"Hackers Paradise," The Fantasy Island of Cyber Deception, Threats, and Nightmares

Barbara Shults

Legislative IS Auditor

Division of Local Government Audit

May 9, 2025

Meet My People

About Us

Jason Mumpower

Jim Arnette

THE BOSSES

Nathan Abbott

Elisha Crowell

Twyla Smith

Rachel DePriest

Bethany Graves

Chrisvonta Smith

Jeni Paladeni

Barbara Shults

Emma Hayse

Shania Leonard

Julie Davis-Shelton

TENNESSEE COMPTROLLER OF THE TREASURY

Division of Local Government Audit

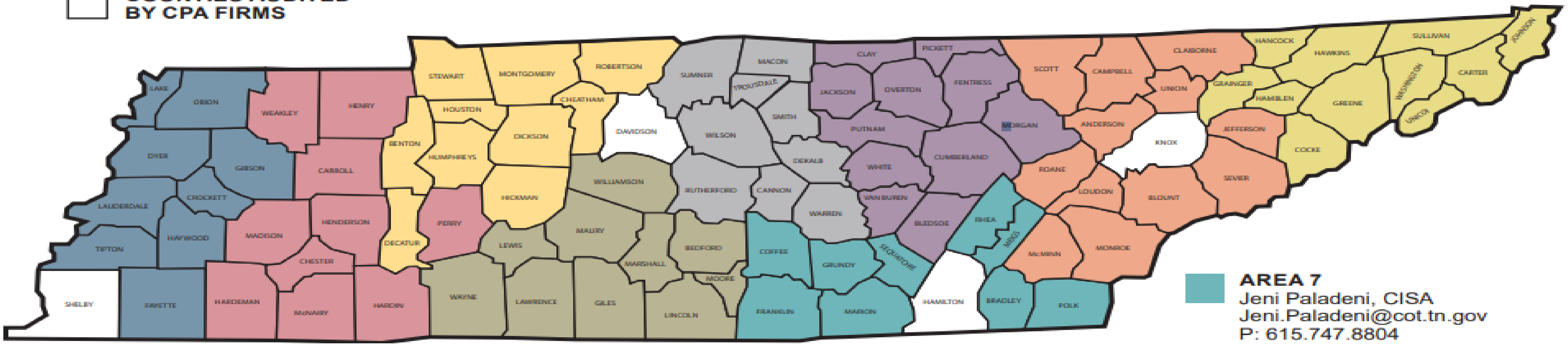
IS AUDIT ASSIGNMENTS

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 Smith, CISA
Twyla.Smith@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

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.

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

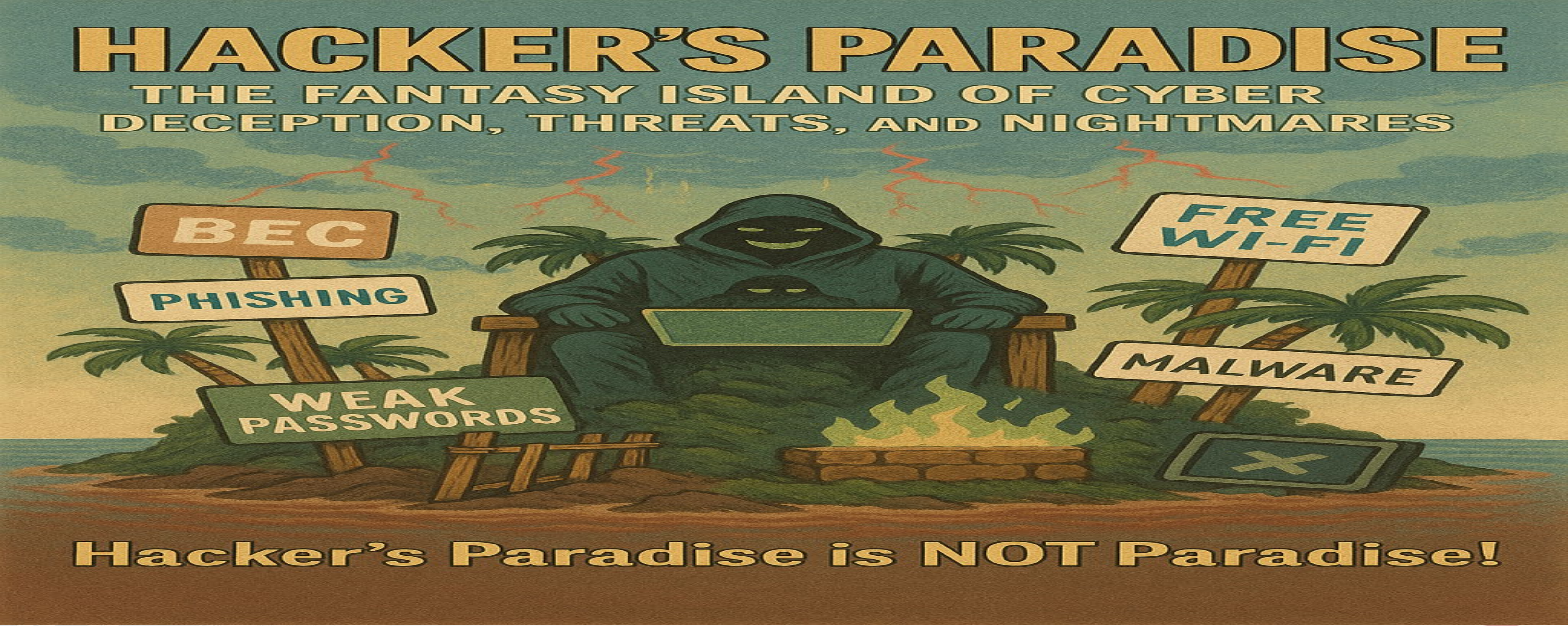
. IV. Rules of Protection

a. Cybersecurity Training

b. Create Strong Passwords

c. Multifactor Authentication

V. Conclusion/Questions


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!

🌴 Fantasy Island vs. Hacker’s Paradise 🌴

Don’t Be a Tourist
In
Hacker’s Paradise.

Feature	**Fantasy Island**	**Hacker’s Paradise**
Welcome Message	“Your dreams come true here.”	“Your worst digital nightmares start here.”
Main Attraction	Magical wish fulfillment.	Exploiting your digital desires (free Wi-Fi, too-good-to-be-true deals).
Guests	Tourists looking for fantasy experiences.	Hackers, scammers, cybercriminals looking for low-hanging fruit.
Hotel Wi-Fi	Just convenient.	Public and unsecured—ripe for **man-in-the-middle attacks**.
Key Souvenirs	Photos, memories.	**User credentials**, **bank logins**, **sensitive emails**.
Tour Guides	Charming and helpful.	**Social engineers** posing as tech support, HR, or even friends.
Entertainment	Adventure, romance, and mystery.	**Phishing emails**, **vishing calls**, **smishing texts** all disguised as urgent or enticing.
Theme Nights	Masquerade Ball.	**BEC Attacks** (Business Email Compromise) where hackers pretend to be your boss.
Hidden Traps	Cursed relics or strange island magic.	**Weak passwords**, **unpatched IoT devices**, and **default router settings**.
Natural Disasters	Sudden tropical storms.	**Ransomware attacks** that lock up your files and demand Bitcoin.
Exit Plan	Return flight home.	No easy way out without **backups**, **cyber hygiene**, and **incident response plans**.

“Hacker’s Paradise”

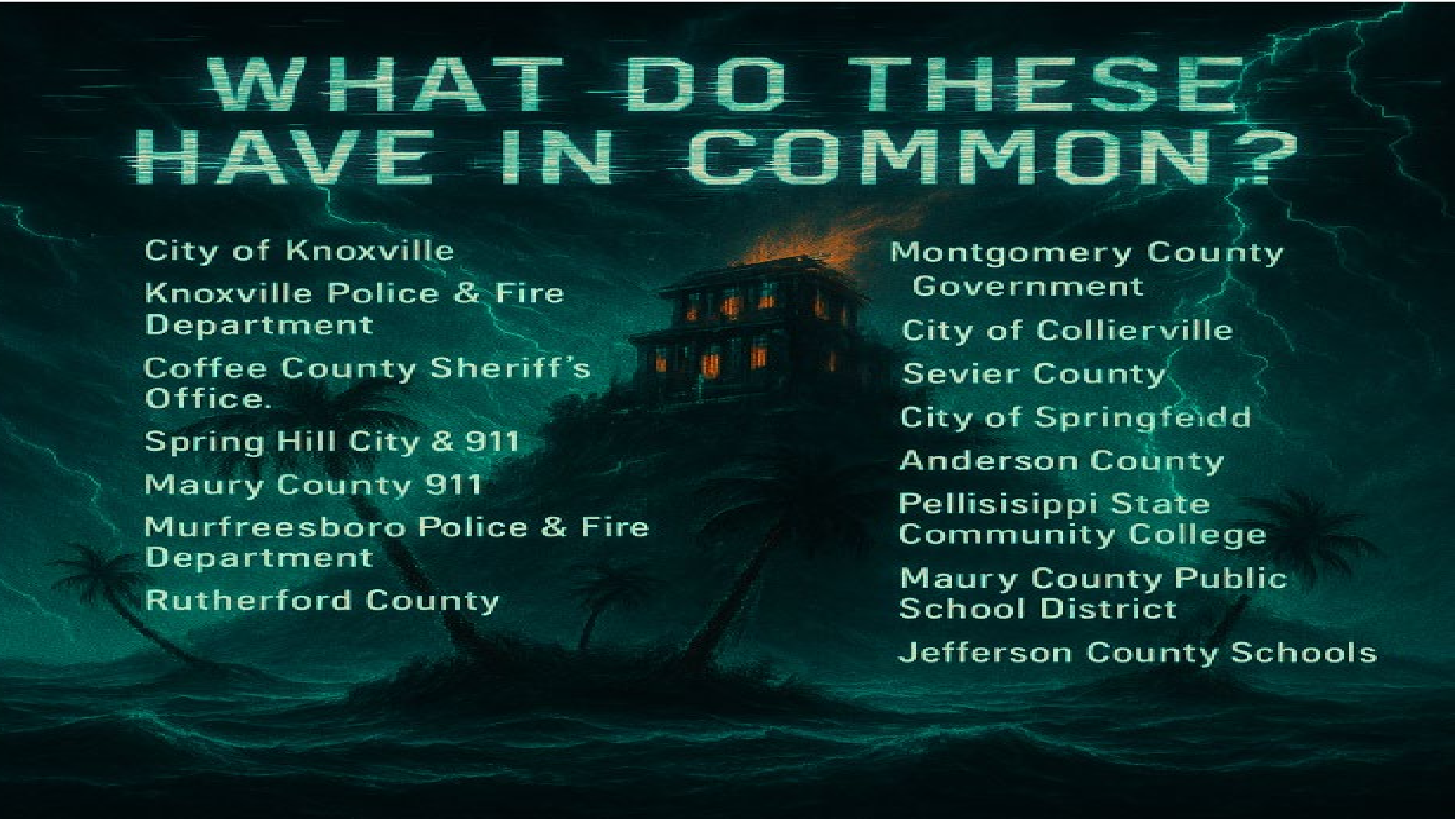
NOT A VACATION HAVEN
Paradise is NOT Paradise!
Don’t be a tourist.

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.

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

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 Springfeidd
- Anderson County
- Pellisisippi State Community College
- Maury County Public School District
- Jefferson County Schools

I. DEFINE CYBERSECURITY

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.

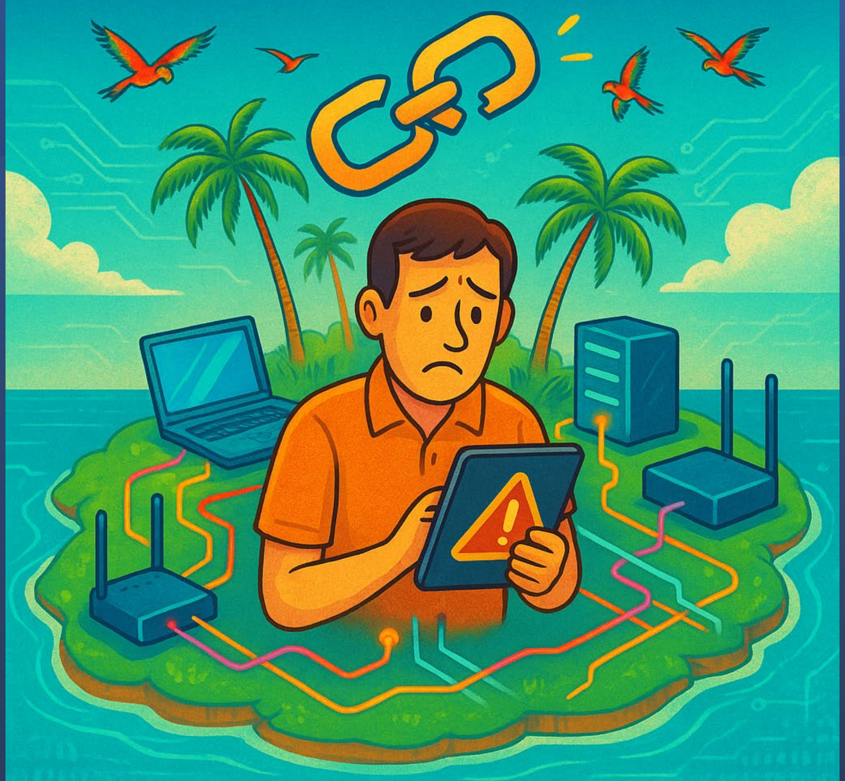
CIA TRIAD
CONFIDENTIALITY
INTEGRITY
AVAILABILITY

II. RESPONSIBILITY

SHARED RESPONSIBILITY

KEEP THE ISLAND SAFE!!!

WEAKEST LINK



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

Source: IBM Study

Who is at risk of a cyber-attack?

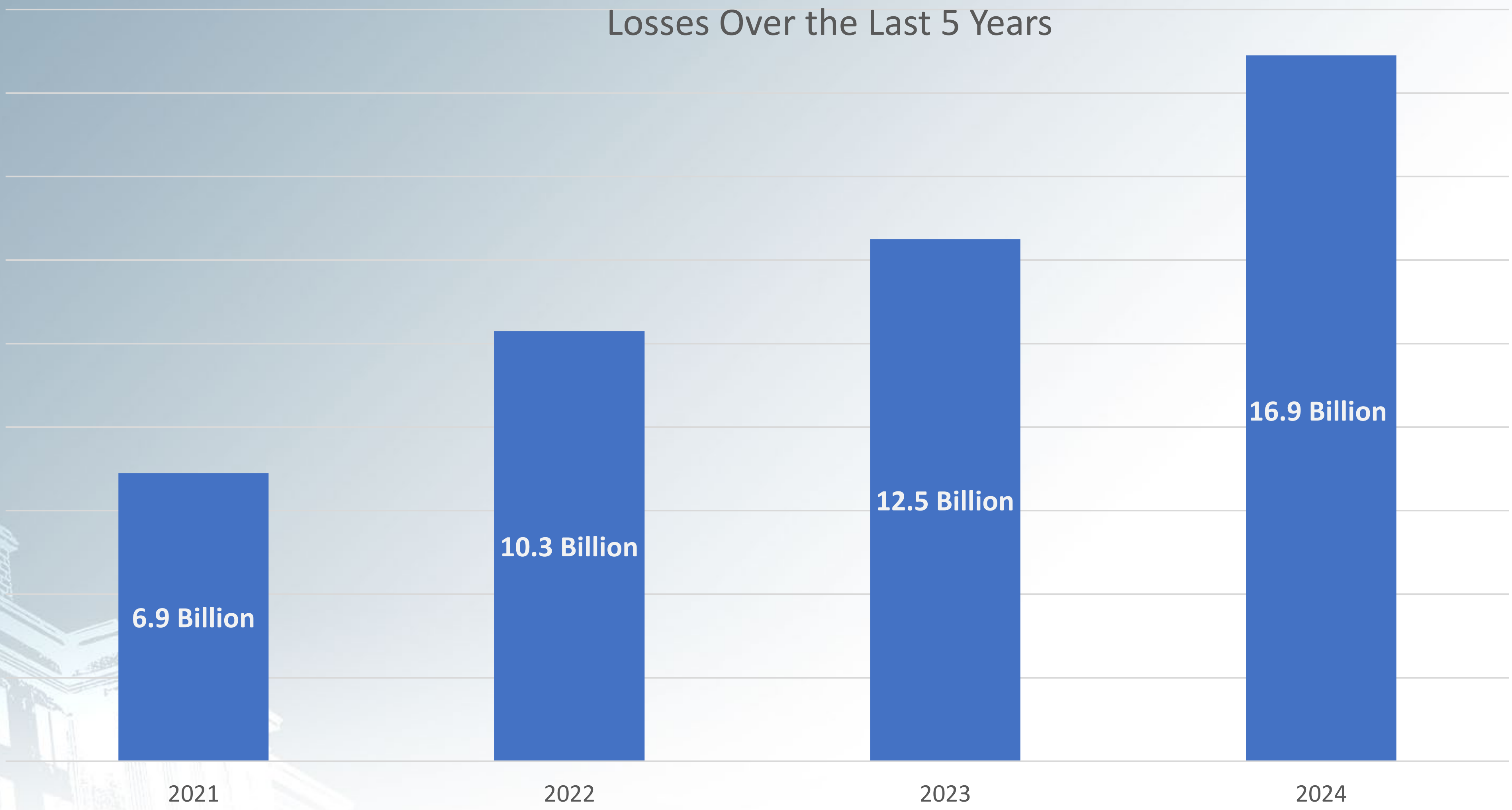
00:39
EVERY
39
SECONDS

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

Cisco CEO
Chuck Robbins

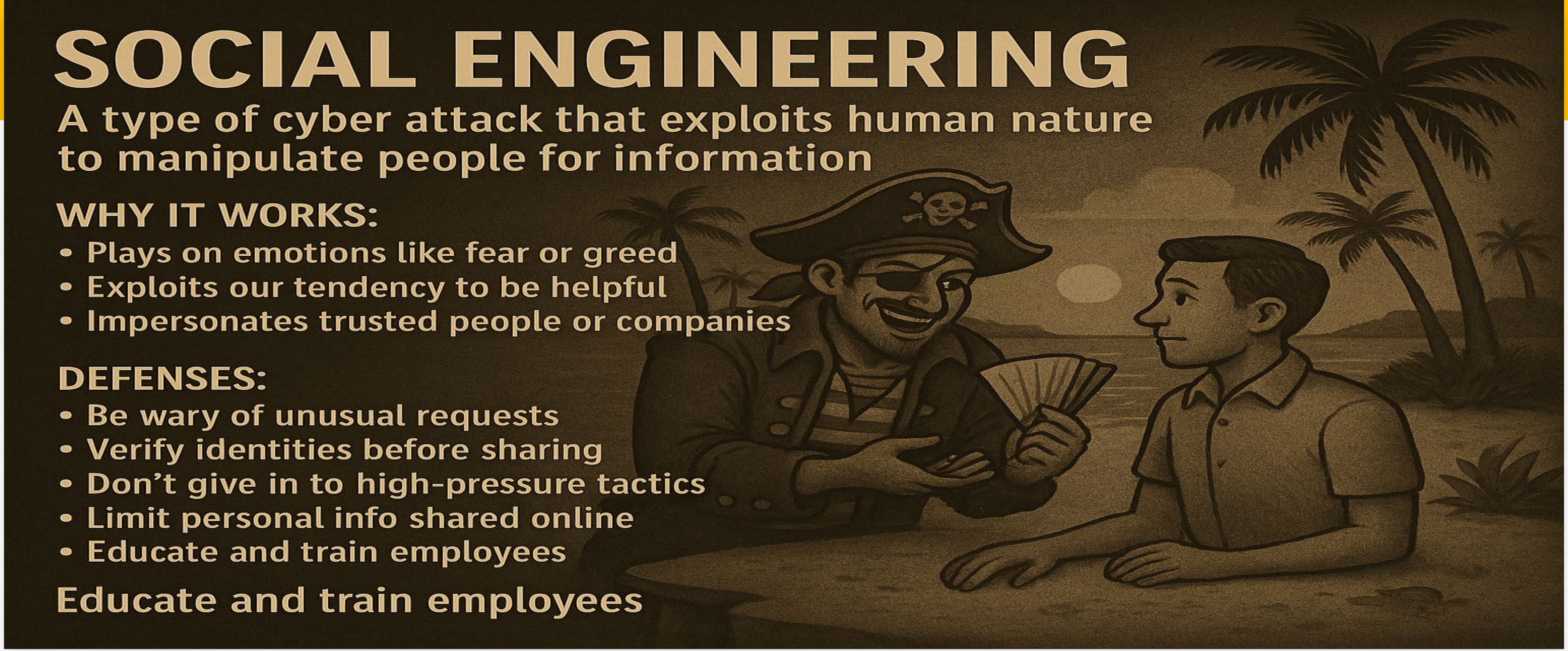
GROSS DOMESTIC PRODUCT-TOP COUNTRIES 2024

1. United States $25.43 trillion
2. China $14.72 trillion
3. . Cybercrimes $8 trillion-2023 (Estimated to be $9.5 trillion 2024)
4. Japan $4.25 trillion
5. Germany $3.85 trillion


Losses Over the Last 5 Years
6.9 Billion
10.3 Billion
12.5 Billion
16.9 Billion
2021
2022
2023
2024

Cyber Deception/ Threats/Nightmares

How People Think They Get Hacked!



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:

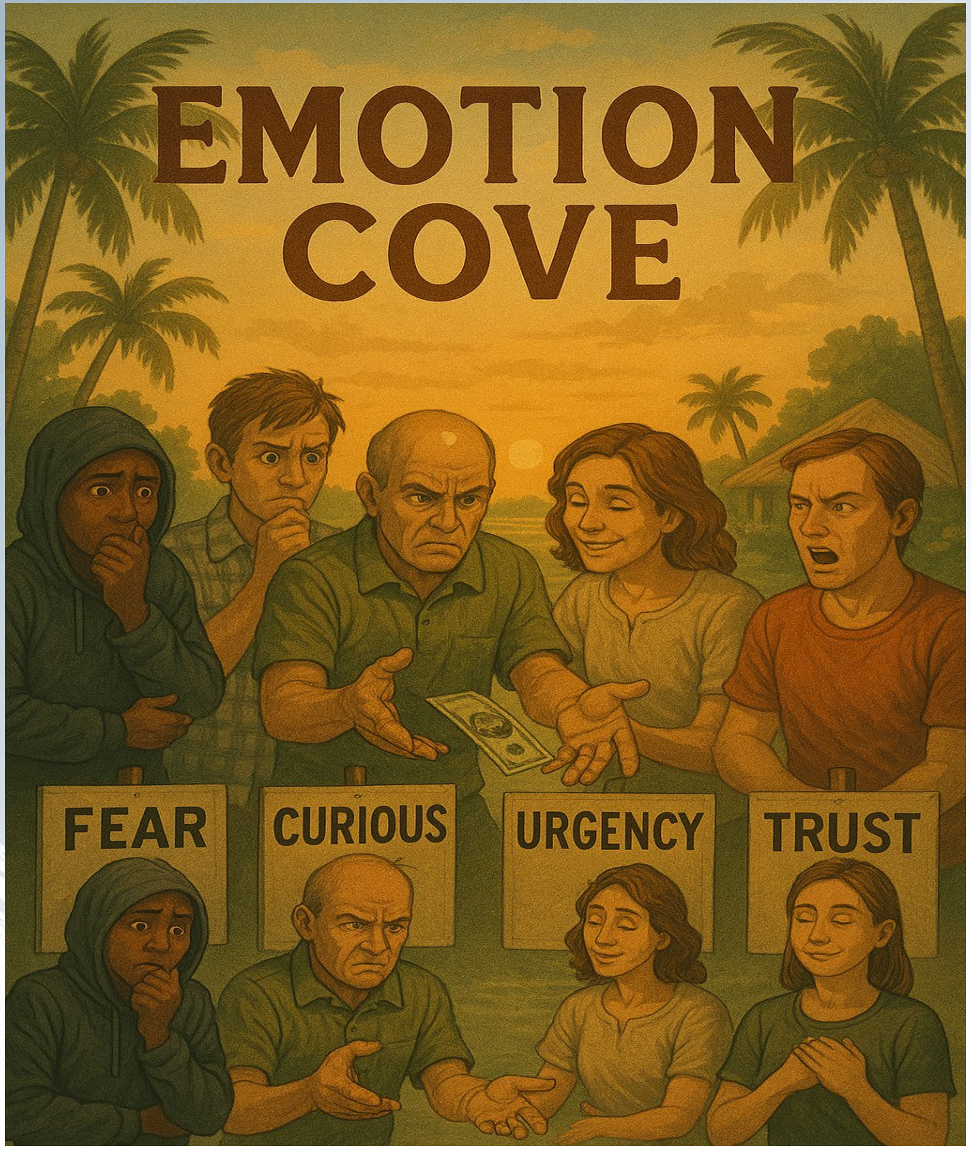
- Be wary of unusual requests
- Verify identities before sharing
- Don’t give in to high-pressure tactics
- Limit personal info shared online
- Educate and train employees

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 divulging confidential or personal information that may be used for fraudulent purposes.

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



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

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

CYBER THREATS
BEC
WEAK PASSWORDS
PHISHING/ VISHING/ SMISHING
RANSOMWARE /MALWARE

PHISHING
AND
BUSINESS EMAIL COMPROMISE

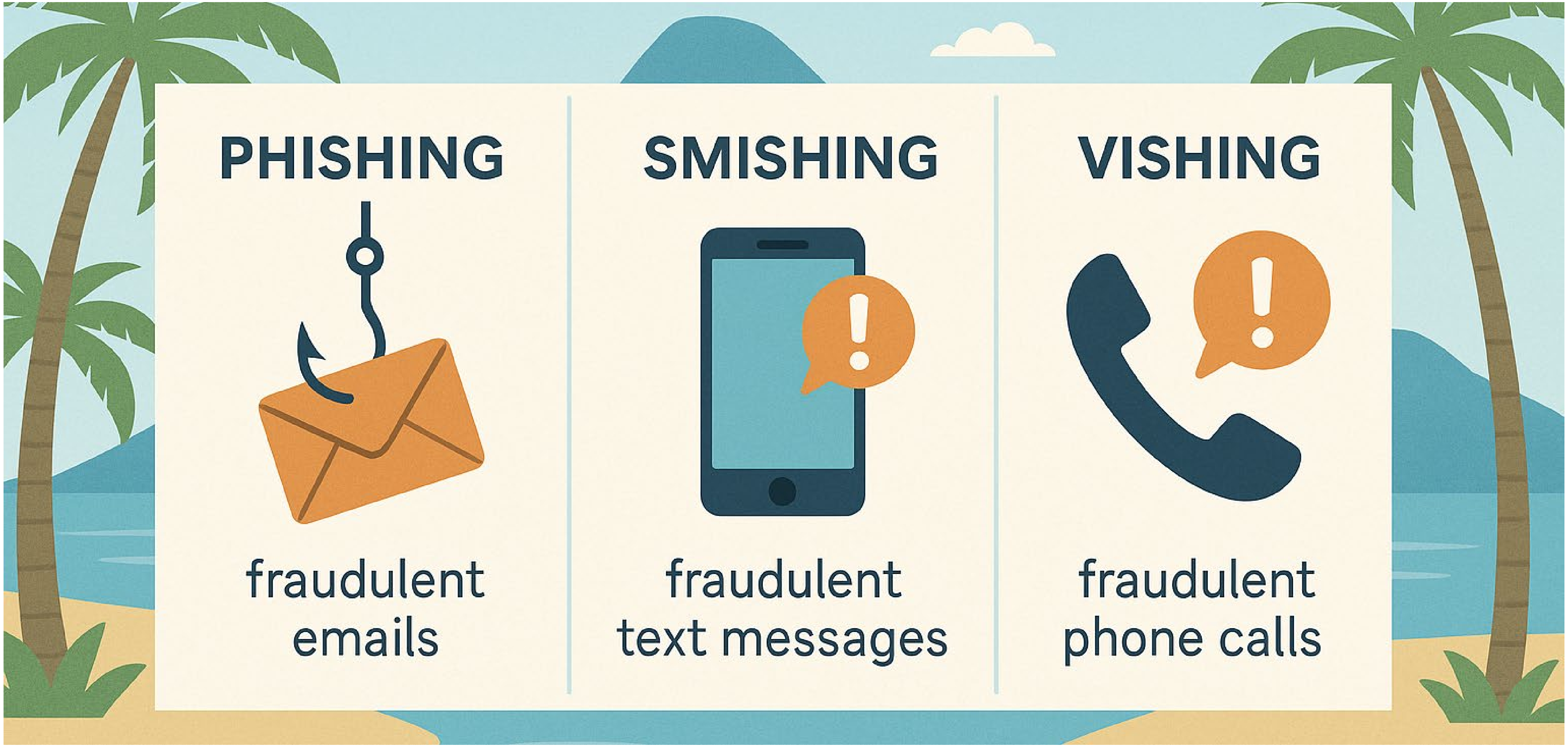
THE OFFICER SAID I HAD BEEN SCAMMED THROUGH PHISHING
BUT I HAVEN'T BEEN DOWN TO THE RIVER IN YEARS!
imgflip.com

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
and
What are they Phishing For?



PHISHING

fraudulent emails

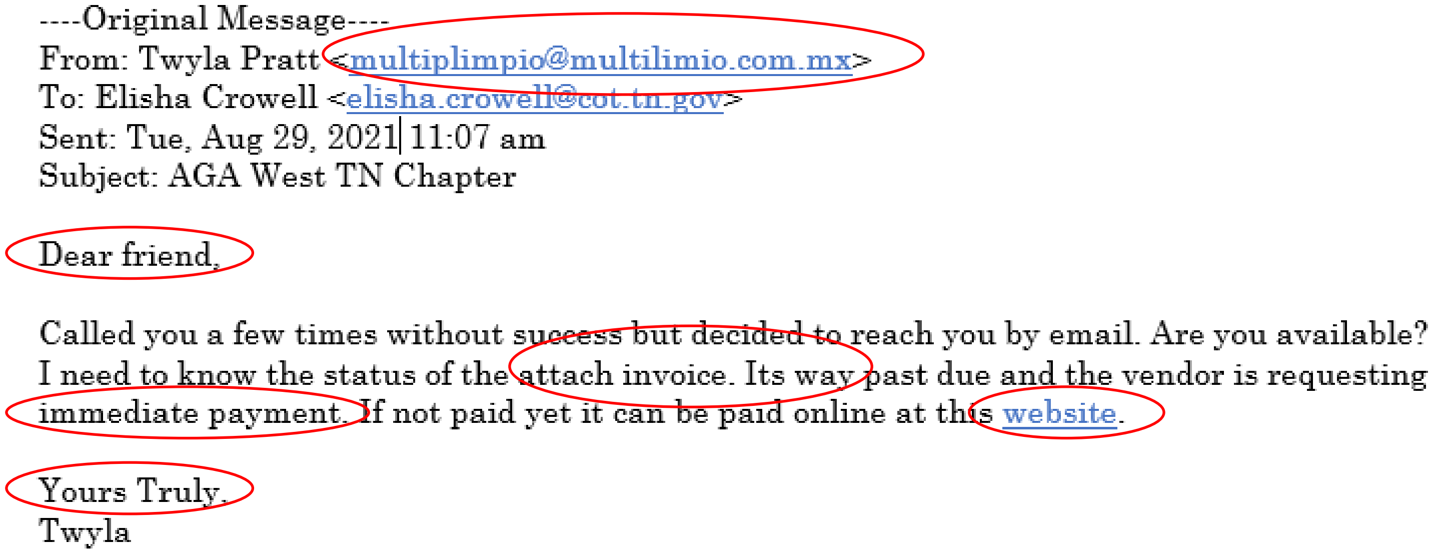
SMISHING

fraudulent text messages

VISHING

fraudulent phone calls

Phishing Email



----Original Message----
From: Twyla Pratt <multiplimpio@multilimio.com.mx>
To: Elisha Crowell <elisha.crowell@cot.tn.gov>
Sent: Tue, Aug 29, 2021 11:07 am
Subject: AGA West TN Chapter

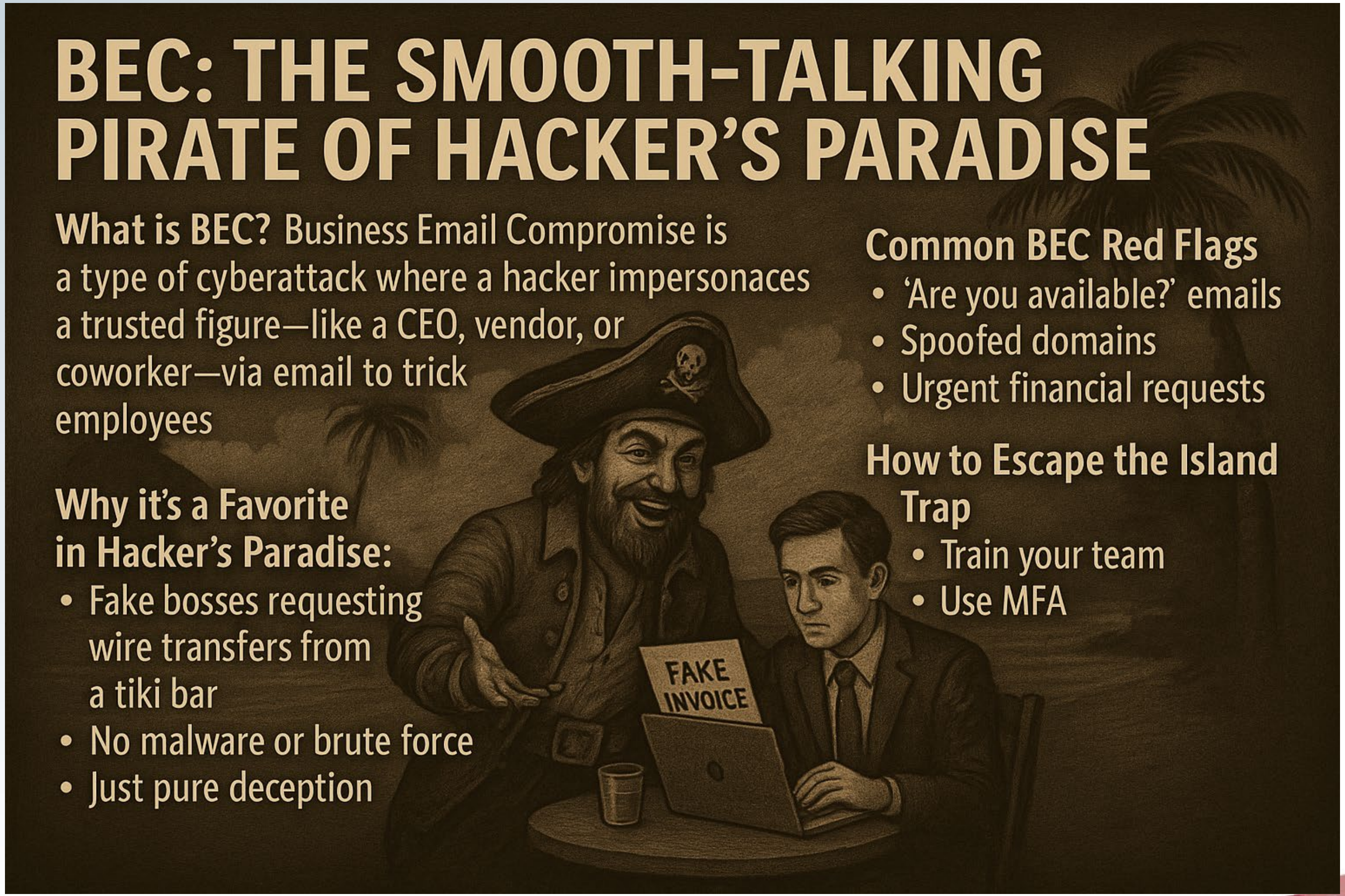
Dear friend,

Called you a few times without success but decided to reach you by email. Are you available? I need to know the status of the attach invoice. Its way past due and the vendor is requesting immediate payment. If not paid yet it can be paid online at this website.

Yours Truly,
Twyla

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 impersonaces a trusted figure—like a CEO, vendor, or coworker—via email to trick employees

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

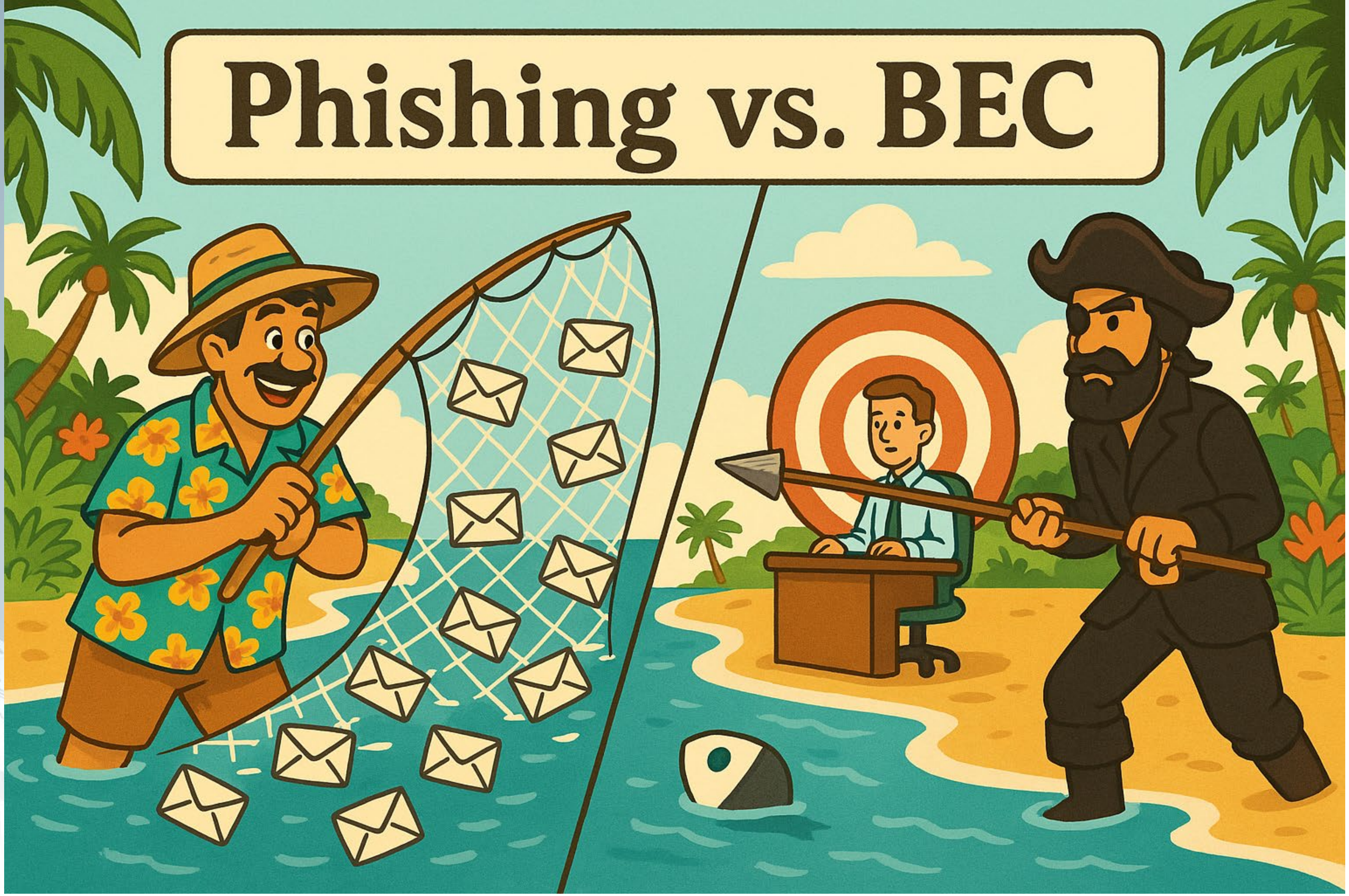
- Fake bosses requesting wire transfers from a tiki bar
- No malware or brute force
- Just pure deception

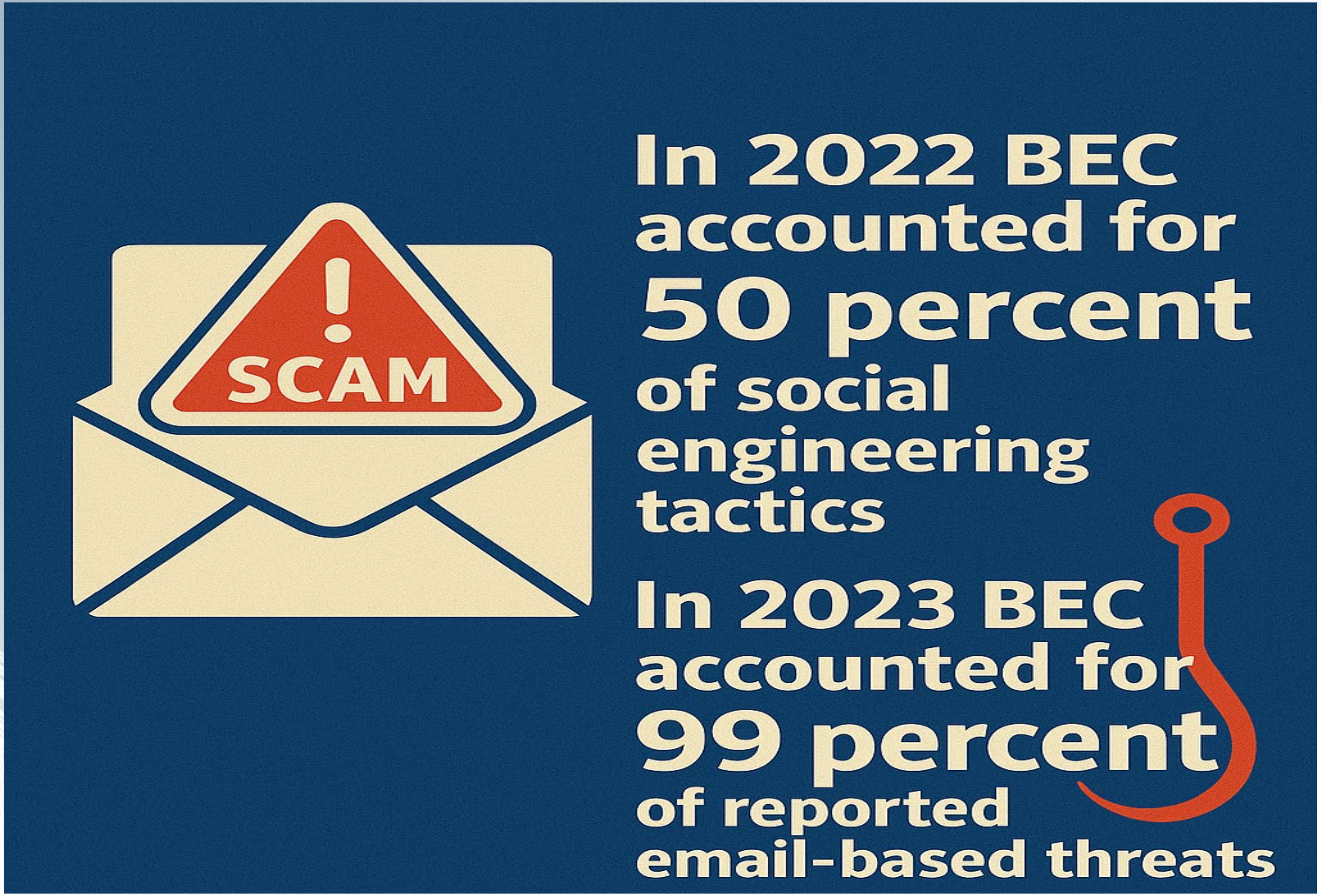
Common BEC Red Flags

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

How to Escape the Island Trap

- Train your team
- Use MFA

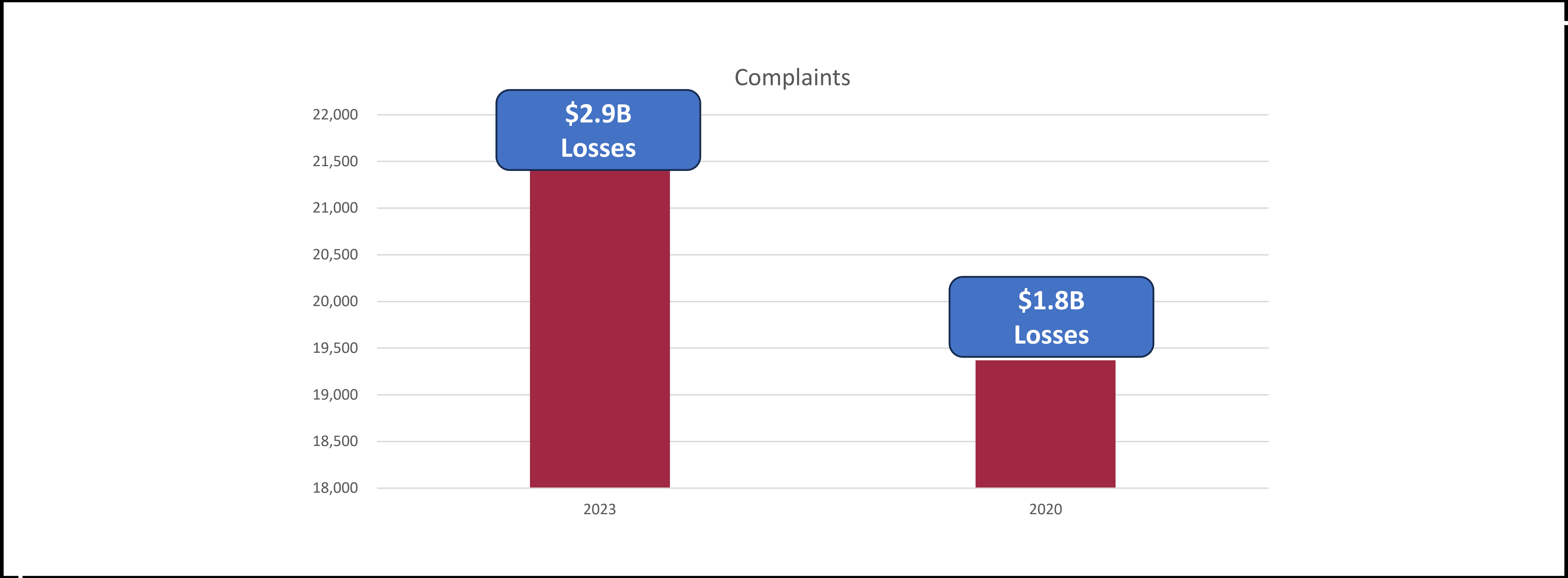

Phishing vs. BEC

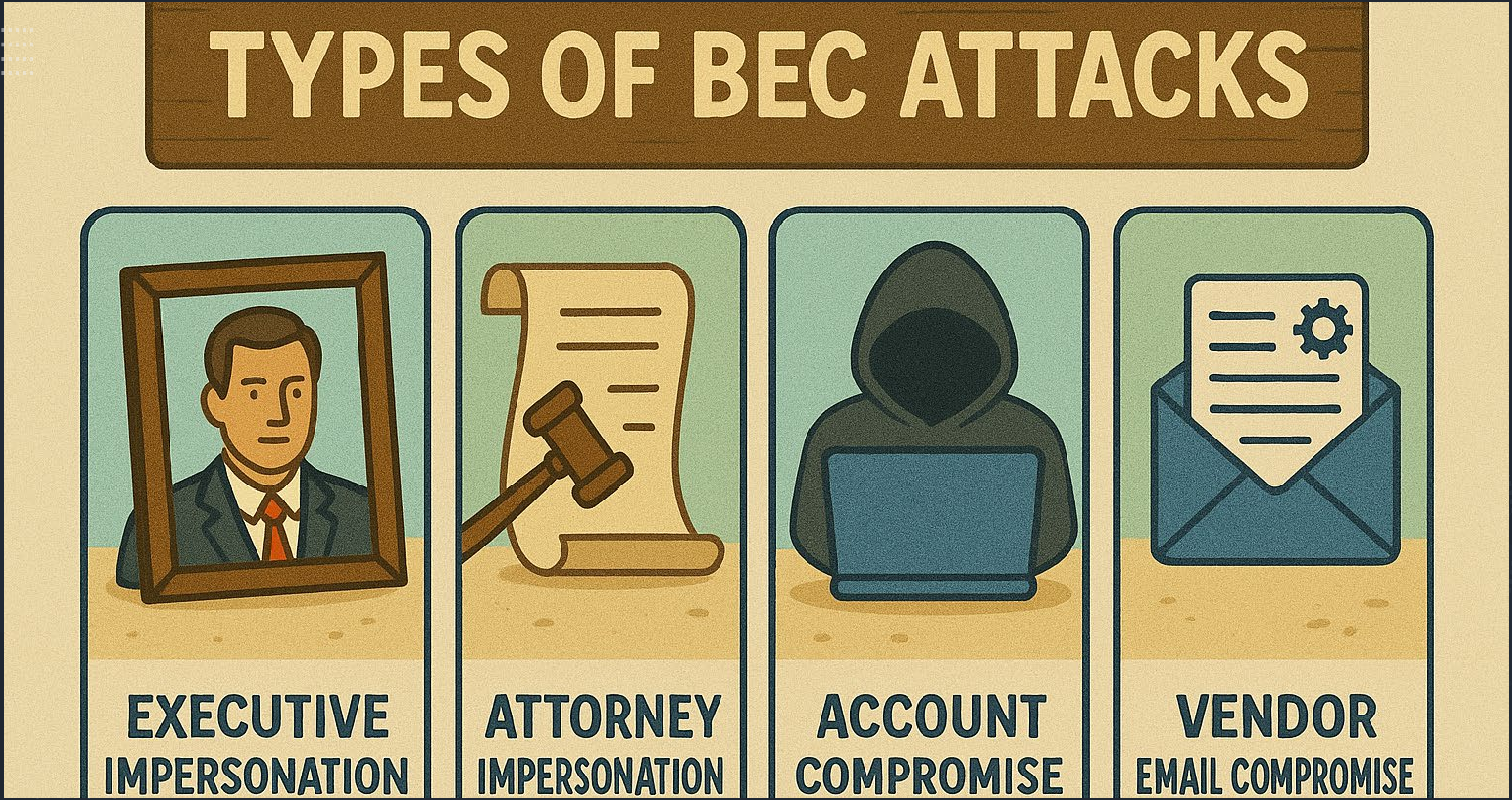


In 2022 BEC accounted for **50 percent** of social engineering tactics

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

BEC Complaints and Losses




TYPES OF BEC ATTACKS
EXECUTIVE IMPERSONATION
ATTORNEY IMPERSONATION
ACCOUNT COMPROMISE
VENDOR EMAIL COMPROMISE

The Great Email Heist:
A BEC Tale from Paradise

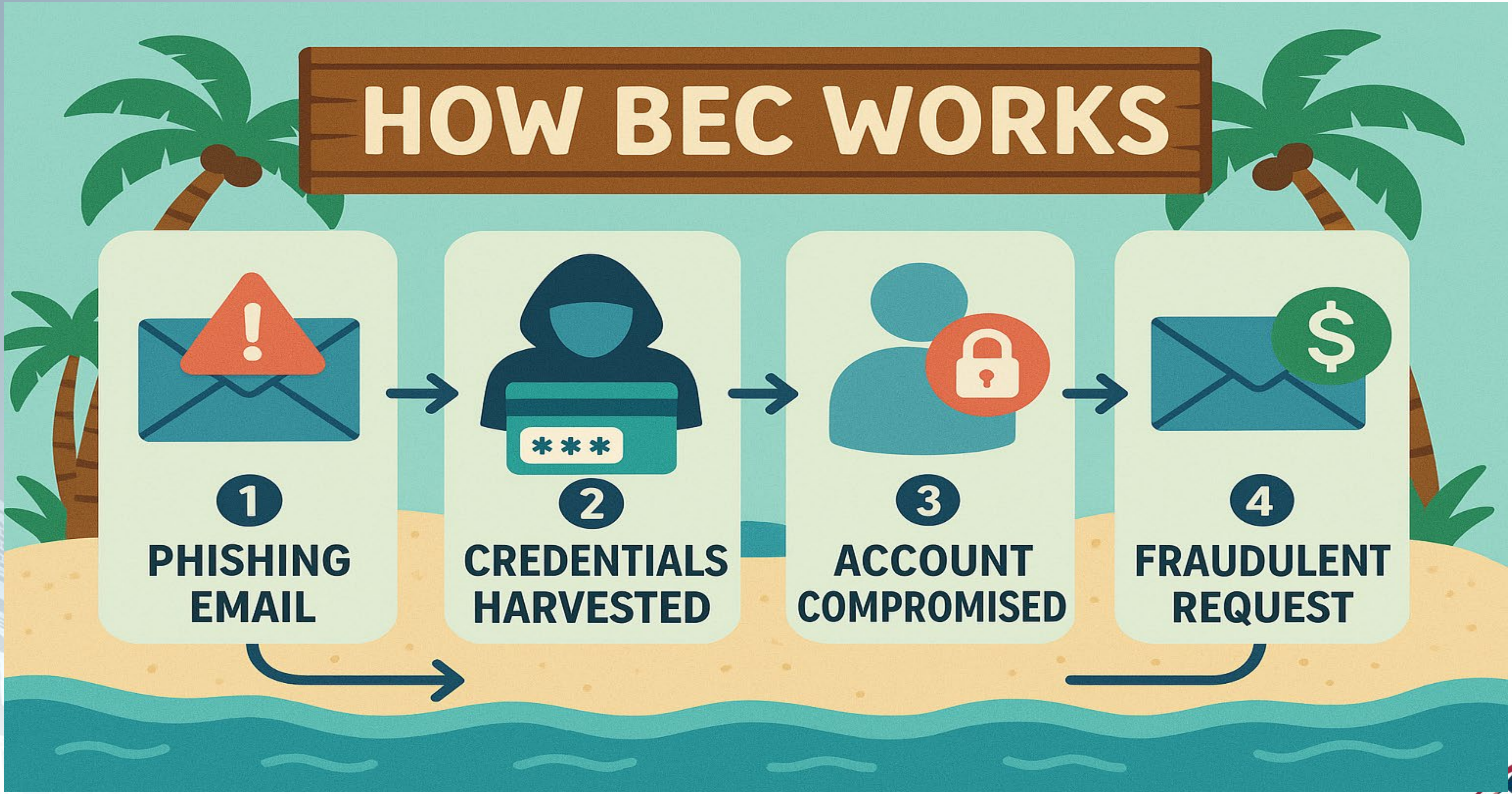
Send payment to our new vendor account—ASAP.
SAFE

Scene 1: *The Disguised* Castaway

Scene 2: Deceptive Message from '*the boss.*

Scene 3: The Yanishing **Message in a bottle**

Scene 4: The Vanishing Treasure



HOW BEC WORKS

1 PHISHING EMAIL

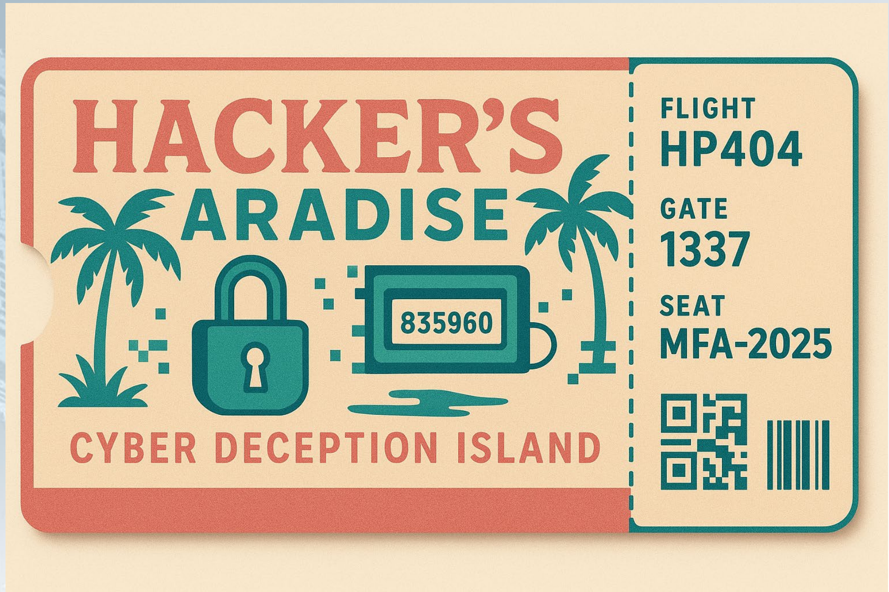
2 CREDENTIALS HARVESTED

3 ACCOUNT COMPROMISED

4 FRAUDULENT REQUEST

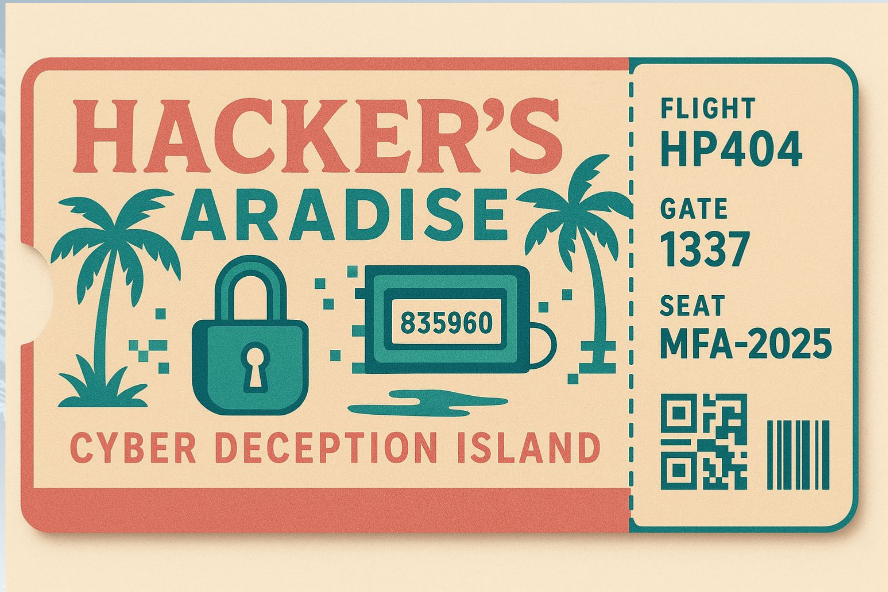
Real Life Examples of BEC Attacks

BEC Attacks



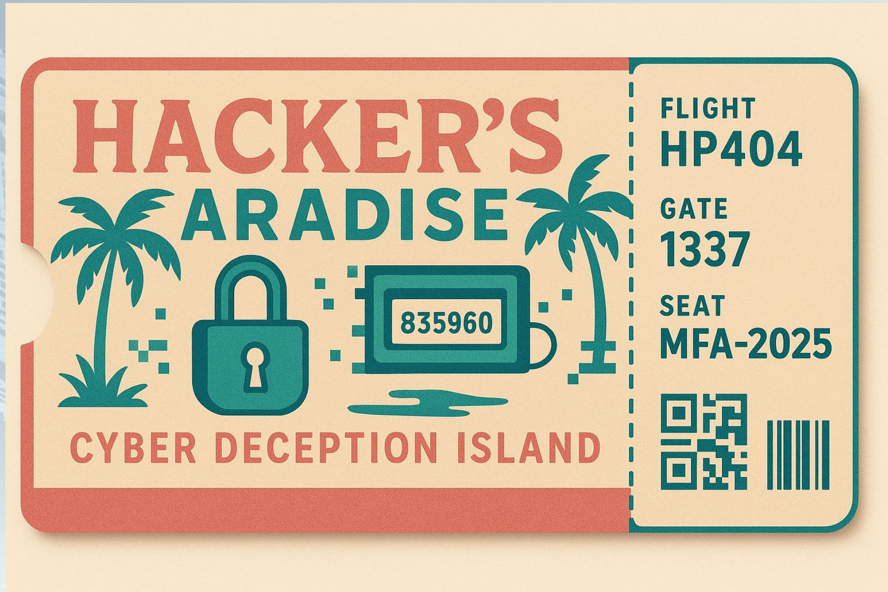
In 2018, the city of Atlanta, Georgia experienced a ransomware attack that severely disrupted municipal services. The ransomware encrypted critical files across the city's network, forcing systems offline and leading to significant recovery efforts. The attack, which did not involve a ransom payment,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

BEC Attacks



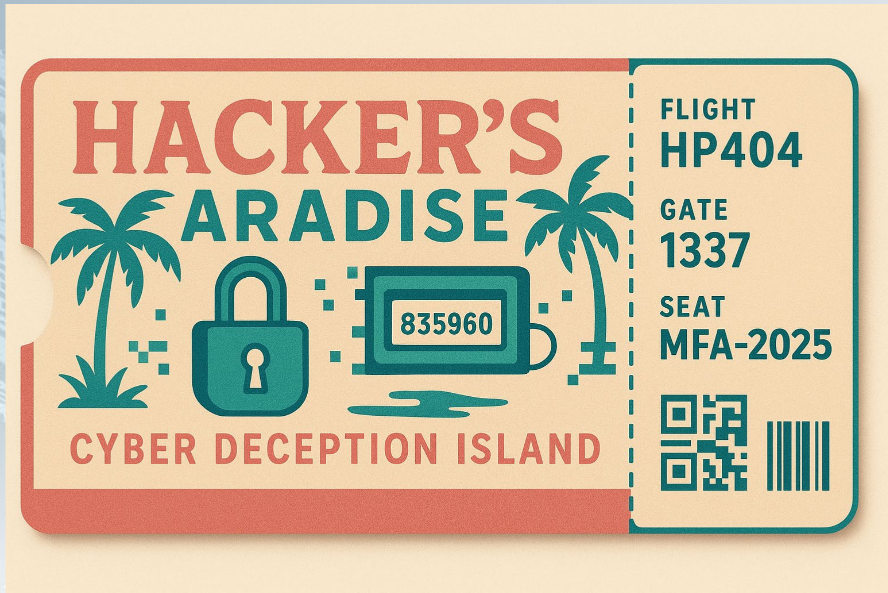
Atlanta-Children's Hospital -CFO was impersonated convinces the A/P dept. to switch bank on file and send $3.6 million dollars.

BEC Attacks



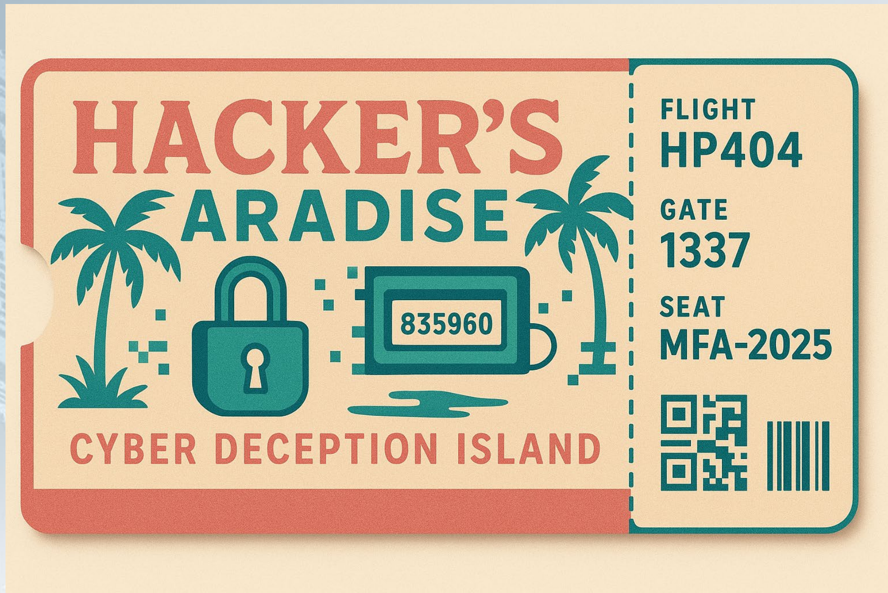
Eagle Mountain City, Utah- Vendor emails that appeared to be legitimate were sent to the city. Instructions were changed on the ACH payment, and $1.13 million dollars were sent to a fraudulent account. Account compromise for vendor and a VEC for the city.

BEC Attacks



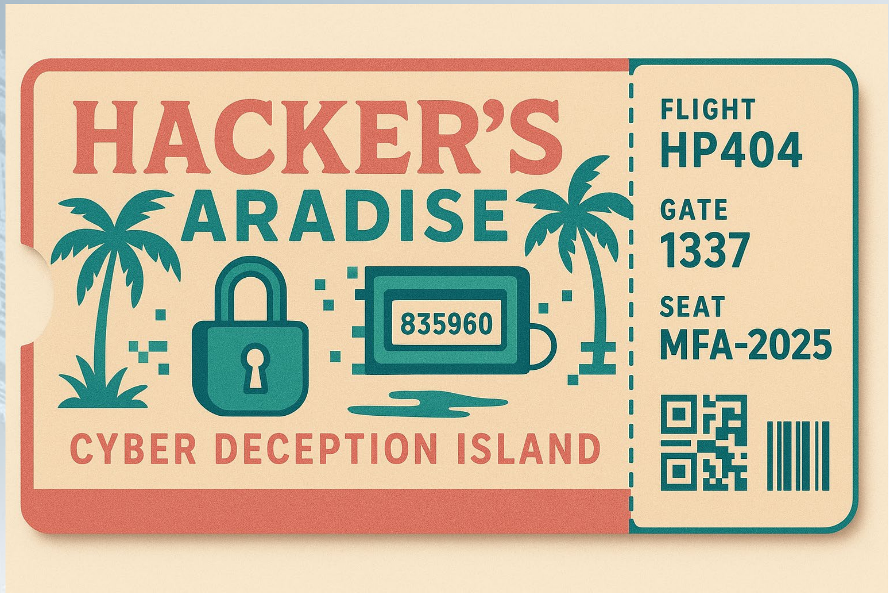
Toyota-3rd party hacker posed as a business partner-Subsidiary emails were sent to the accounting dept. asking them to send funds to a specific bank account or that production would be stopped. This was an account compromise of the business partner and a VEC compromise for Toyota.

BEC Attacks



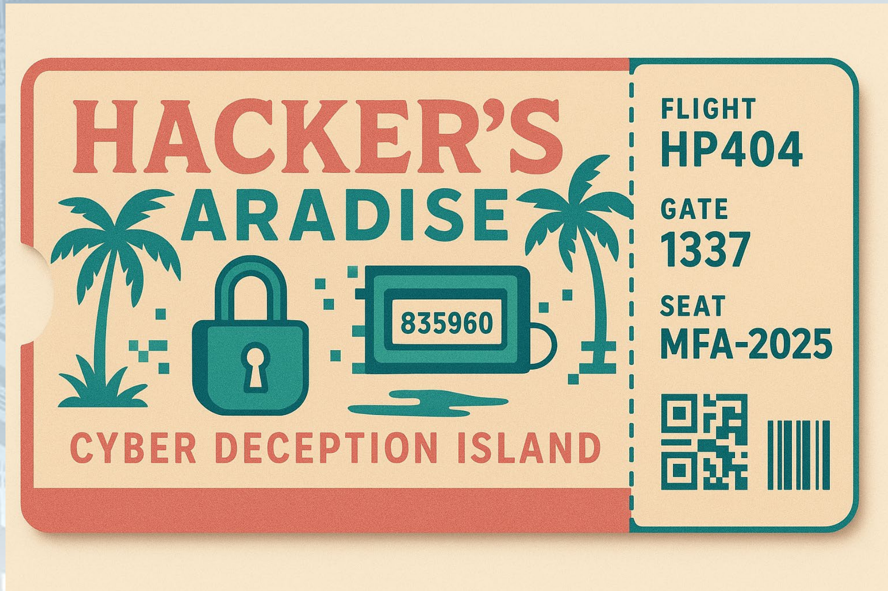
City of Lexington, KY-hacker claims to be from Community Action Council which is a local housing group. They asked to update their account information. 4 million dollars was sent.

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.

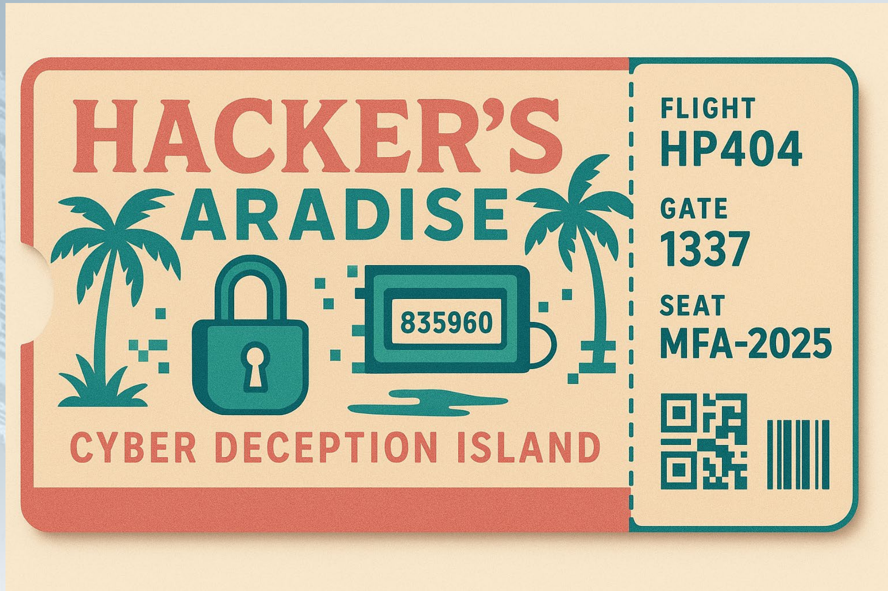
BEC Attacks



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.

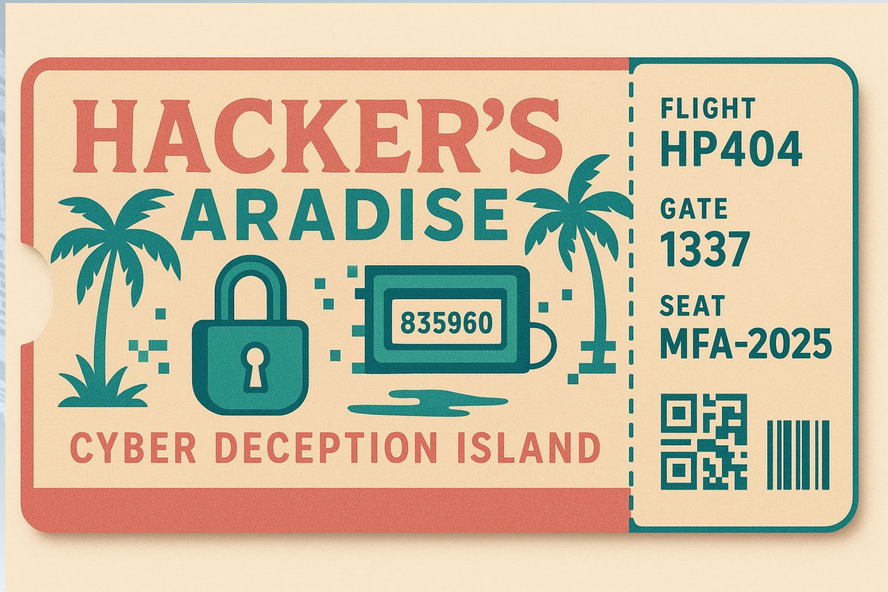
The city of Jackson suffered a loss of approximately $1.5 million due to this attack.

BEC Attacks

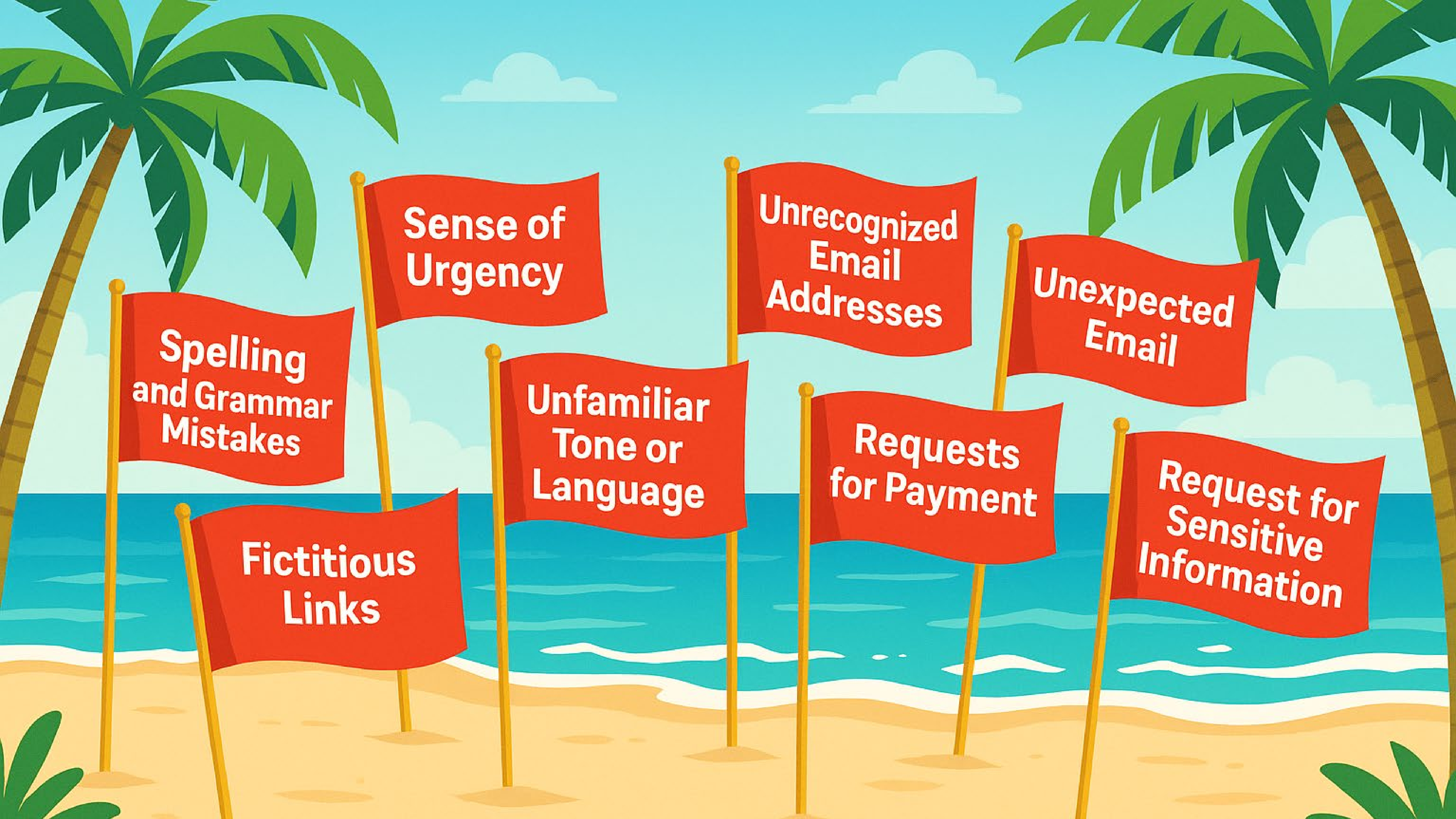


In 2019, the City of Memphis in Tennessee experienced a BEC attack where attackers targeted the city's finance department by compromising email accounts and using them to impersonate officials. This led to fraudulent wire transfers, resulting in approximately $3.2 million in losses.

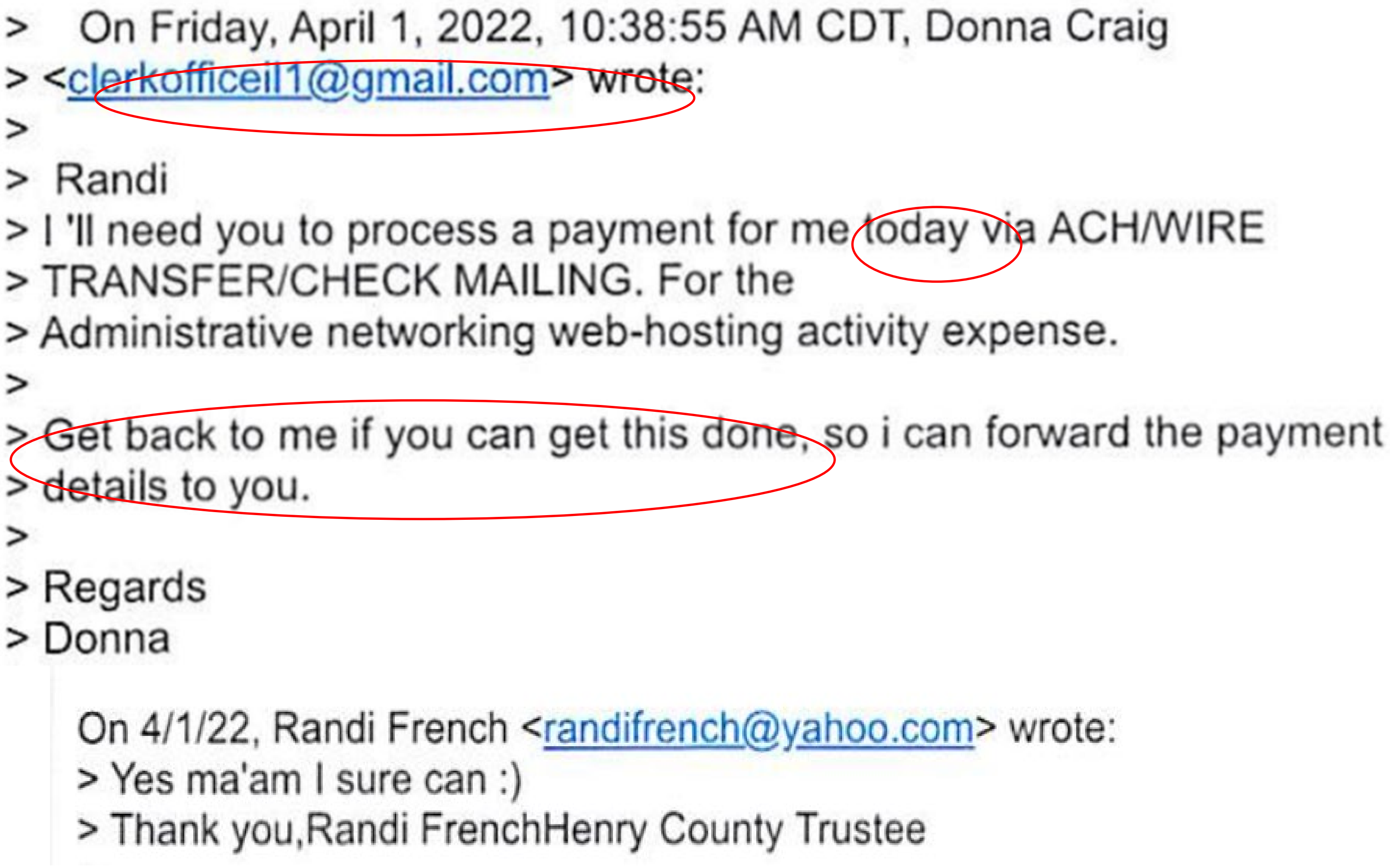
BEC Attacks



In 2019, the city of New Bedford, Massachusetts experienced a BEC attack where attackers used a fake invoice scheme to defraud the city. As a result, the city lost approximately $3.5 million.


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

Real-World Example

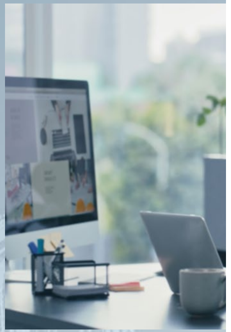


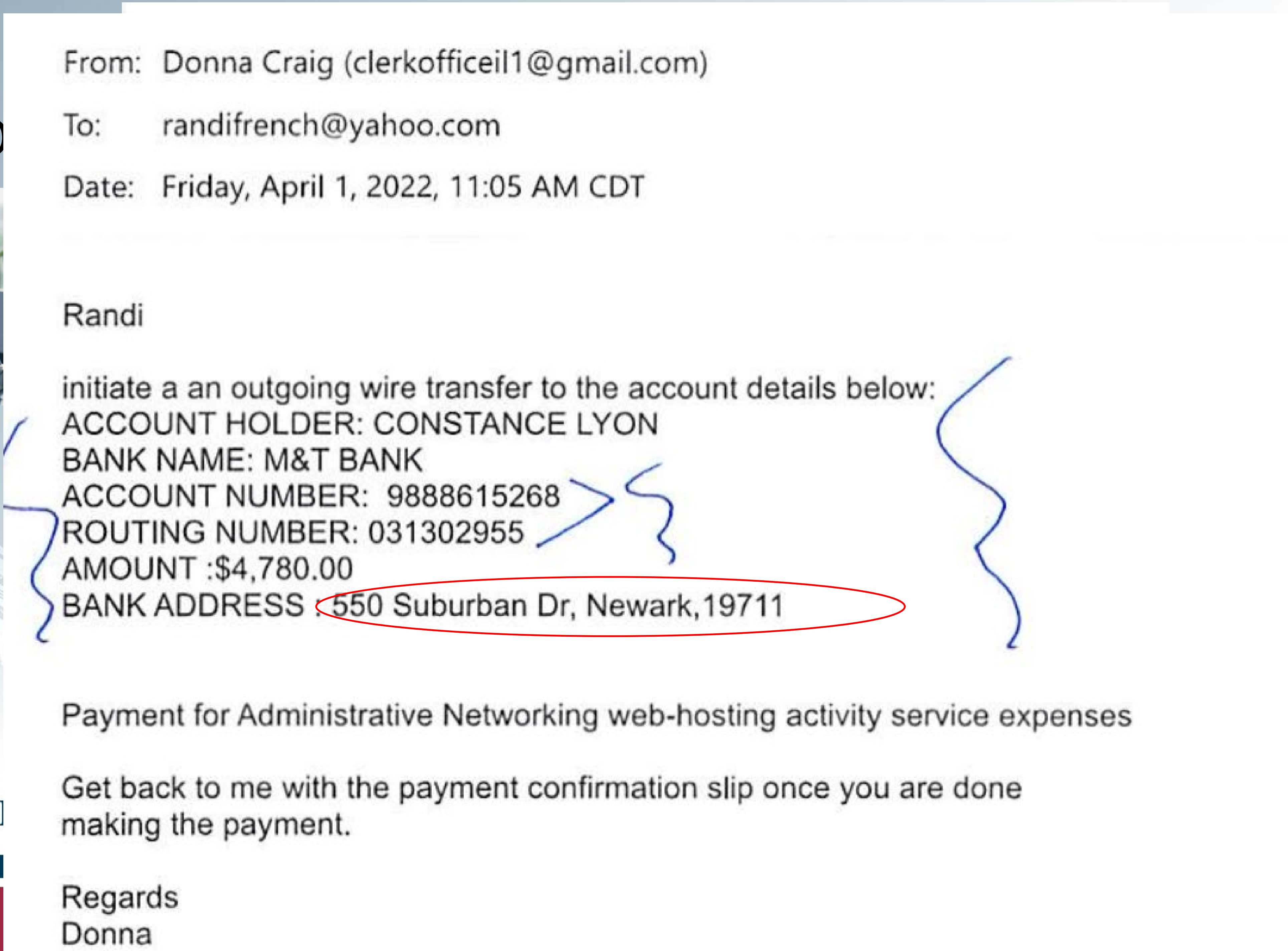
> On Friday, April 1, 2022, 10:38:55 AM CDT, Donna Craig
> <clerkofficeil1@gmail.com> wrote:
>
> Randi
> I 'll need you to process a payment for me today via ACH/WIRE
> TRANSFER/CHECK MAILING. For the
> Administrative networking web-hosting activity expense.
>
> Get back to me if you can get this done, 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

Ho





From: Donna Craig (clerkofficeil1@gmail.com)

To: randifrench@yahoo.com

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

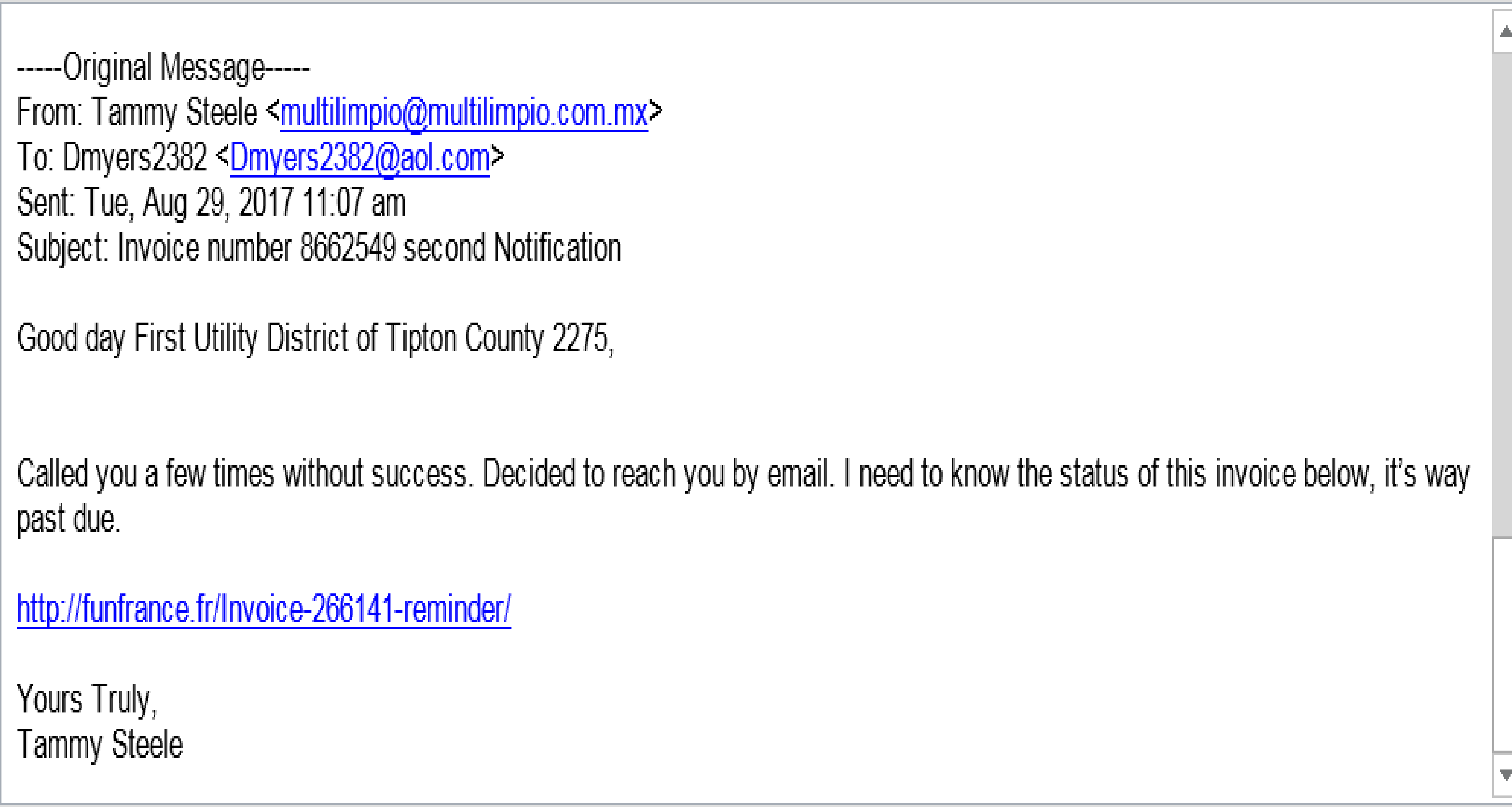
Randi

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



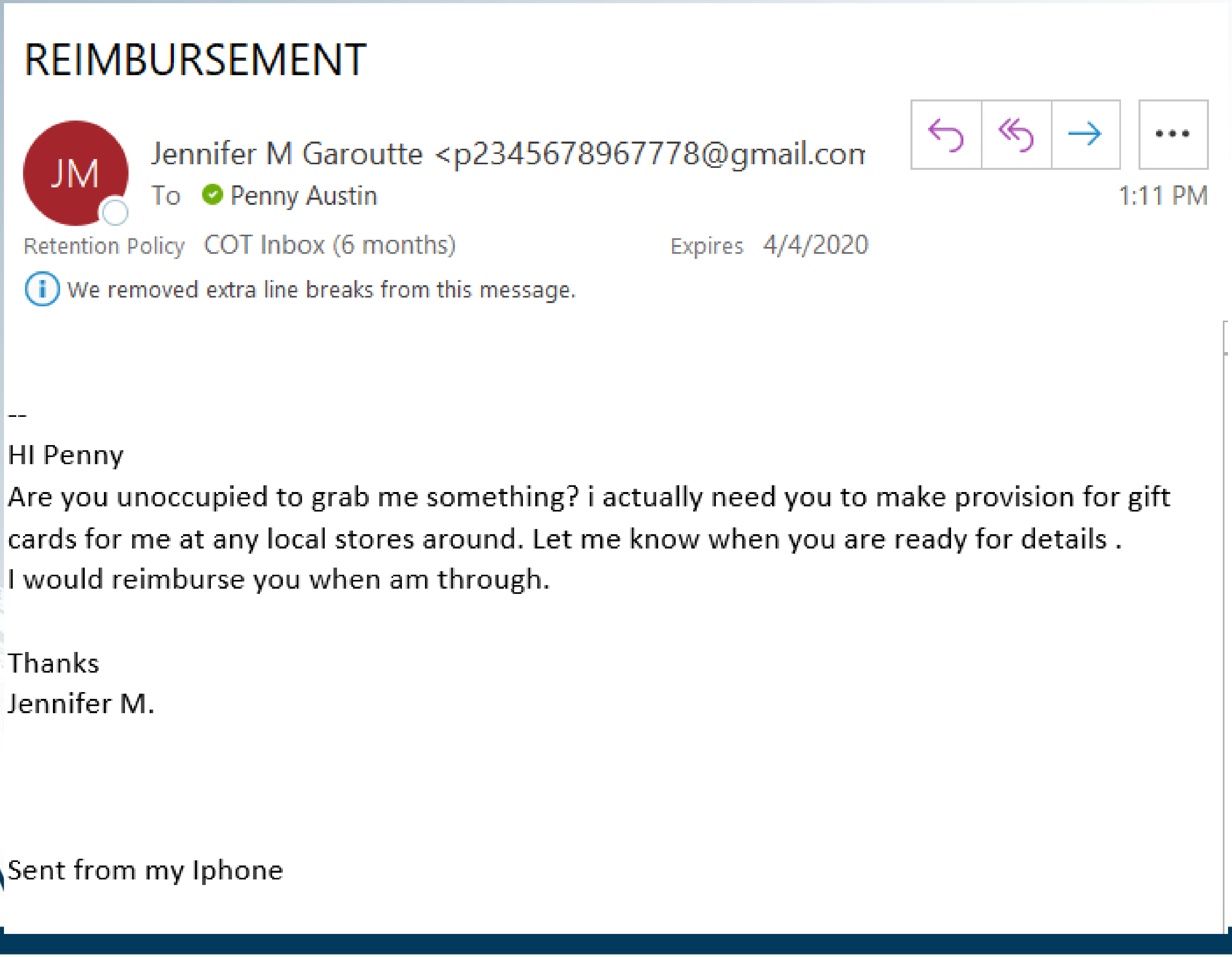
-----Original Message-----
From: Tammy Steele <multilimpio@multilimpio.com.mx>
To: Dmyers2382 <Dmyers2382@aol.com>
Sent: Tue, Aug 29, 2017 11:07 am
Subject: Invoice number 8662549 second Notification

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



REIMBURSEMENT

Jennifer M Garoutte <p2345678967778@gmail.con

To Penny Austin

1:11 PM

Retention Policy COT Inbox (6 months) Expires 4/4/2020

ⓘ We removed extra line breaks from this message.

--

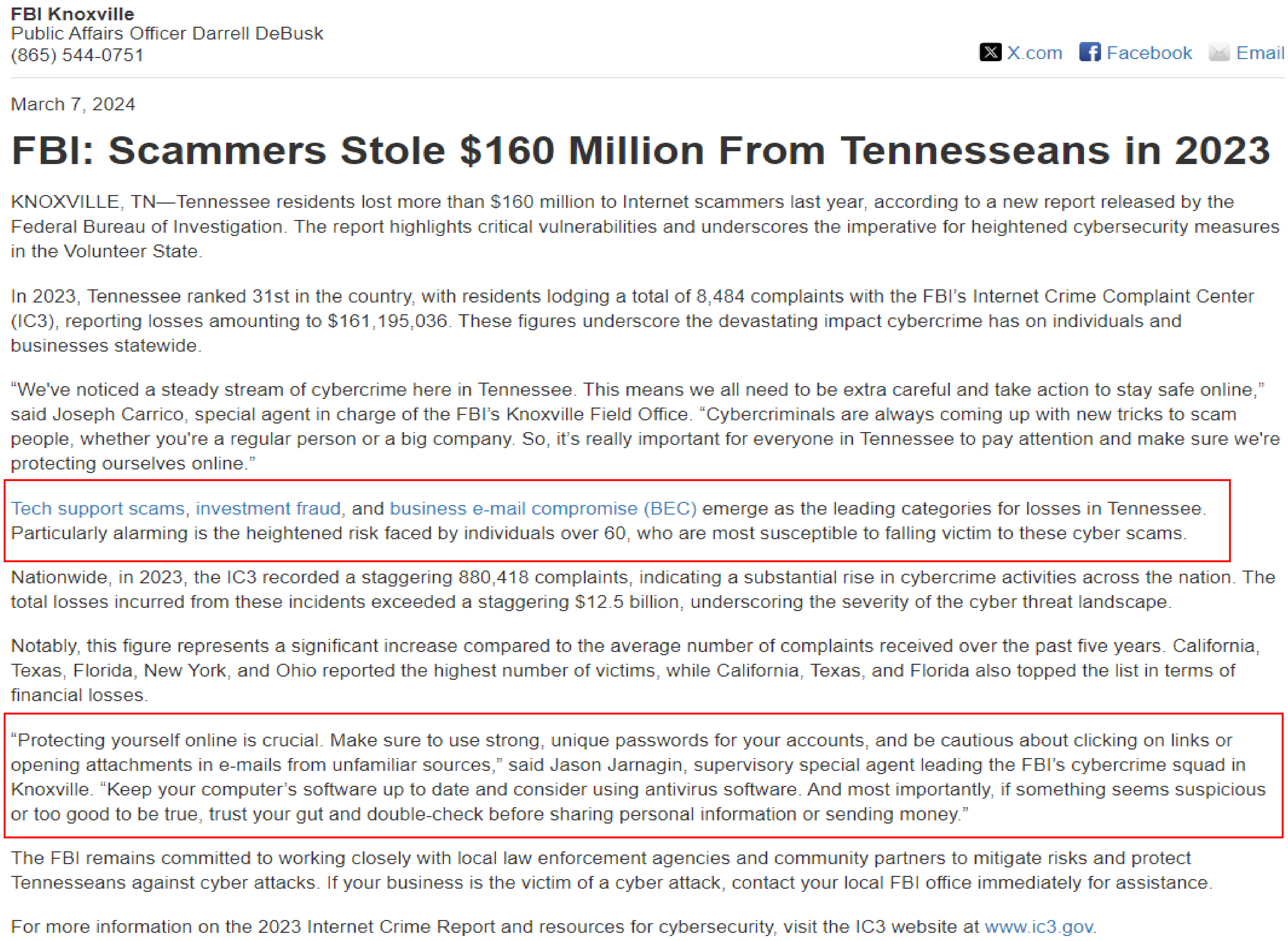
HI Penny

Are you unoccupied to grab me something? i actually need you to make provision for gift cards for me at any local stores around. Let me know when you are ready for details .

I would reimburse you when am through.

Thanks
Jennifer M.

Sent from my Iphone



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

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.

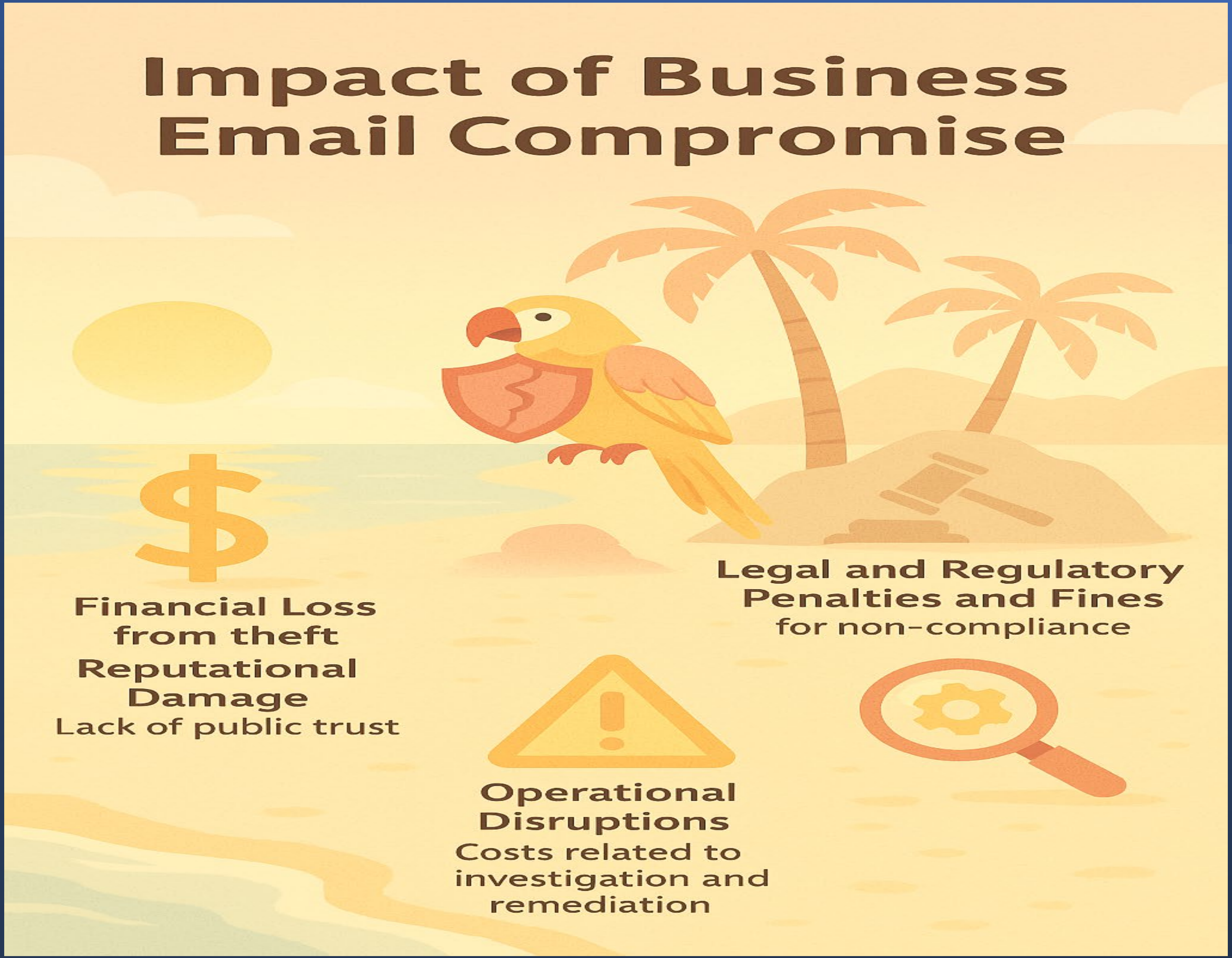
Nationwide, in 2023, the IC3 recorded a staggering 880,418 complaints, indicating a substantial rise in cybercrime activities across the nation. The total losses incurred from these incidents exceeded a staggering $12.5 billion, underscoring the severity of the cyber threat landscape.

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.



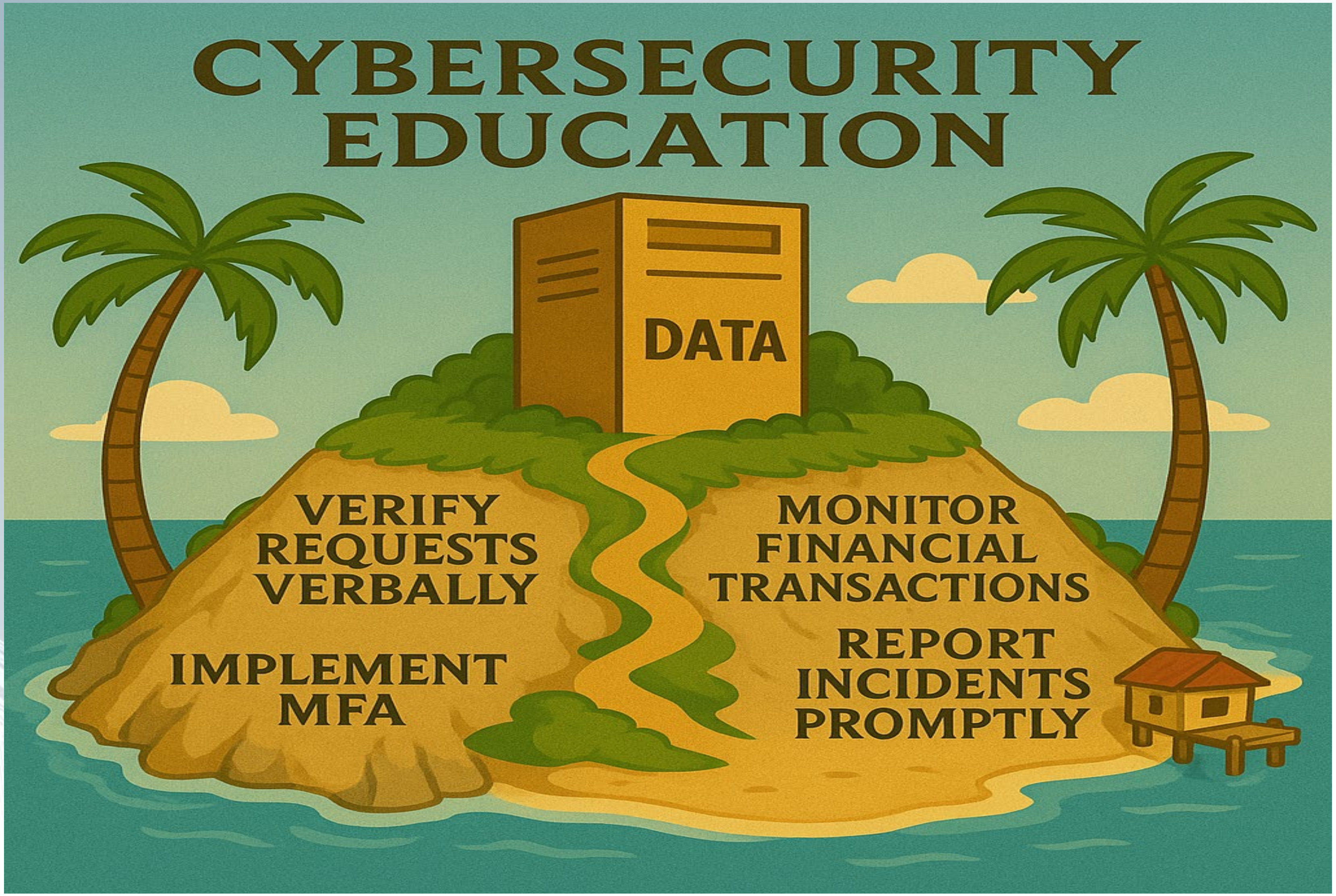
Impact of Business Email Compromise

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


CYBERSECURITY EDUCATION
DATA
VERIFY REQUESTS VERBALLY
IMPLEMENT MFA
MONITOR FINANCIAL TRANSACTIONS
REPORT INCIDENTS PROMPTLY

Ransomware and Malware

Ransomware/Malware Defined

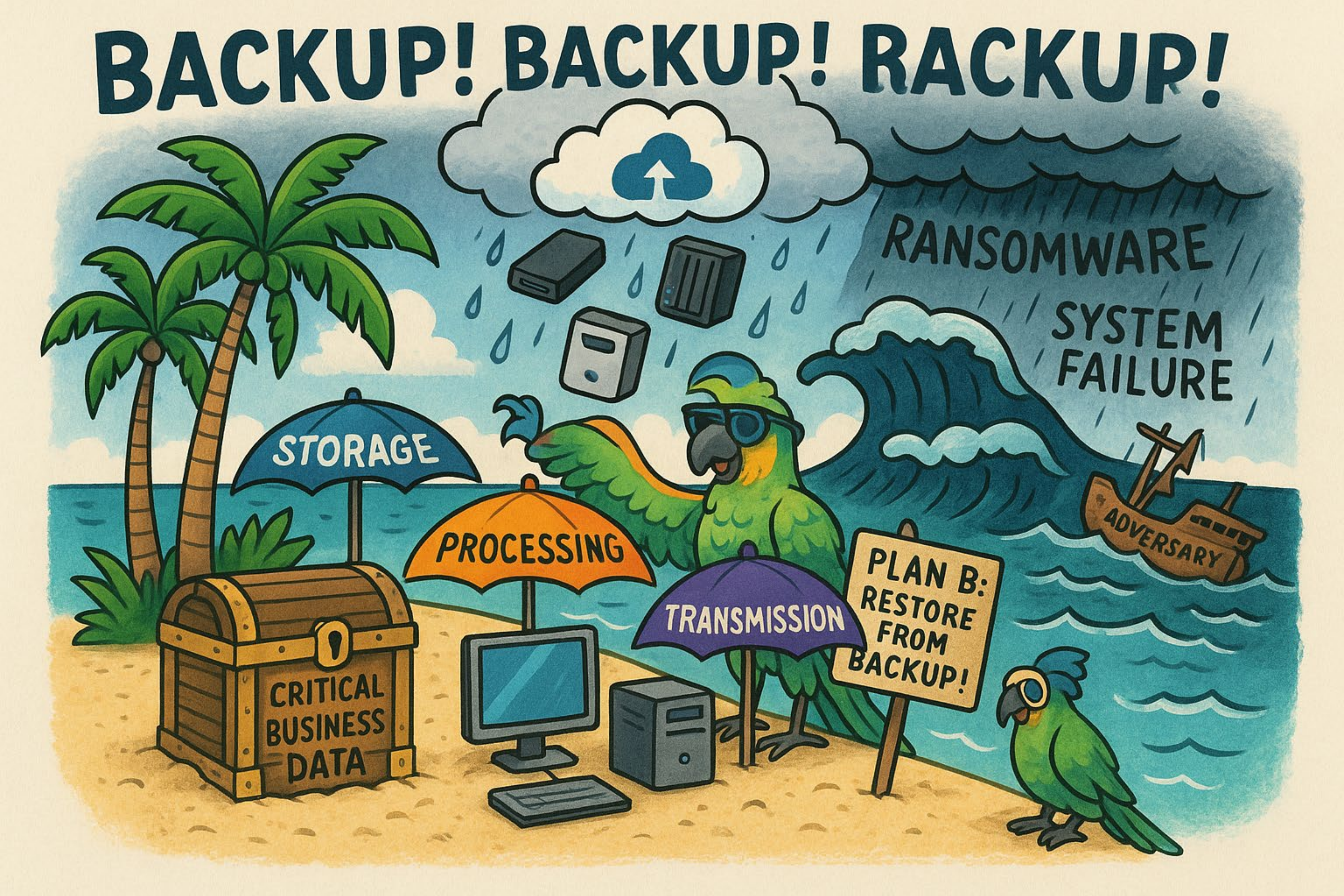
Malware is malicious software.

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.

CLICK CAREFULLY ON HACKER'S PARADISE
RANSWARE
MALWARE
BEC
PHISHING
PHISHING

RANSOMWARE AND MALWARE CLICK! CLICK!

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


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

UPDATE!
OPERATING SYSTEM
VIRUS PROTECTION

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.

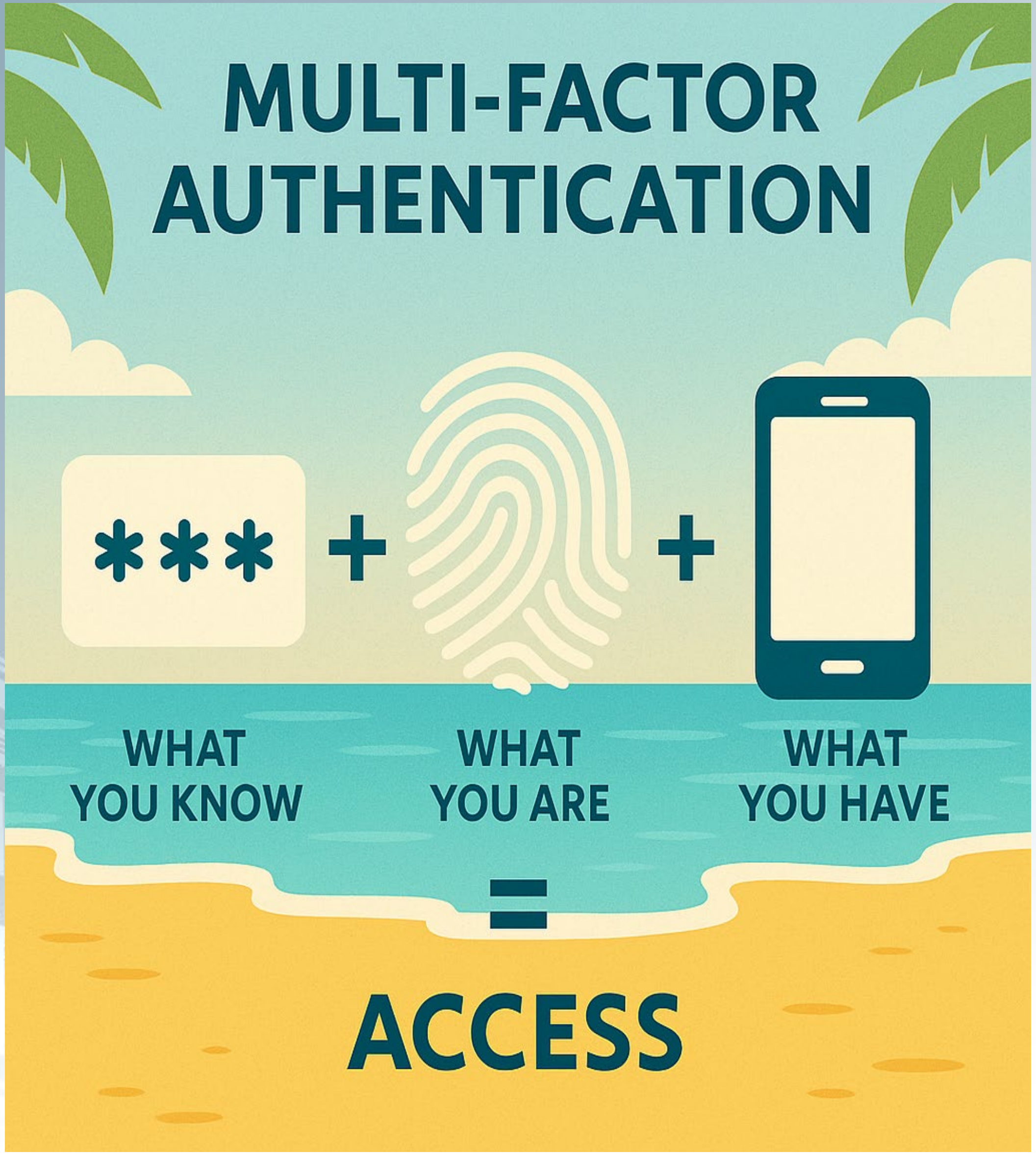
How Do We Stay Away From “Hacker’s Paradise?”

STRONG PASSWORDS AND MULTI-FACTOR AUTHENTICATION

CREATE STRONG PASSWORDS
PASSWORD
PHISHING
MFA
MFA IS YOUR SUNSCREEN— DON'T GO ONLINE WITHOUT IT!

MFA

REQUIRES MORE THAN A PASSWORD

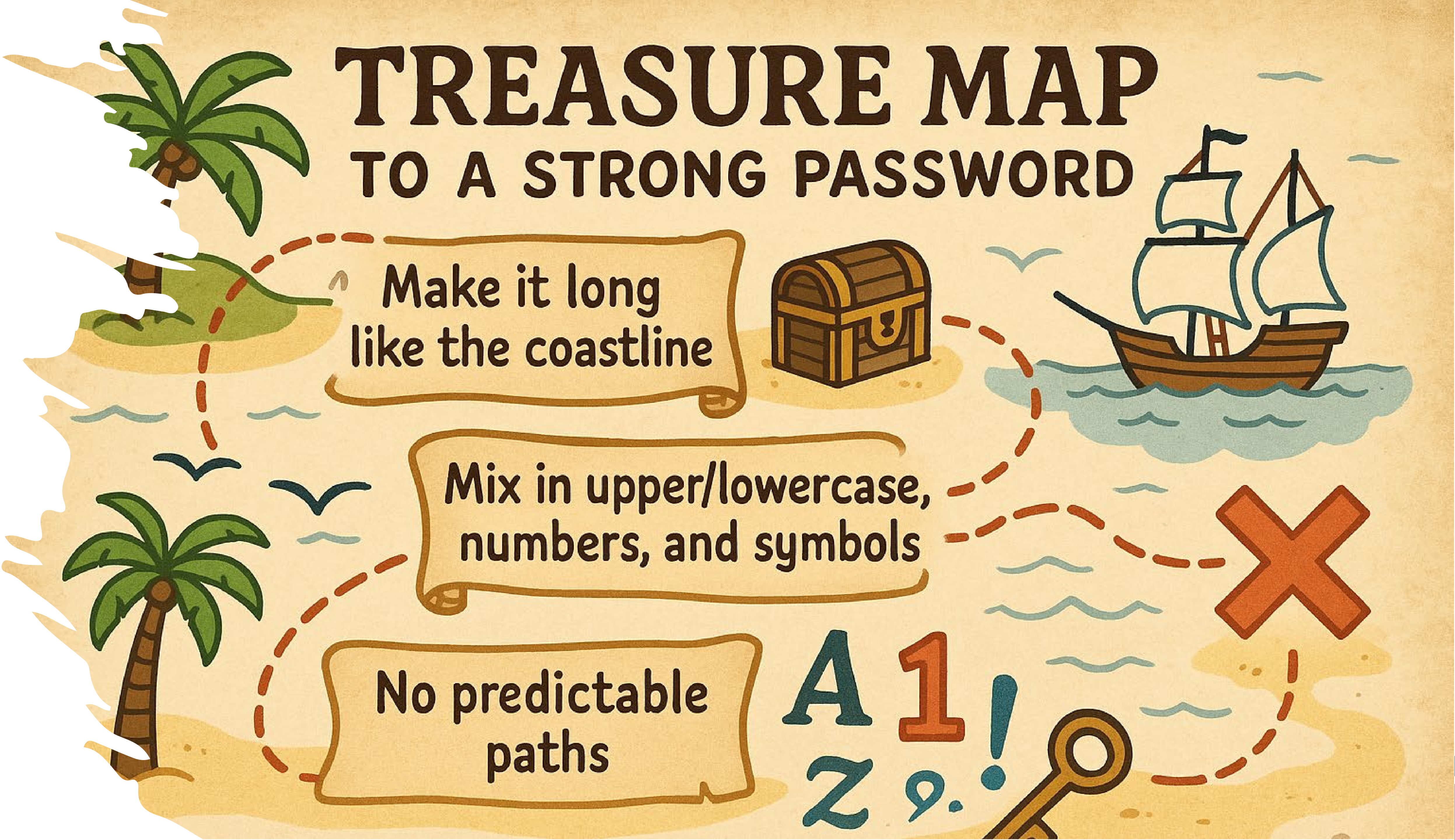


Password
Know

Biological
Who You Are

Key Card/
Phone/
Sunscreen
What You Have

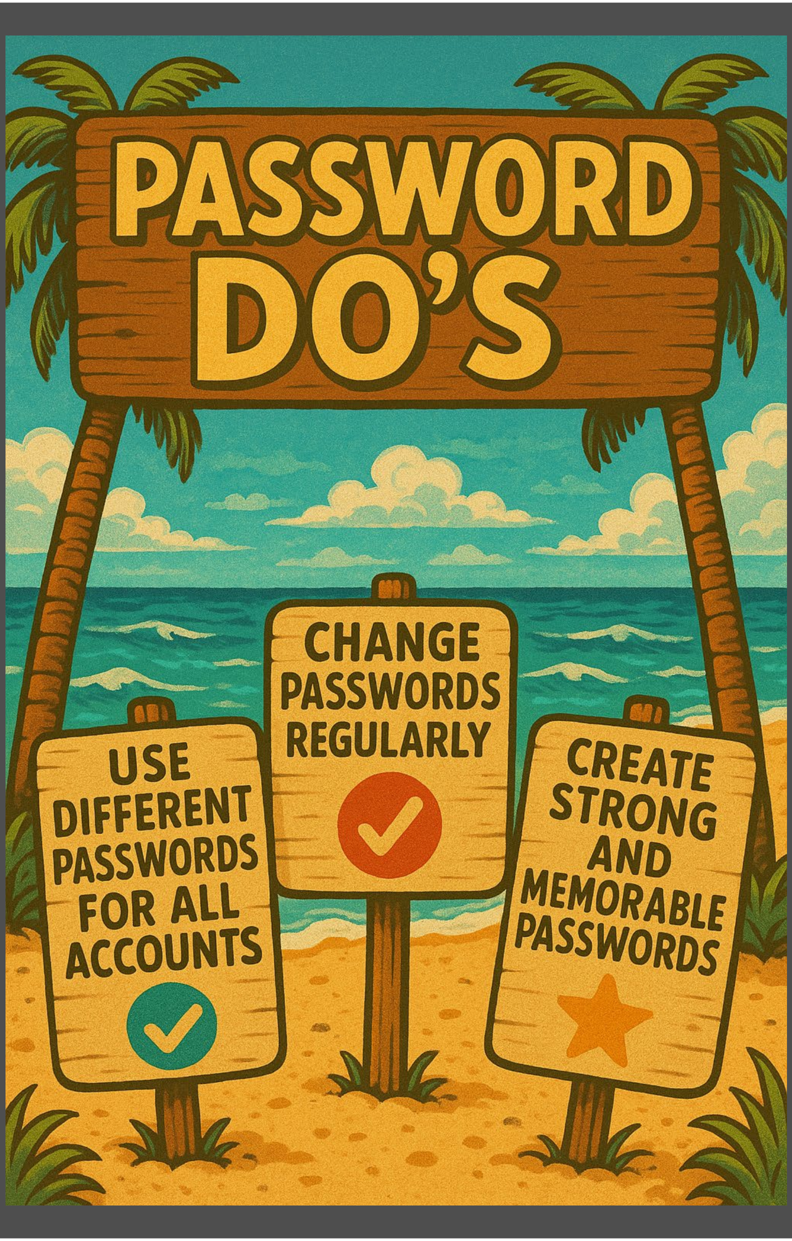
TREASURE MAP
TO A STRONG PASSWORD

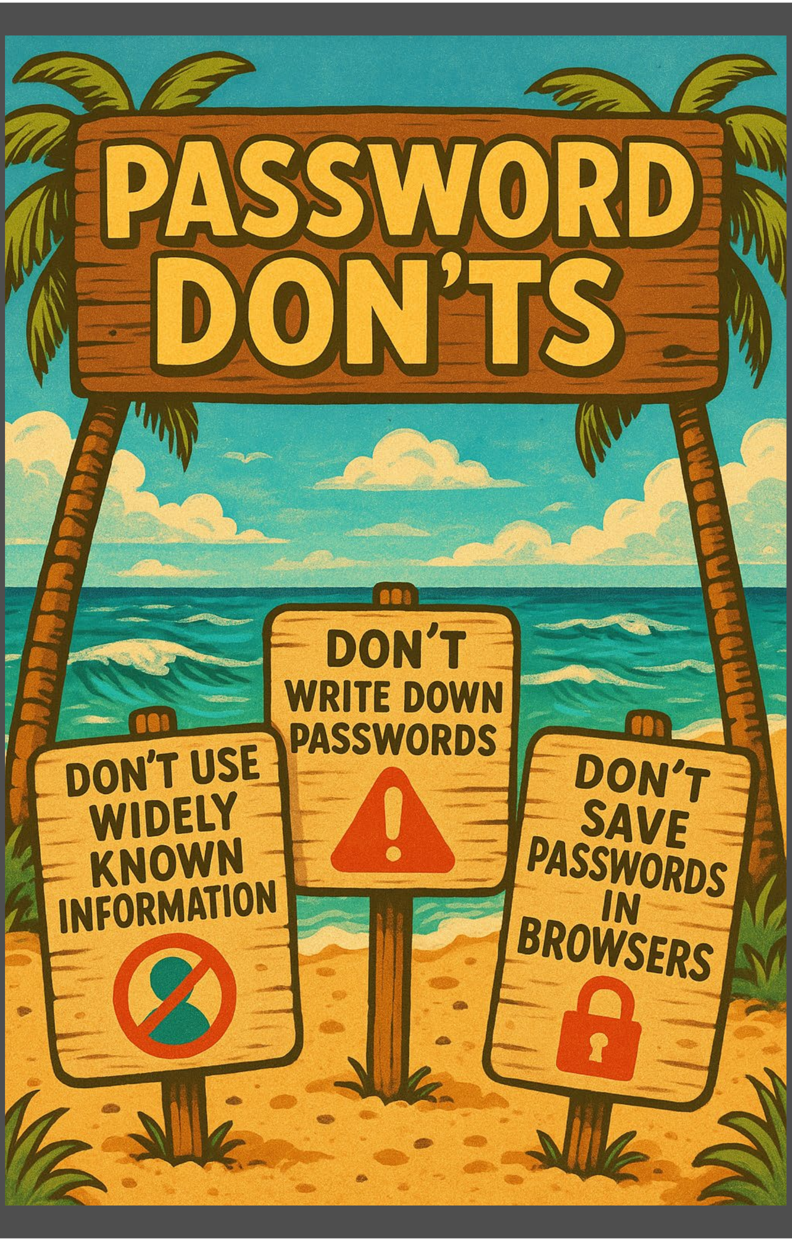


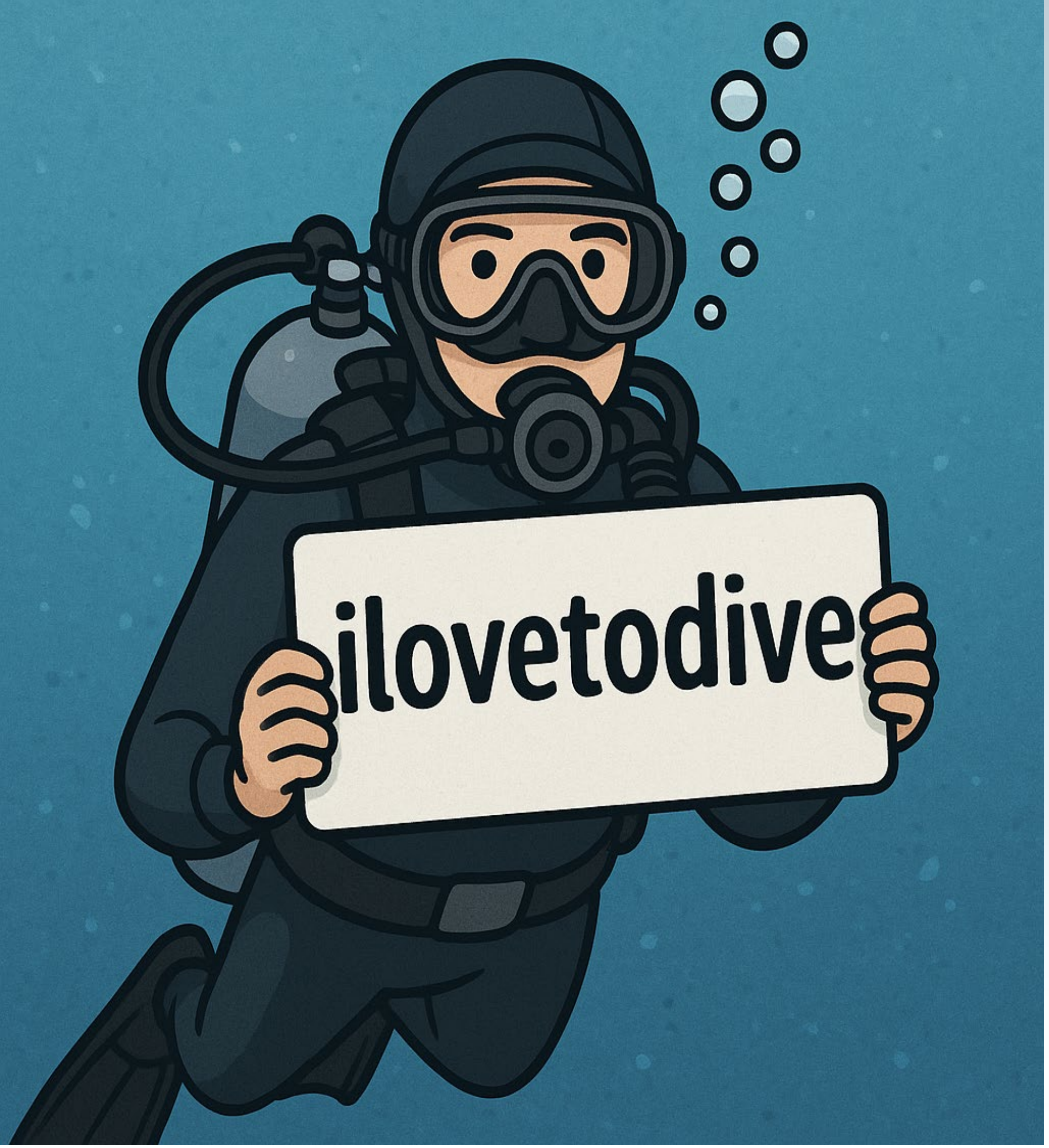
Make it long like the coastline

Mix in upper/lowercase, numbers, and symbols

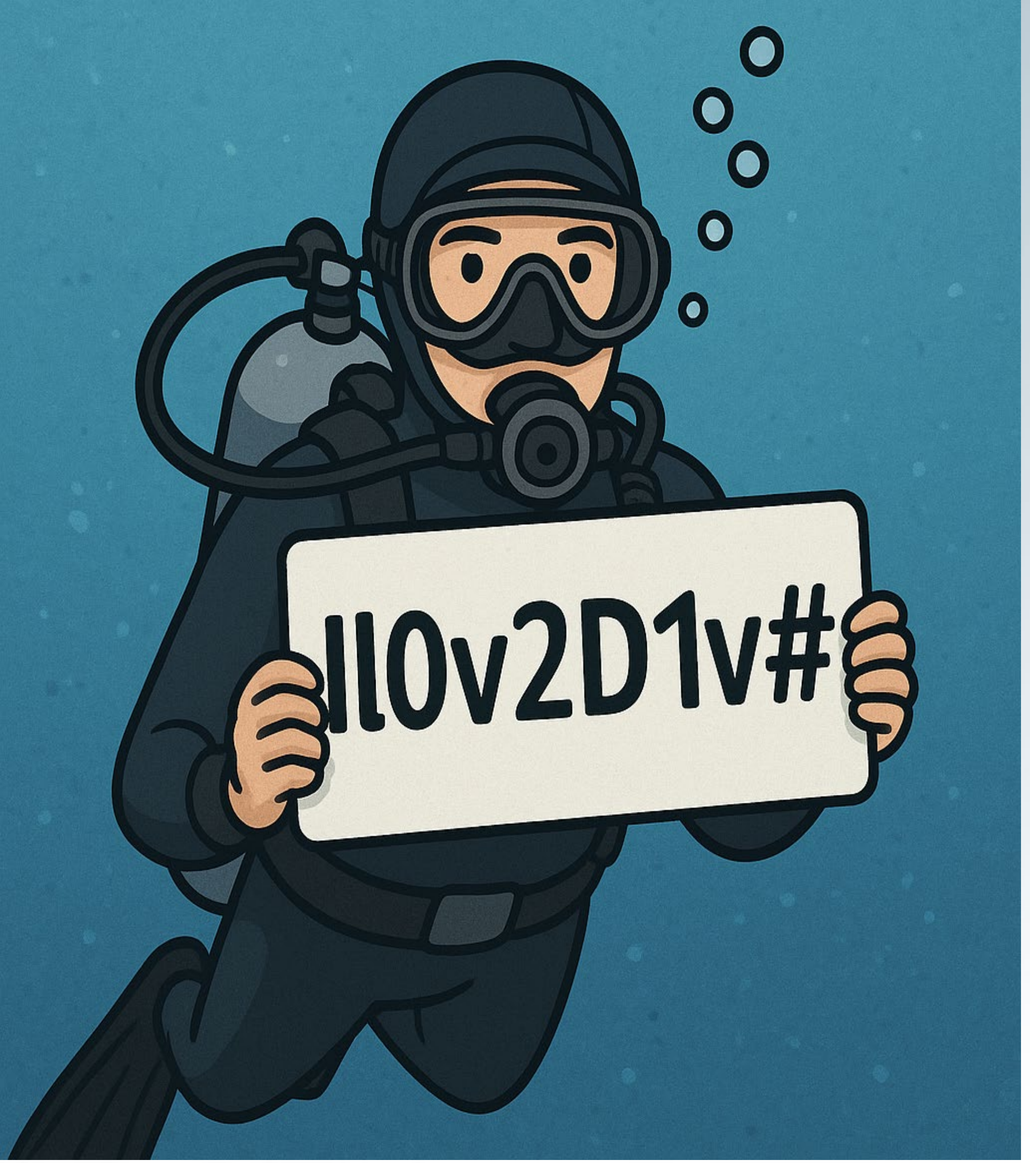
No predictable paths


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

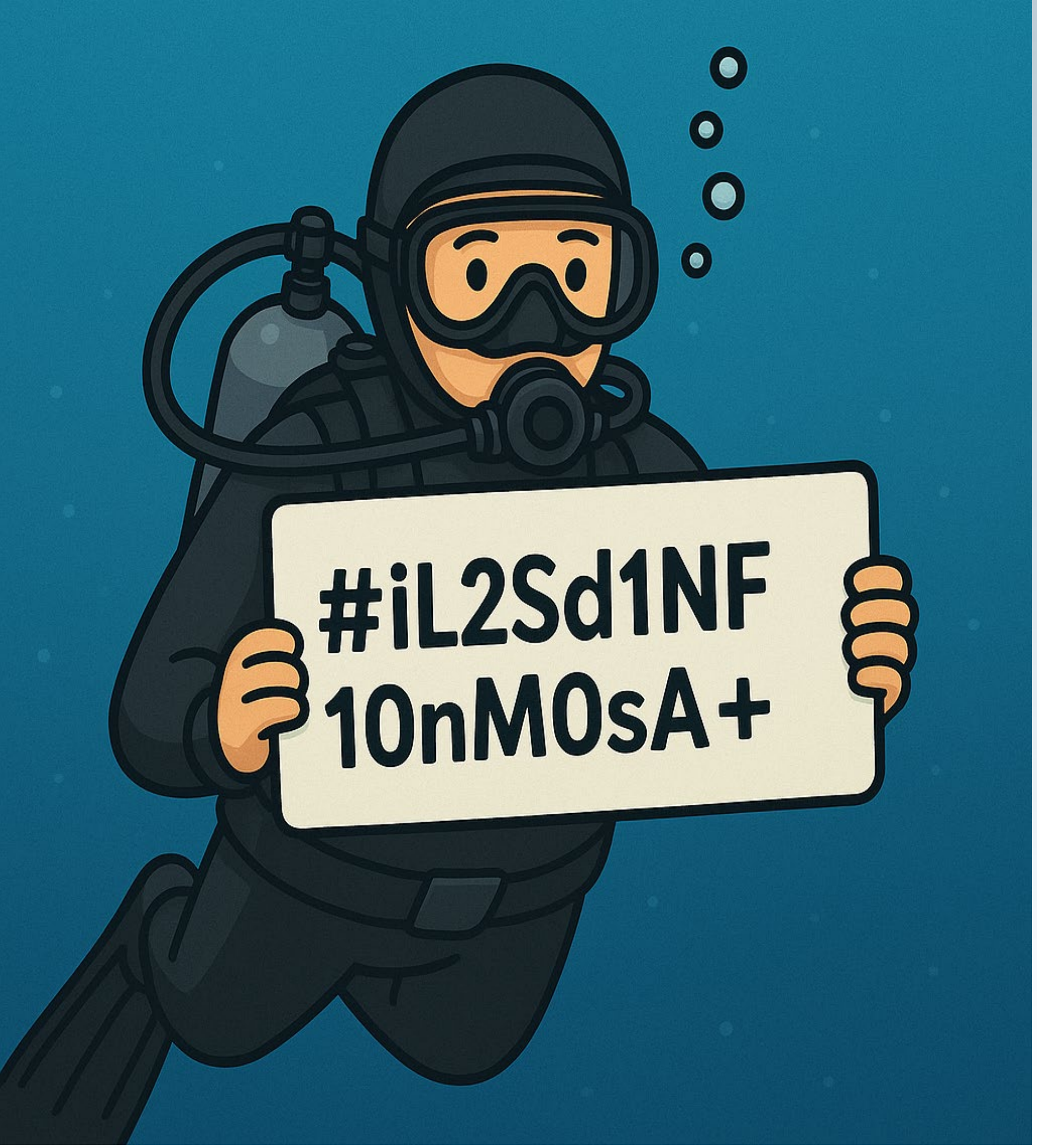

PASSWORD DON'TS
DON'T USE WIDELY KNOWN INFORMATION
DON'T WRITE DOWN PASSWORDS
DON'T SAVE PASSWORDS IN BROWSERS



WEAK



MODERATE



STRONG

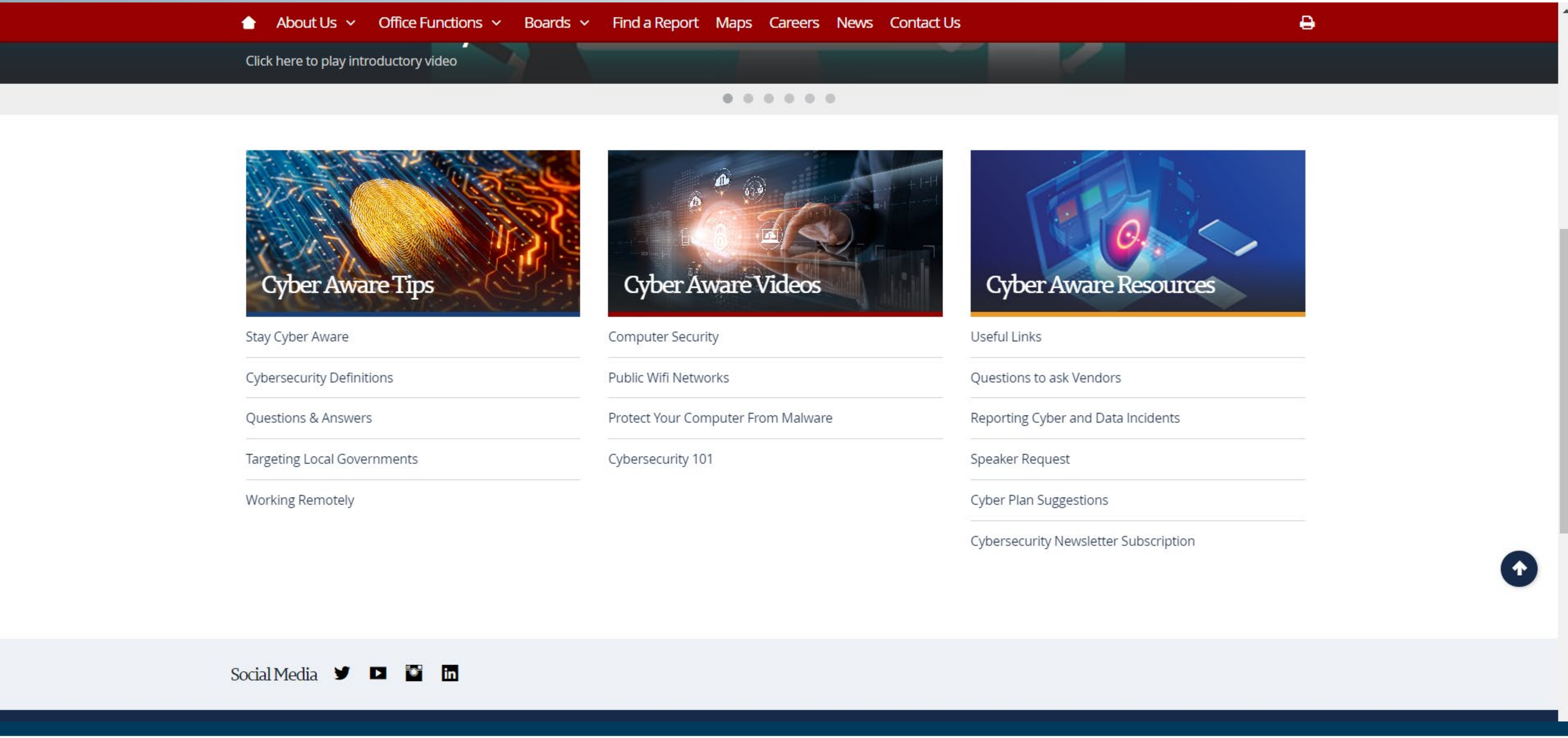
CREATE STRONG PASSWORDS
USE LONG, STRONG AND UNIQUE PASSWORDS
password
1234556
letmein

Other Important Protection Rules

Education

Security Awareness Training

TNCOT.CC/CYBERAWARE



Cyber Aware Tips

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

Cyber Aware Videos

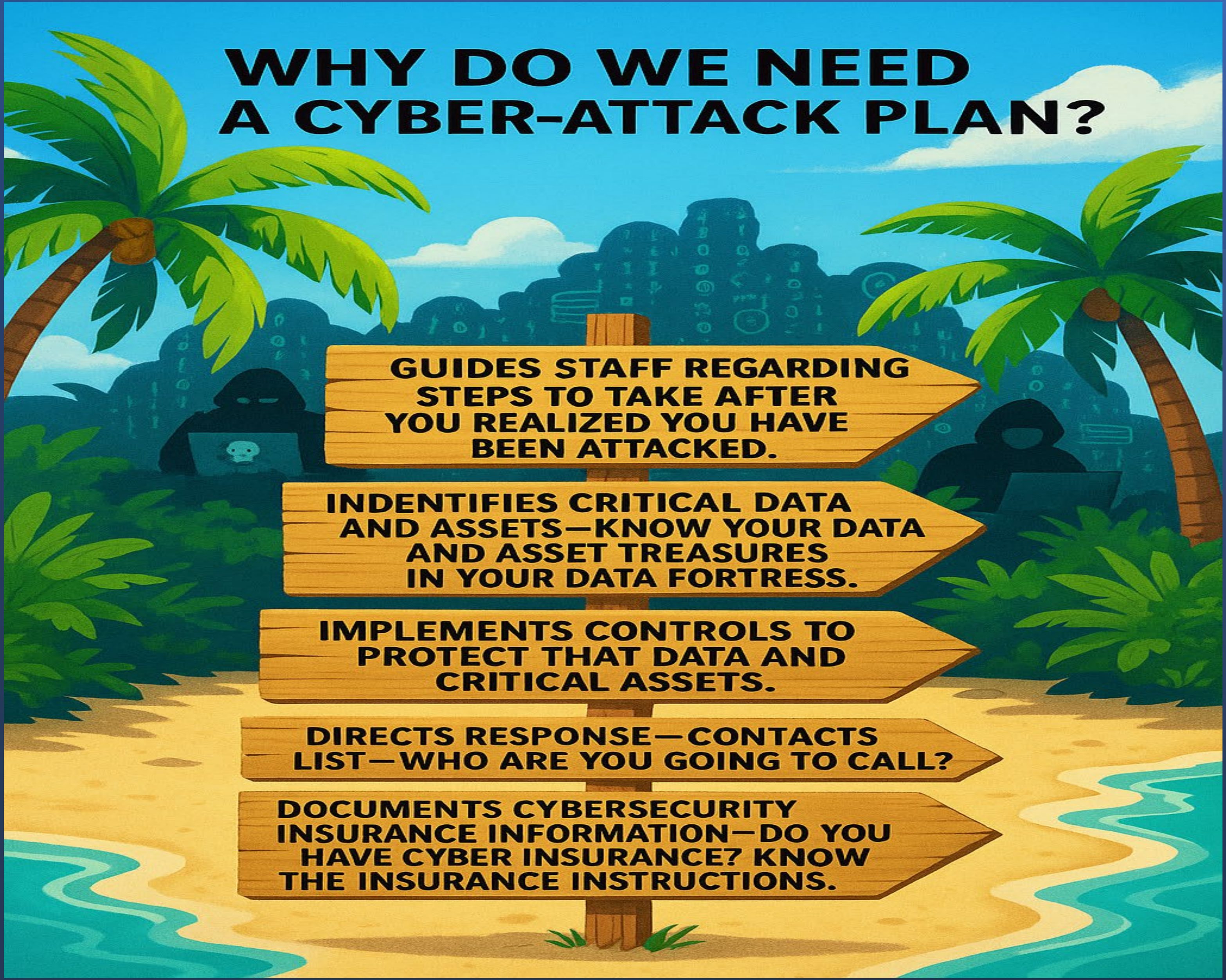
- Computer Security
- Public Wifi Networks
- Protect Your Computer From Malware
- Cybersecurity 101

Cyber Aware Resources

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

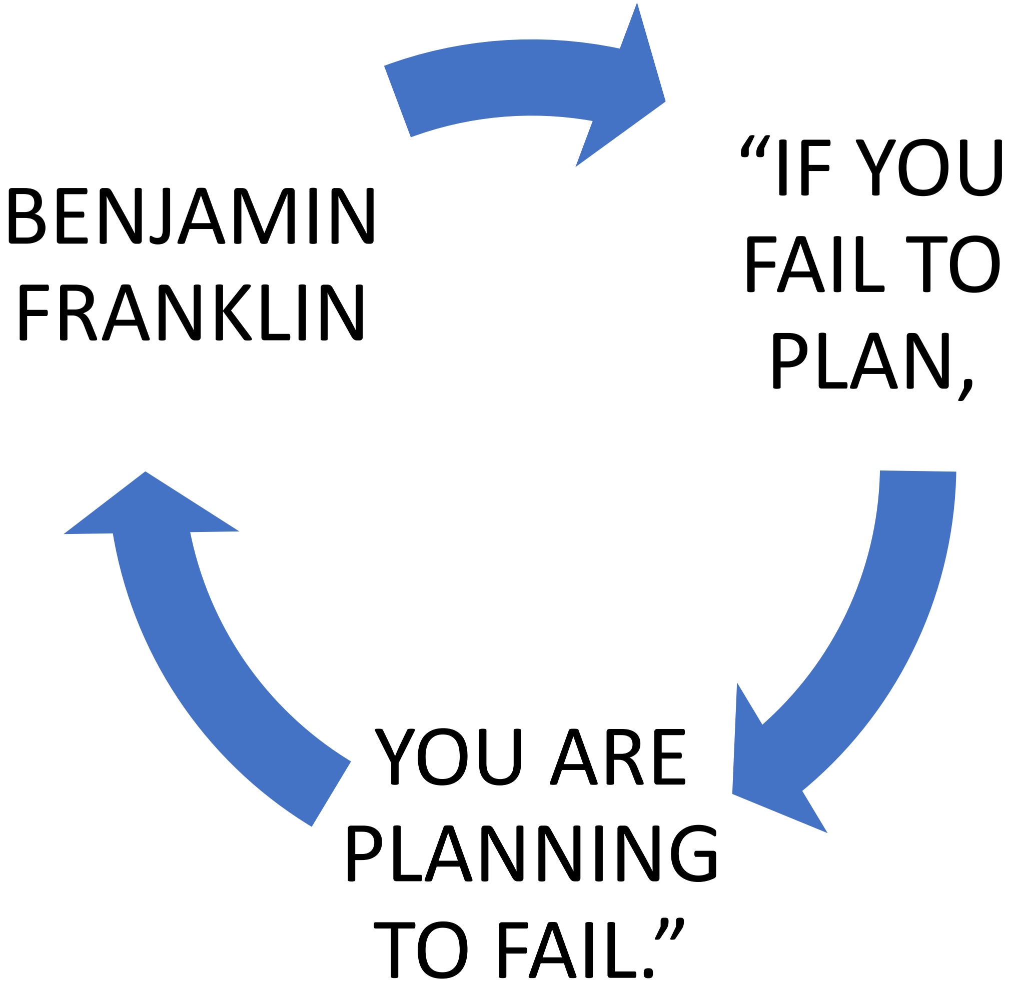
UNDERSTAND YOUR CYBERSECURITY POSTURE!
?
CYBERSECURITY POSTURE!

HAVE A PLAN!
PLAN
PLAN
CYBERSECURITY



WHY DO WE NEED A CYBER-ATTACK PLAN?

- GUIDES STAFF REGARDING STEPS TO TAKE AFTER YOU REALIZED YOU HAVE BEEN ATTACKED.
- INDENTIFIES CRITICAL DATA AND ASSETS—KNOW YOUR DATA AND ASSET TREASURES IN YOUR DATA FORTRESS.
- IMPLEMENTS CONTROLS TO PROTECT THAT DATA AND CRITICAL ASSETS.
- DIRECTS RESPONSE—CONTACTS LIST—WHO ARE YOU GOING TO CALL?
- DOCUMENTS CYBERSECURITY INSURANCE INFORMATION—DO YOU HAVE CYBER INSURANCE? KNOW THE INSURANCE INSTRUCTIONS.



BENJAMIN FRANKLIN

“IF YOU FAIL TO PLAN,

YOU ARE PLANNING TO FAIL.”

https://www.goodreads.com/quotes/460142-if-you-fail-to-plan-you-are-planning-to-fail

Conclusion

CIA TRIAD
CONFIDENTIALITY
INTEGRITY
AVAILABILITY

Protection Measures-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 Date 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

• 🌴 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 keys 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.

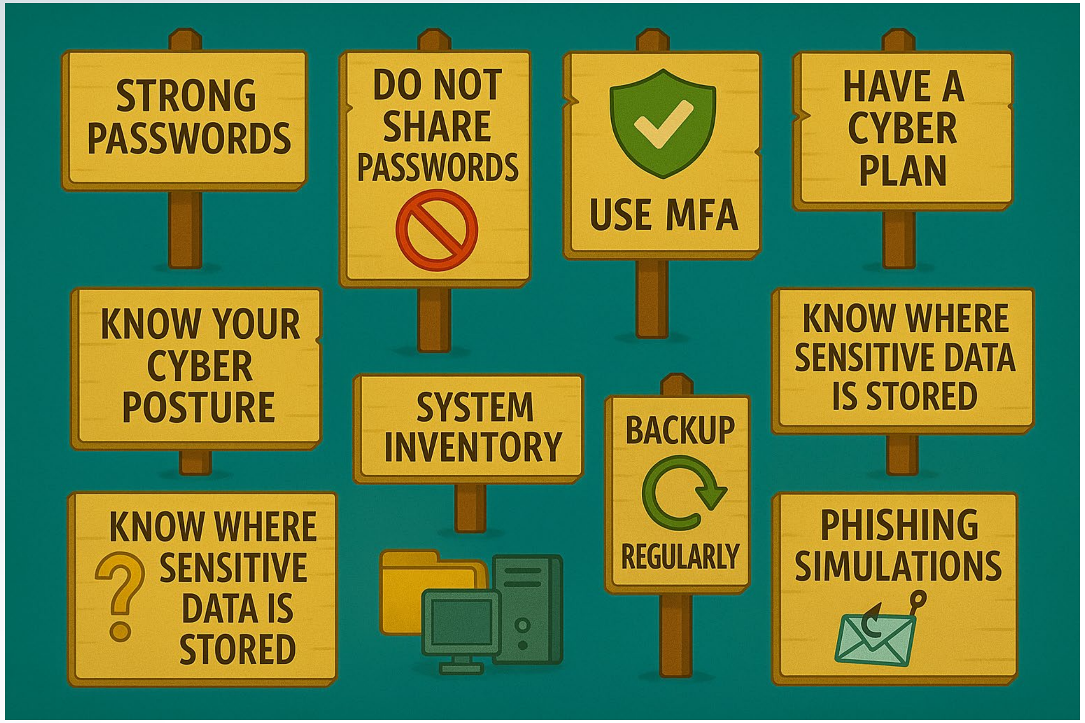
8. **Keep Operating Systems Updated**
🛠️ Patch those leaky beach huts.
.

9. **Backup Regularly**
☁️ Keep a lifeboat ready offshore.

10. **Run Phishing Simulations**
🎣 Practice spotting the fake bait.

10. **Be a Good Crew Member**
🧠 Stay alert, think before you click, and report anything suspicious.

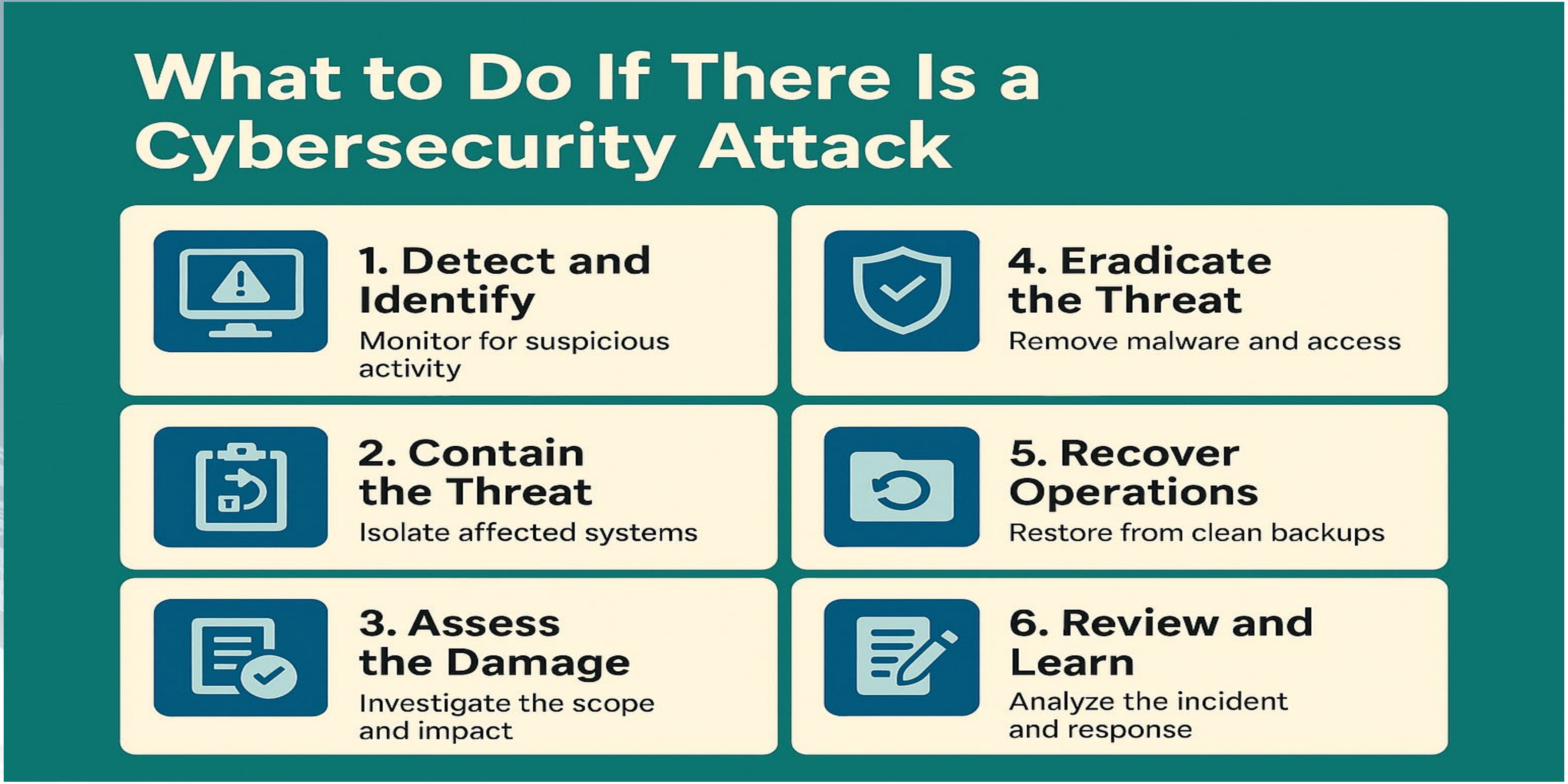
CYBERSECURITY TRAINING
UPDATE VIRUS PROTECTION AND ANTI-MALWARE
BACKUP REGULARLY



Data Island Safety Measures

Map Out the Island

ISLAND SECURITY MAP
Malware Mountain
Training Tower
CIA Triad Temple
Password Point
Password Point
Cybersecurity Mastery
Communication Enclave
Backup Beach
N
W
E
S



What to Do If There Is a Cybersecurity Attack

1. Detect and Identify
Monitor for suspicious activity

2. Contain the Threat
Isolate affected systems

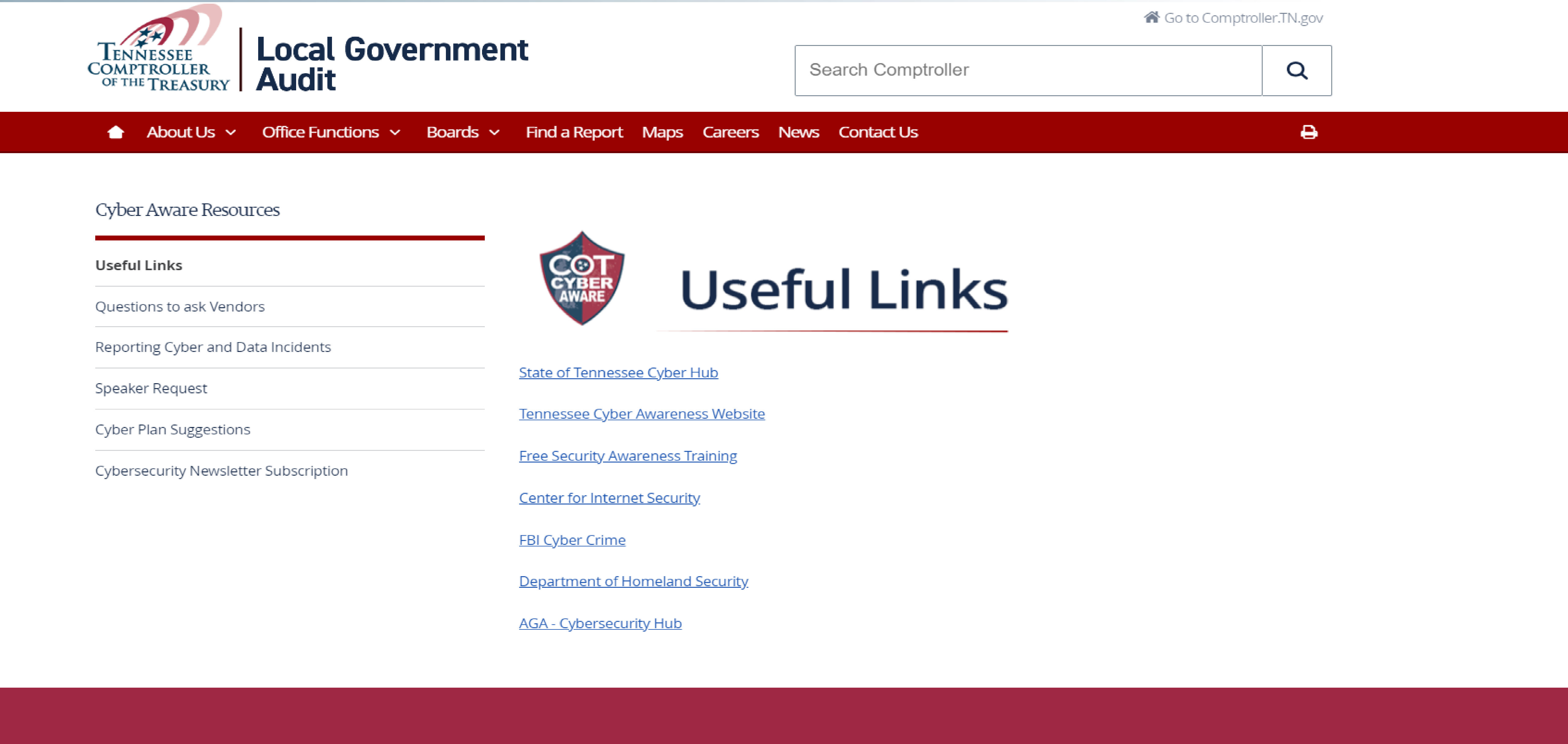
3. Assess the Damage
Investigate the scope and impact

4. Eradicate the Threat
Remove malware and access

5. Recover Operations
Restore from clean backups

6. Review and Learn
Analyze the incident and response

tncot.cc/cyberaware



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

Free Security Awareness Training

Center for Internet Security

FBI Cyber Crime

Department of Homeland Security

AGA - Cybersecurity Hub

Questions?

Barbara Shults

Barbara.Shults@cot.tn.gov

615-747-5359

tn.cot.cc/cyberaware