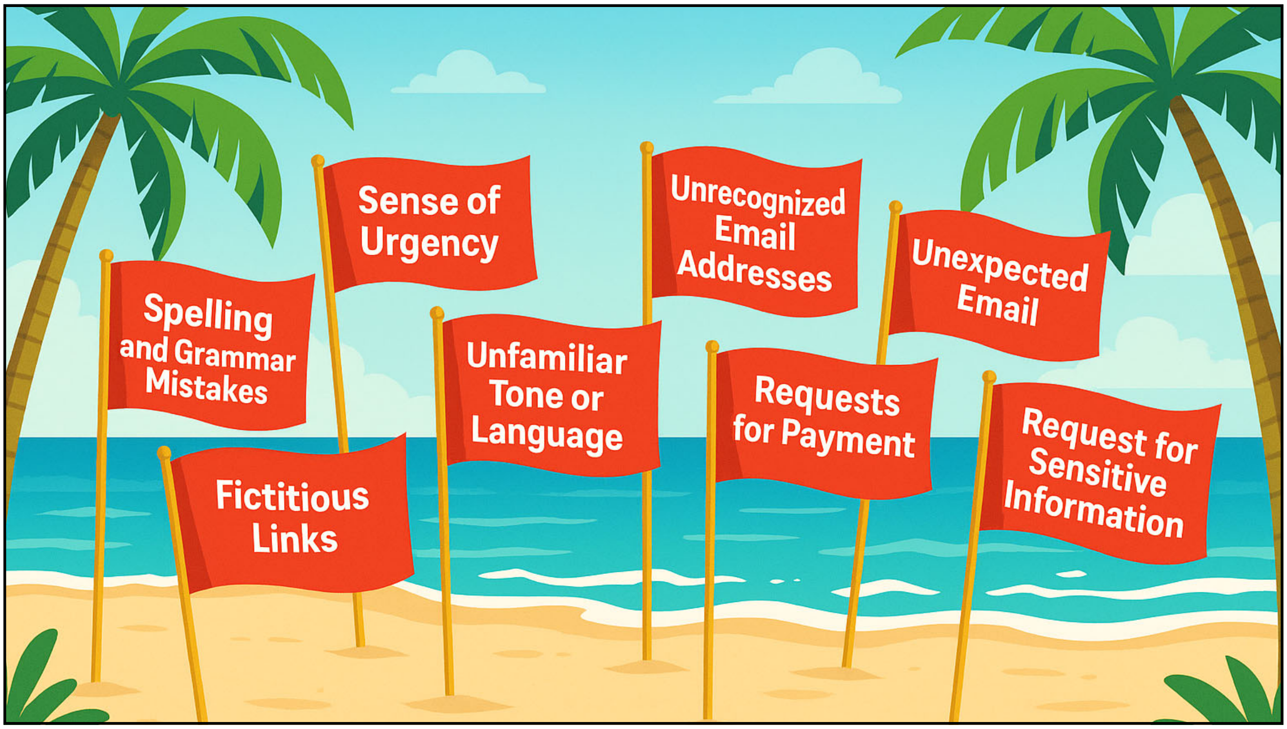
Updated: July 17, 2024 9:43 AM CT | Published: July 17, 2024 4:00 AM CT

The transaction is described as a loss due to "ACH Fraud." ACH stands for the Automated Clearing House, a network that allows transfers among U.S. banks.
The loss occurred more than two years ago and was not acknowledged at the time or at any time during former Memphis Mayor Jim Strickland's administration. Memphis Mayor Paul Young's administration returned a June 2024 records request referring to the alleged scam.
The alleged scam reportedly occurred when someone impersonated Zellner Construction, a local construction company, on an existing city contract where invoices were regularly paid.
The city said a city employee paid a company they believed to be Zellner. Instead, the payment went to the alleged scammer. When the city discovered the error, the money could not be recovered.
During early 2022, the city was operating under COVID-19-era protocols that had relaxed the controls on such wire transactions, a city official said.

36

- In 2020, Rutherford County, 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 million for the county.

37

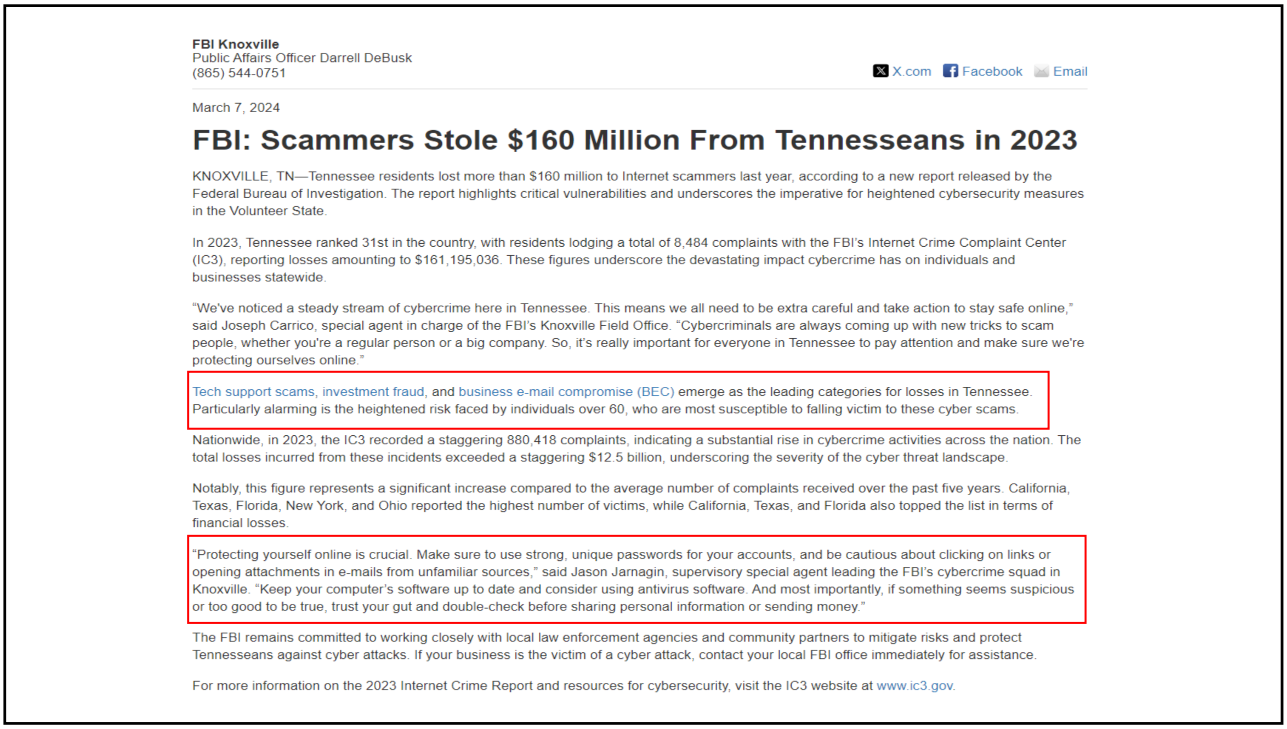

Spelling and Grammar Mistakes
Sense of Urgency
Fictitious Links
Unfamiliar Tone or Language
Unrecognized Email Addresses
Requests for Payment
Unexpected Email
Request for Sensitive Information

38

Impact of Business Email Compromise

Financial Loss from theft
Reputational Damage
Lack of public trust
Legal and Regulatory Penalties and Fines
for non-compliance
Operational Disruptions
Costs related to investigation and remediation

39



FBI Knoxville
Public Affairs Officer Darrell DeBusk
(865) 544-0751

X.com Facebook Email

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 $161,195,036. 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 Carrico, 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."

Tech support scams, investment fraud, and business e-mail compromise (BEC) emerge 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.

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 $12.5 billion, underscoring the severity of the cyber threat landscape.

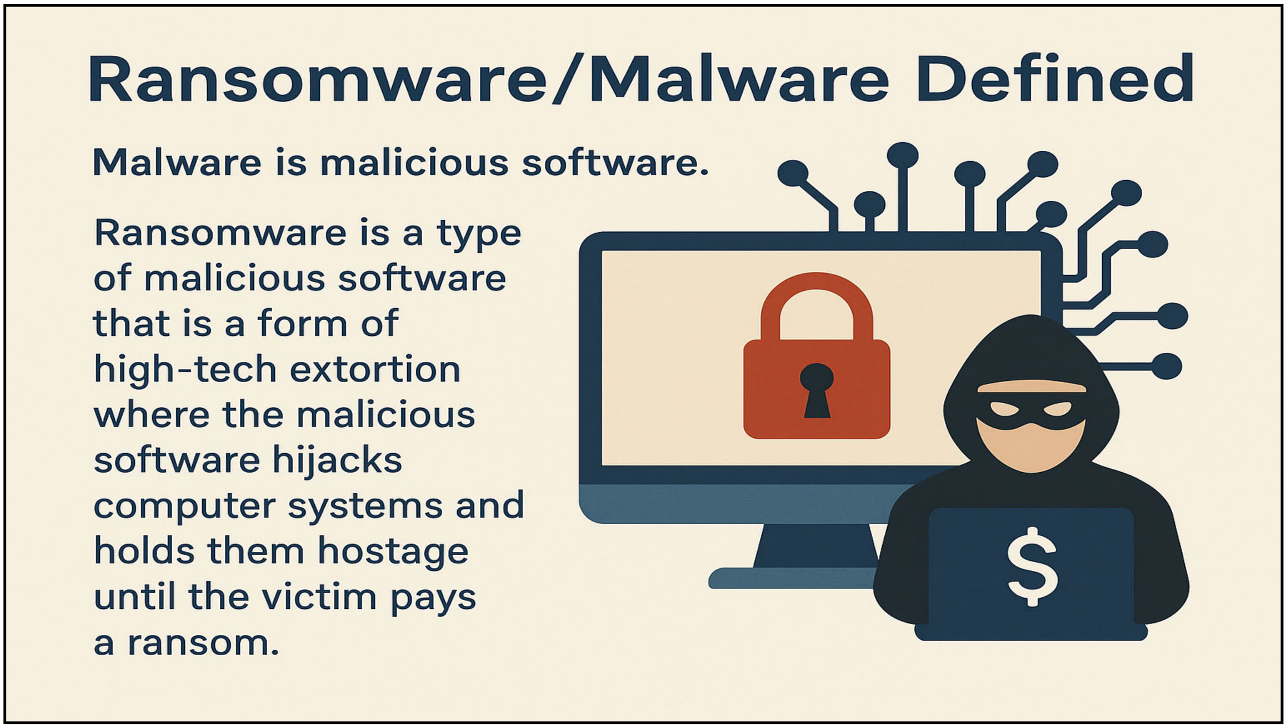
Notably, this figure represents a significant increase compared to the average number of complaints received over the past five years. California, Texas, Florida, New York, and Ohio reported the highest number of victims, while California, Texas, and Florida also topped the list in terms of financial 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 e-mails from unfamiliar sources," said Jason Jarnagin, 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 Tennesseans 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.

40

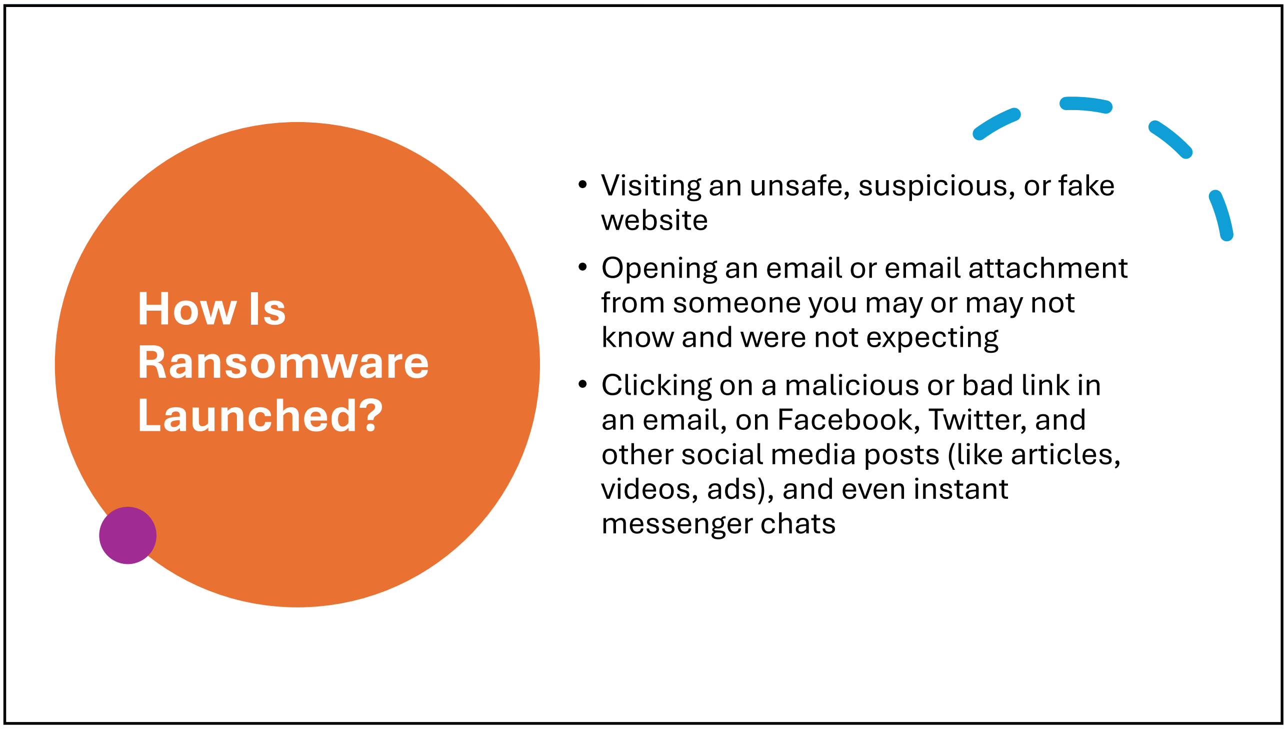


Ransomware/Malware Defined

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.

41



How Is Ransomware Launched?

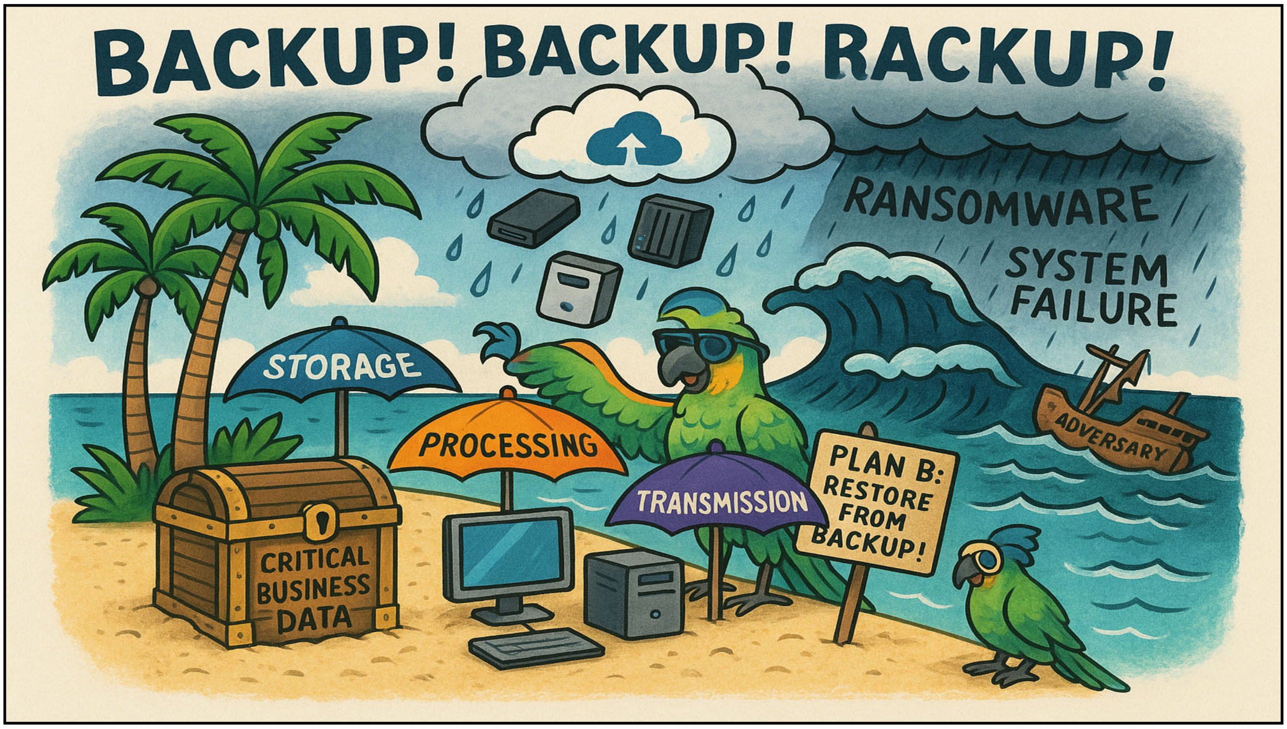
- Visiting an unsafe, suspicious, or fake website
- Opening an email or email attachment from someone you may or may not know and were not expecting
- Clicking on a malicious or bad link in an email, on Facebook, Twitter, and other social media posts (like articles, videos, ads), and even instant messenger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

42

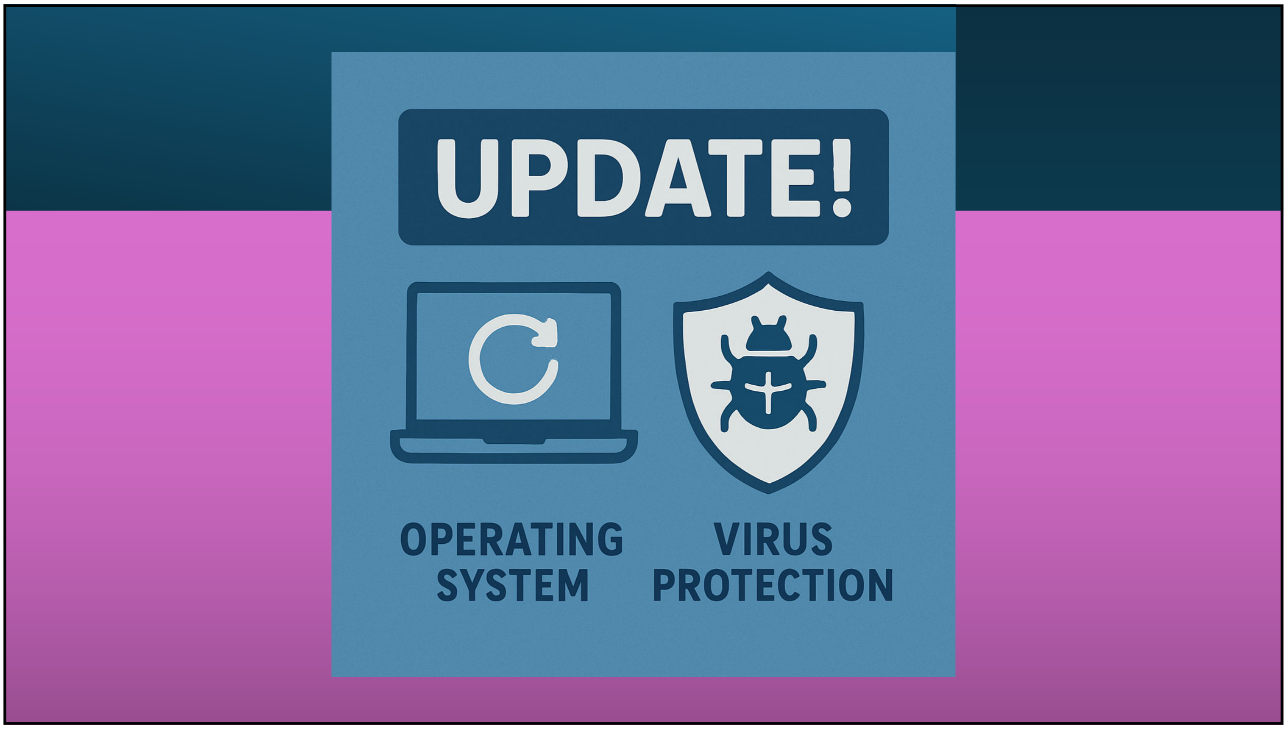
43

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

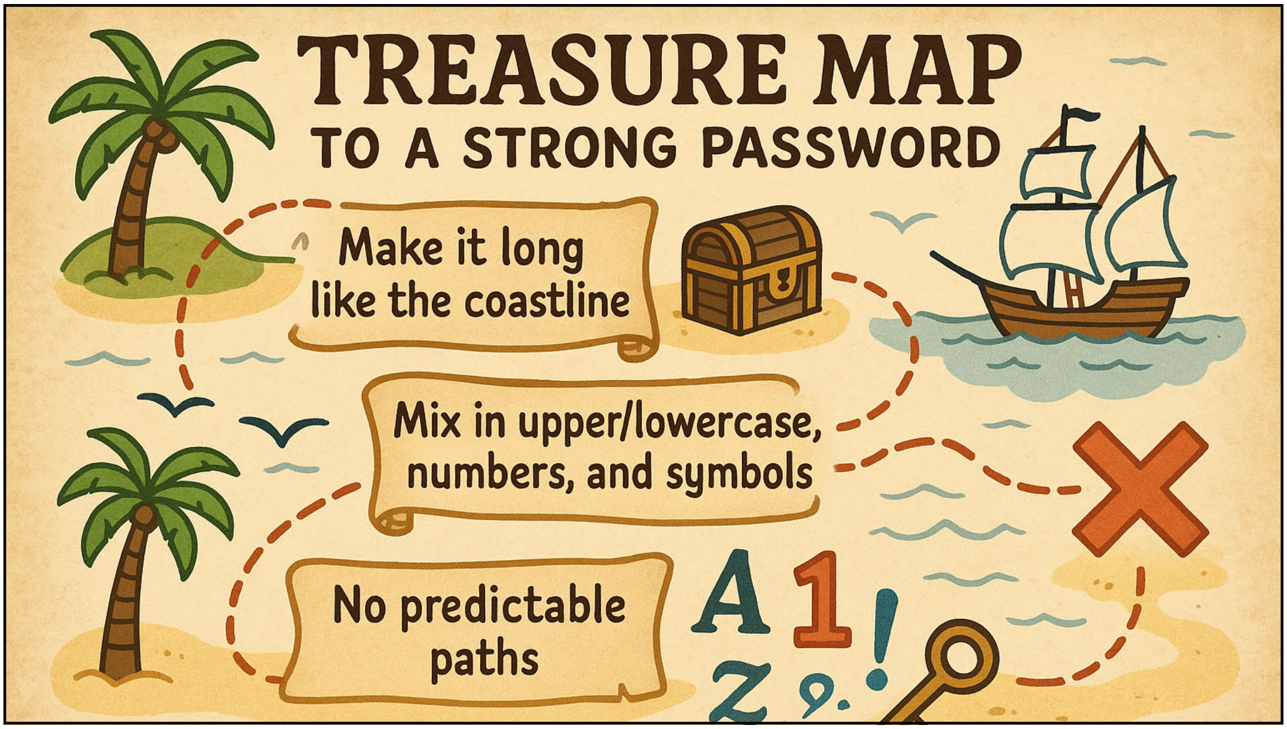
44


BACKUP! BACKUP! RACKUP!
RANSOMWARE
SYSTEM FAILURE
STORAGE
PROCESSING
TRANSMISSION
PLAN B: RESTORE FROM BACKUP!
ADVERSARY
CRITICAL BUSINESS DATA

45


UPDATE!
OPERATING SYSTEM
VIRUS PROTECTION

46



TREASURE MAP

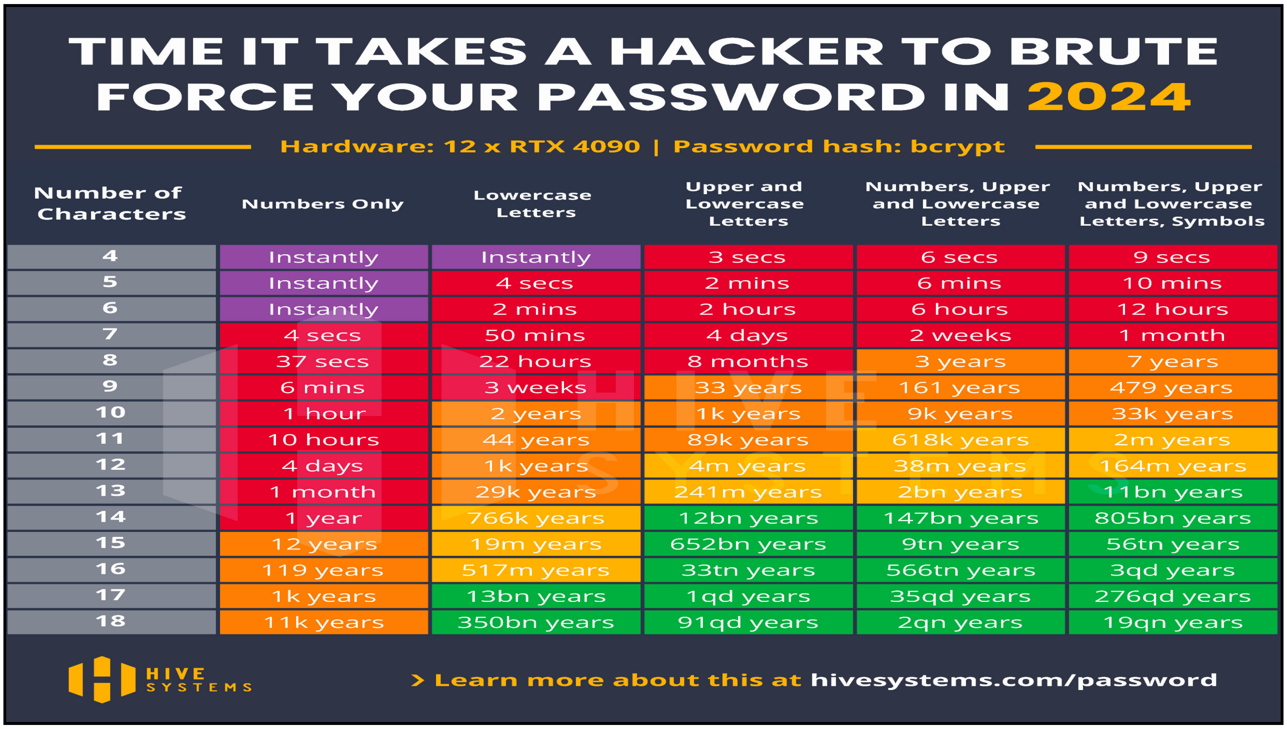
TO A STRONG PASSWORD

Make it long like the coastline

Mix in upper/lowercase, numbers, and symbols

No predictable paths

47



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

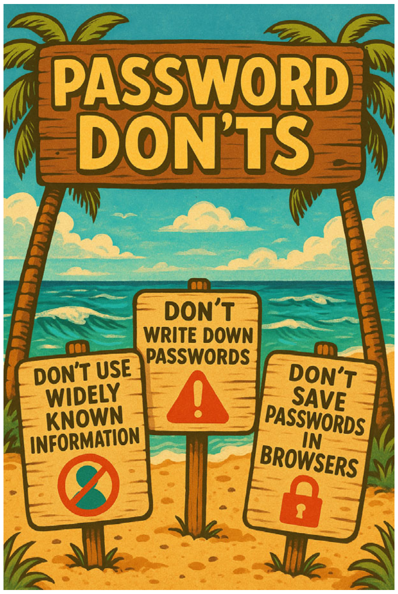
Hardware: 12 x RTX 4090 | Password hash: bcrypt

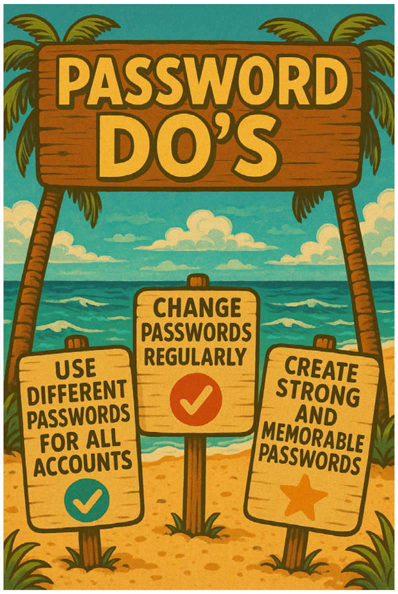
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 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	38m years	164m 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	9tn years	56tn years
16	119 years	517m years	33tn years	566tn 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

48


PASSWORD DON'TS
DON'T USE WIDELY KNOWN INFORMATION
DON'T WRITE DOWN PASSWORDS
DON'T SAVE PASSWORDS IN BROWSERS

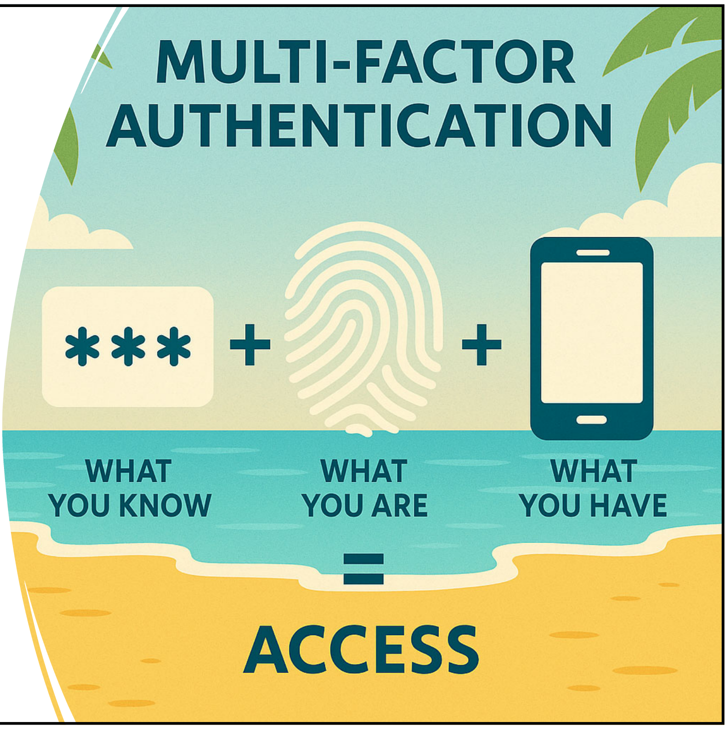

PASSWORD DO'S
USE DIFFERENT PASSWORDS FOR ALL ACCOUNTS
CHANGE PASSWORDS REGULARLY
CREATE STRONG AND MEMORABLE PASSWORDS

49

What you know – Password or Pin

What you are – Your fingerprint, voice recognition, or some other biometric, such as face ID

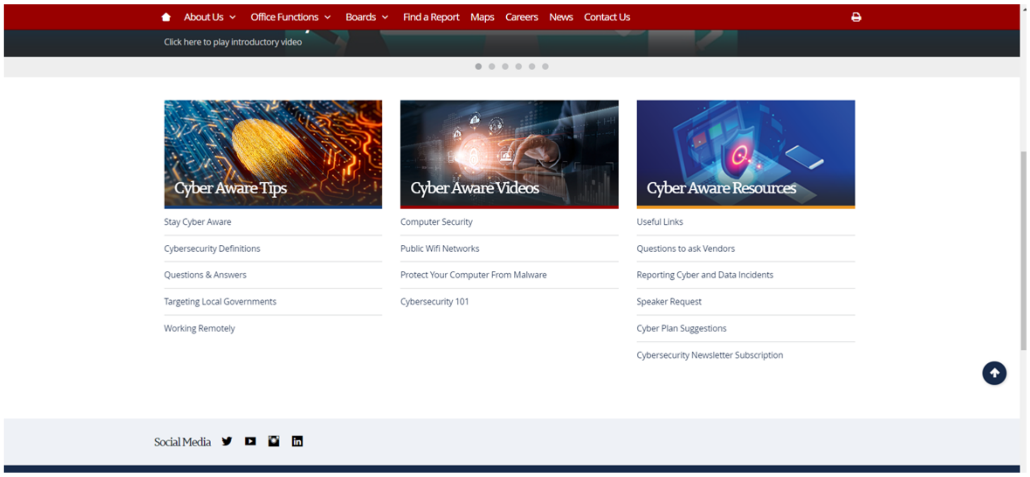
What you have – Access badge



50

51

TNCOT.CC/CYBERAWARE



Cyber Aware Tips

- Stay Cyber Aware
- Cybersecurity Definitions
- Questions & Answers
- Targeting Local Governments
- Working Remotely

Cyber Aware Videos

- Computer Security
- Public Wifi Networks
- Protect Your Computer From Malware
- Cybersecurity 101

Cyber Aware Resources

- Useful Links
- Questions to ask Vendors
- Reporting Cyber and Data Incidents
- Speaker Request
- Cyber Plan Suggestions
- Cybersecurity Newsletter Subscription

52

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.

53

Questions?

Twyla Pratt, CISA, CCFO

Twyla.Pratt@cot.tn.gov

615 – 747 - 8853

tn.cot.cc/cyberaware

54