

BEC: More than Just Bacon, Egg and Cheese

Elisha Crowell, CISA, CFE
IS Audit Manager
Division of Local Government Audit
August 29, 2024



1

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.



2



3

About Us



Jason Mumpower
Comptroller



Jim Arnette
Director



4


IS Audit Team







5



**Division of
Local Government Audit**

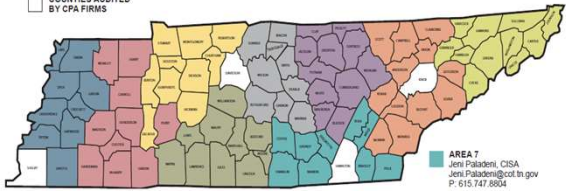
IS AUDIT ASSIGNMENTS

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 1
Rachel DePrest
Rachel.DePrest@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 7
Jeri Paladoni, CISA
Jeri.Paladoni@cot.tn.gov
P: 615.747.8804

AREA 8
Vacant

AREA 9
Shama Leonard
Shama.Leonard@cot.tn.gov
P: 615.401.7853

6

Objectives

- ❖ Definition
- ❖ How It Works
- ❖ Examples
- ❖ Impacts
- ❖ Prevention
- ❖ Response

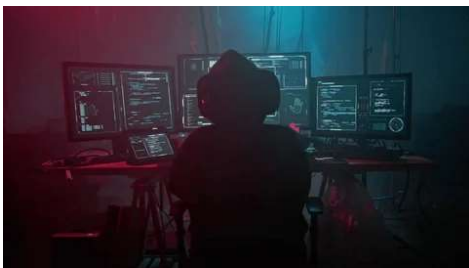


7



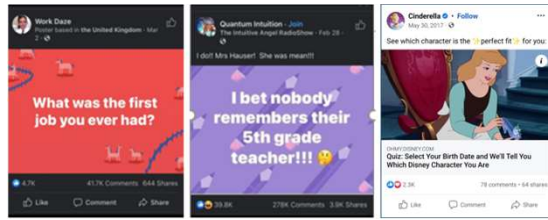
8

How We Think We Get Hacked



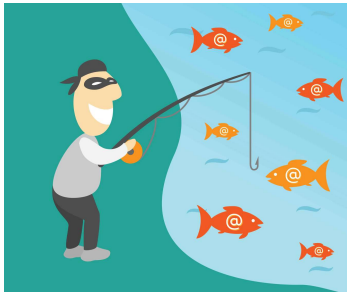
9

How We Really Get Hacked



10

Don't Take the Bait!



11

What is BEC?

- ⚙ **Business Email Compromise**
- ⚙ **A type of cybercrime where attackers gain access to business email accounts to steal sensitive information or funds.**



12

13

14

15

Real-World Example

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

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



16

From: Donna Craig (clerkoffice1@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

17

BEC 101

- **OBSERVE**
 - Do you know the sender?
 - Did you expect the email?
 - Did you expect the attachment?
- **INVESTIGATE**
 - Sender address an alias?



18

From: Donna Craig (clerkoffice1@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

19

BEC 101

⚙ OBSERVE

• Do you know the sender?

• Did you expect the email?

• Did you expect the attachment?

⚙ INVESTIGATE

• Sender address an alias?

• Typos or unusual tone?

• Sense of urgency?

• Where do the message links go?

⚙ DEDUCE

• Call the individual to verify

• Any doubts, report it

TENNESSEE

COMPTROLLER

OF THE TREASURY

20

Letter Received

JH

Jasmine Hodge <Jasmine.Hodge@tn.gov>

To

Elisha Crowell

This sender Jasmine.Hodge@tn.gov is from outside your organization.

1011_001.pdf

153 KB

1012_001.pdf

25 KB

Good morning,

Please see attached. This was received at my office.

Thank you

TN

Department of

Human Services

Jasmine Hodge | Administrative Services Assistant 2

Office of Inspector General, Program Integrity

James K. Polk, 14th Floor

505 Deaderick Street, Nashville, TN 37243

phone: 615-741-5939

jasmine.hodge@tn.gov

tn.gov/humanservices

TENNESSEE

COMPTROLLER

OF THE TREASURY

21

7

PREMIUM

CITY OF MEMPHIS

Phishing scam in 2022 cost Memphis taxpayers \$773K

By Samuel Hernandez, Daily Memphian Updated: July 17, 2024 9:43 AM CT | Published: July 17, 2024 6:00 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. 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.

TENNESSEE

COMPTROLLER

OF THE TREASURY

22

Impact of BEC

- ❖ **Financial Loss: Direct theft of funds**
- ❖ **Reputational Damage: Loss of trust among citizens and partners**
- ❖ **Legal and Regulatory Penalties: Fines for non-compliance**
- ❖ **Operational Disruption: Costs related to investigation and remediation**

TENNESSEE

COMPTROLLER

OF THE TREASURY

23

How to Prevent BEC

- ❖ **Strong Passwords**


TENNESSEE

COMPTROLLER

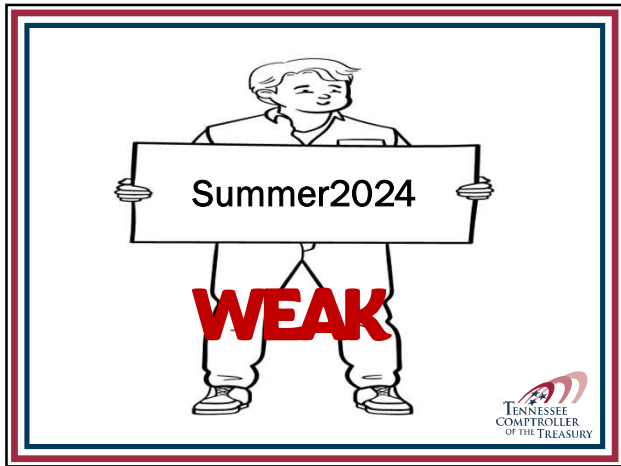
OF THE TREASURY

24

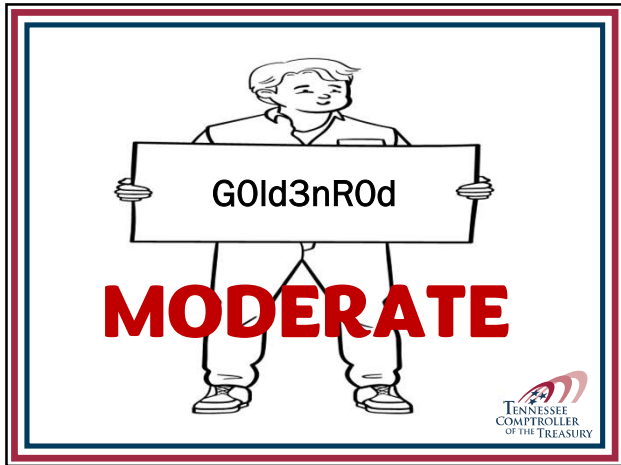
| TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024 | | | | | |
|---|--------------|-------------------|-----------------------------|--------------------------------------|---|
| Hardware: 12 x RTX 4090 Password hash: bcrypt | | | | | |
| Number of Characters | Numbers Only | Lowercase Letters | 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 |

 [Learn more about this at hivesystems.com/password](https://hivesystems.com/password)

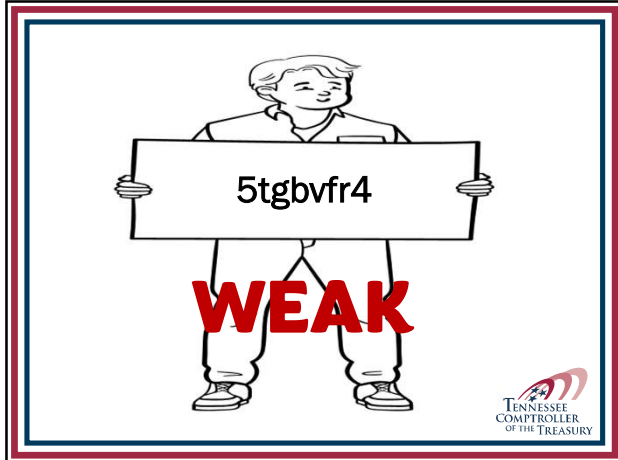
25



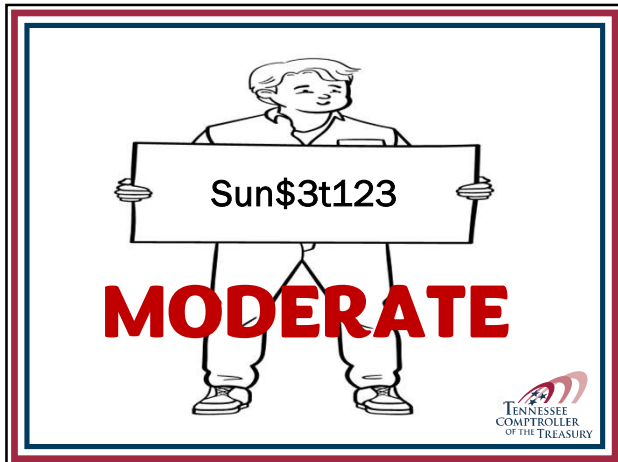
26



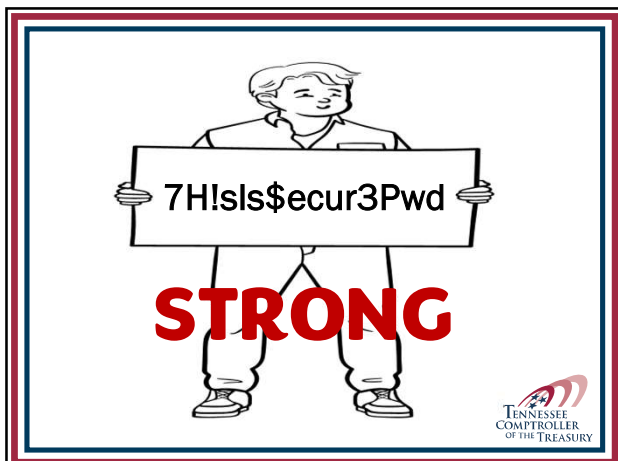
27



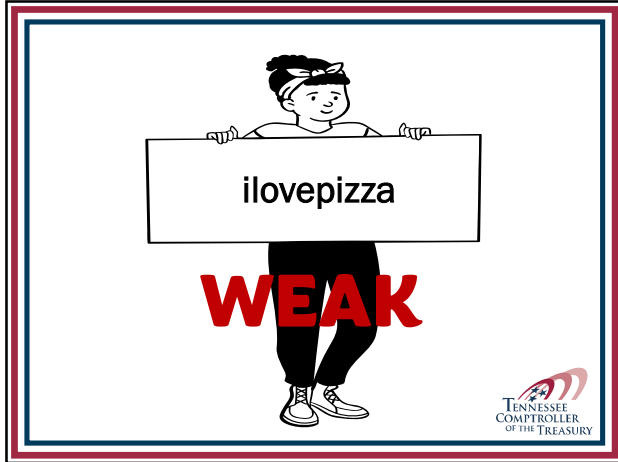
28



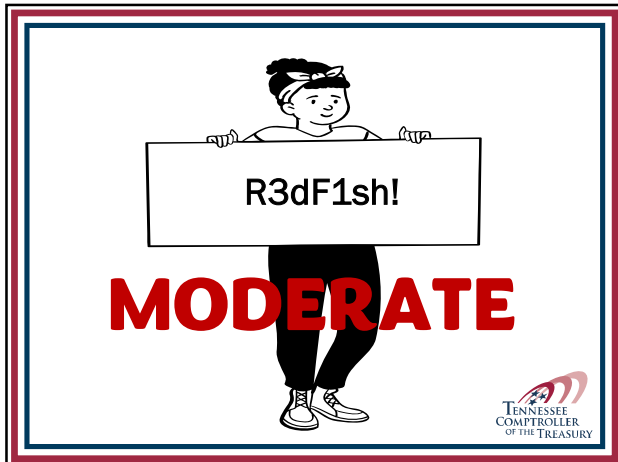
29



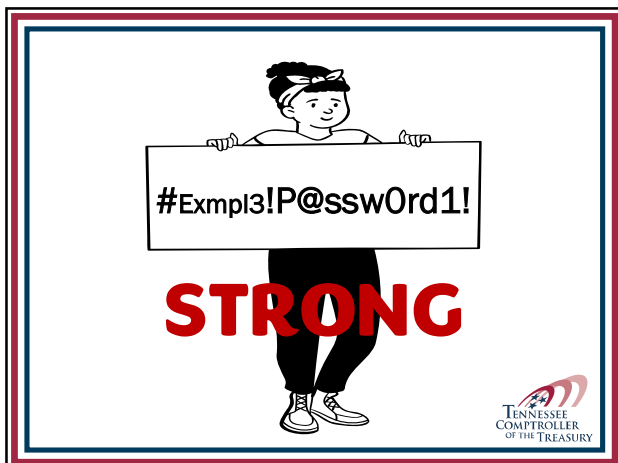
30



31



32



33



34



35

Passwords – Dos and Don'ts

| DO | DON'T |
|--|---|
| <ul style="list-style-type: none"> ⚙ Use different passwords for all accounts ⚙ Change passwords regularly ⚙ Create strong, memorable passwords | <ul style="list-style-type: none"> ⚙ Don't use widely known information ⚙ Don't write down and "hide" your password ⚙ Don't save passwords in browsers |


36



37

Password Creation Tip

- **Nine people floating the Snake River**
- **Step 1: Remove spaces and add uppercase letters**
 - **NinePeopleFloatingTheSnakeRiver**
- **Step 2: Add special characters and numbers**
 - **(9PplFloatingSN@K3River)**



38

How to Prevent BEC

- **Multi-factor authentication**




39



40



41



42

Responding to a BEC Incident




 TENNESSEE
 COMPTROLLER
 OF THE TREASURY

43

Questions?

Elisha Crowell
IS Audit Manager
 Local Government Audit
 615-747-8806
Elisha.Crowell@cot.tn.gov


 TENNESSEE
 COMPTROLLER
 OF THE TREASURY

44
