Fortifying Your **Data**

Practical Ways to Create an Army using Awareness

Almando Cox M.Sc., ITIL

Getting **Ready**

- Rules
- Promise

Our **Agenda**

- Exercise #1
- In the News
- Why are the bad actors winning?
- What are they doing?
- Examples of attacks
- Important Terms to Know
- How can we fortify?
- Bonus - Checklist
- Exercise #2

Exercise #1

BSJ Hit by CYBERATTACK

BARBADOS

NESS ARTS & CULTURE

FSC leak

0 Comments · Make a comment

September 17, 2023

THE

Jonathan Greig

December 27th, 2023

EE NEWSLETTER

Magazine D

News Briefs

Government

Cybercrime

Media Kit

Home » Firew:

Cybe

Strik

ip

The victim

cial medical

entity in tl

by thecyberexpress

Get more insights with the Recorded Future Intelligence Cloud.

Trinidad and Tobago social security agency hit with post-Christmas ransomware attack

A key government agency in Trinidad and Tobago said it was hit with a ransomware attack that will limit its operations for at least the rest of the year.

The country's National Insurance Board (NIBTT) — which runs the nation's social security system serving more than 630,000 people — wrote that all offices will be closed from Wednesday to Friday due to a recently-discovered ransomware attack.

"The company is currently assessing our systems after having experienced a ransomware attack on Tuesday, December 26. All steps are being taken to protect our data integrity and technology hardware," NIBTT said in social media messages to the public.

The FSC has confirmed that it was the victim of a ransomware attack which has resulted in some files being published on the dark web.

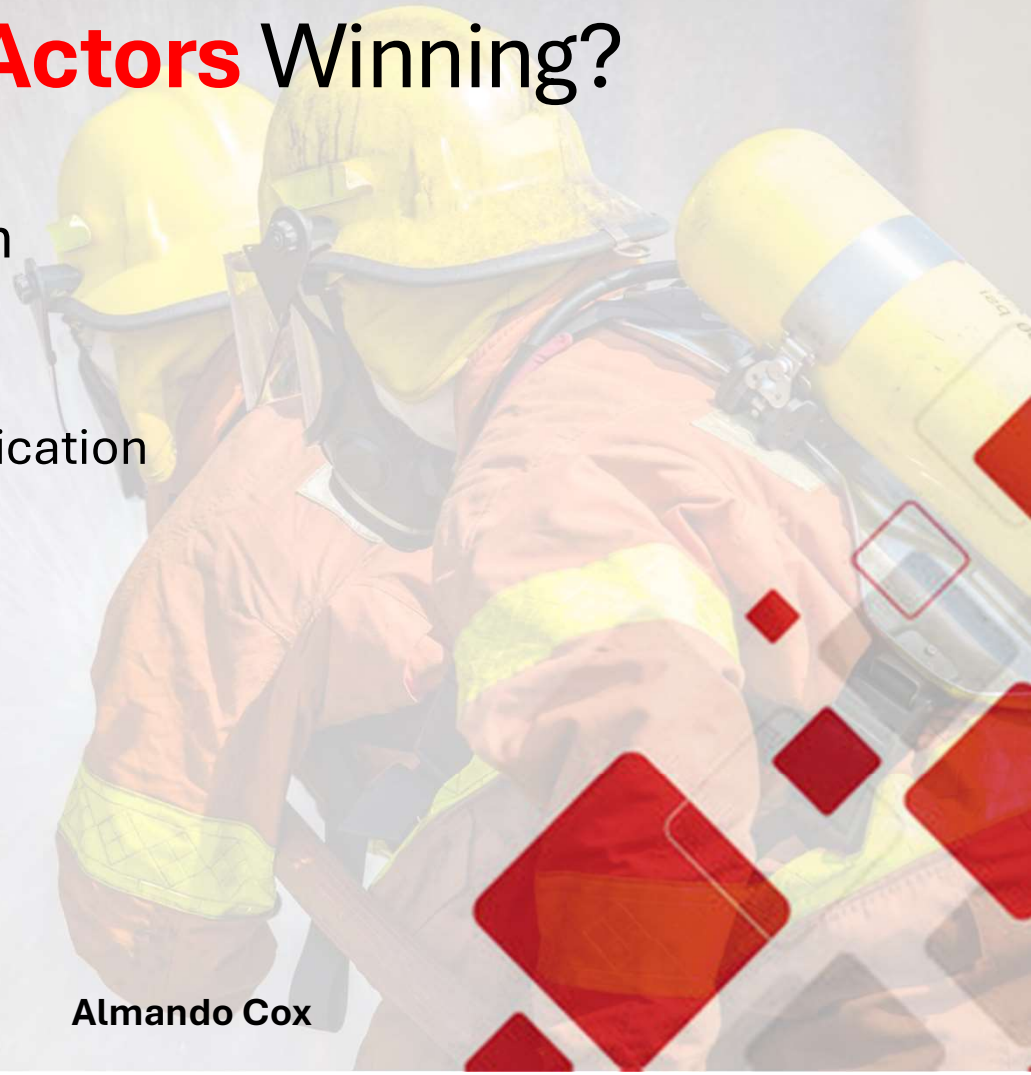
ces

s

run agency to be hit by a cyberattack that has affected some aspects of the entity's service delivery.

Why are **Bad Actors** Winning?

- Information System
  - ✓Hardware
  - ✓Software
  - ✓Network Communication
  - ✓Data
  - ✓Process
  - ✓**People**



Why are **Bad Actors** Winning?

Forbes

connect.comptia.org/content/articles/the-cost-of-a-breach-10-terrifying-cybersecurity-stats-your-msp-s-customers-need-to-know

Thinl

Wha

How
work

Type
attac

most

is thr

95%

of Breaches are Caused by Human Error

Source: Cybint

The global information security market is forecasted to reach $170.4 billion in 2022, according to Gartner. And while that number is so large it's hard to wrap your head around it, here's another stat that might hit closer to home. According to Cybint, 95% of cybersecurity breaches are caused by human error, meaning they were likely preventable. Yes, you read that right. Would that catch your customer's attention?

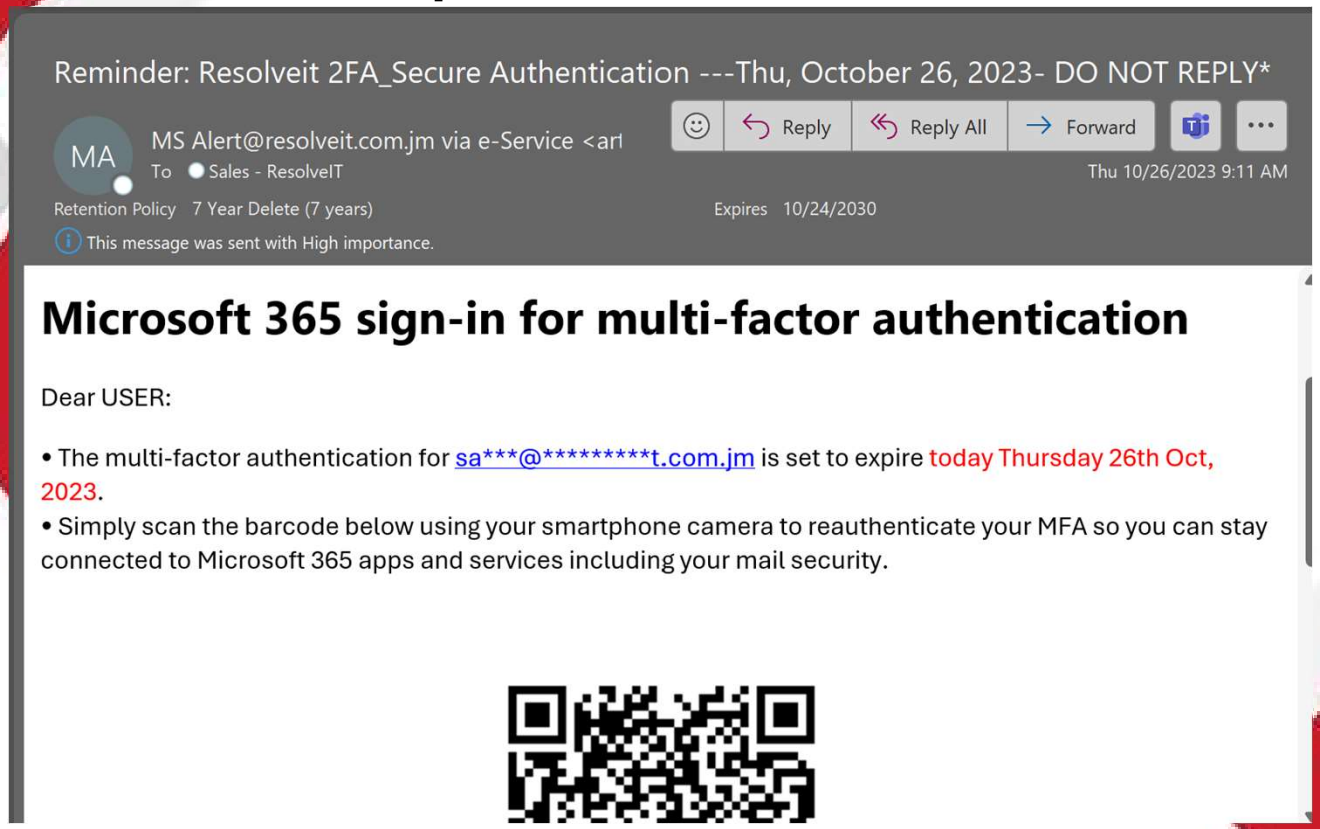
k of
ne
).
ıe

What are they doing ☹?

- Impersonate senders
- Create urgency
- Appeal to your emotions
- Provide links to download malware
- Provide link with fake forms
- Set baits

[redacted]

Example of an attack #1



Reminder: Resolveit 2FA_Secure Authentication ---Thu, October 26, 2023- DO NOT REPLY*

MA

MS Alert@resolveit.com.jm via e-Service <arl

To Sales - ResolveIT

Reply | Reply All | Forward

Thu 10/26/2023 9:11 AM

Retention Policy 7 Year Delete (7 years)

Expires 10/24/2030

This message was sent with High importance.

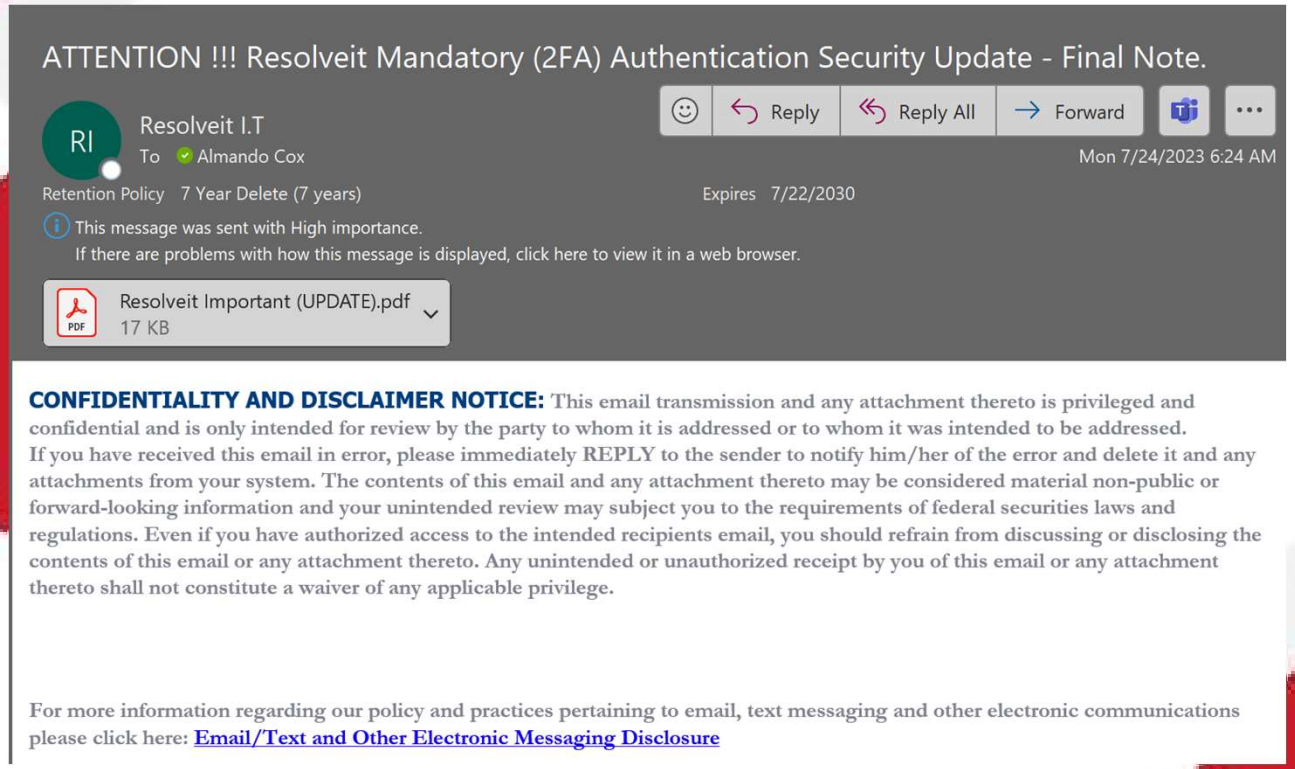
Microsoft 365 sign-in for multi-factor authentication

Dear USER:

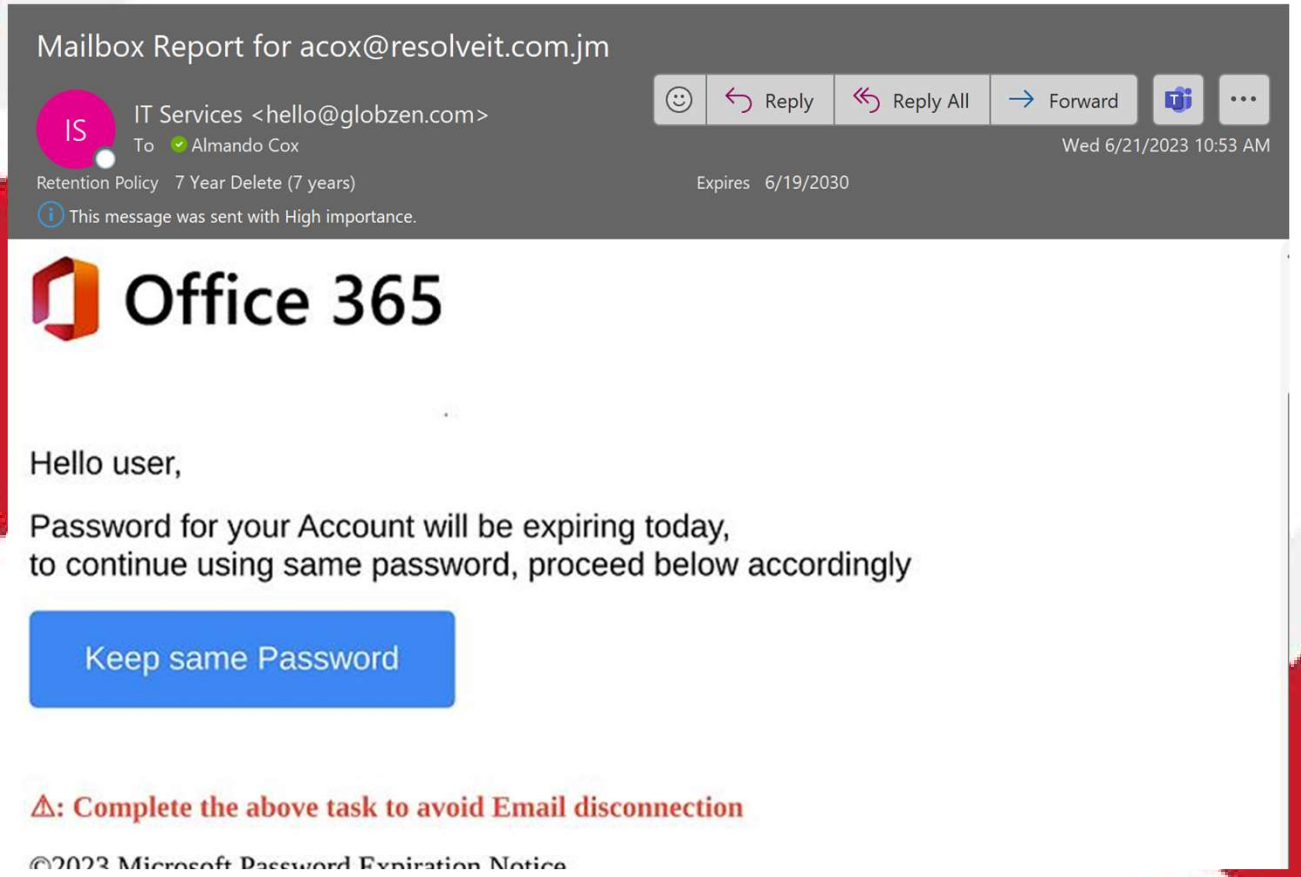
• The multi-factor authentication for sa***@*********t.com.jm is set to expire today Thursday 26th Oct, 2023.

• Simply scan the barcode below using your smartphone camera to reauthenticate your MFA so you can stay connected to Microsoft 365 apps and services including your mail security.

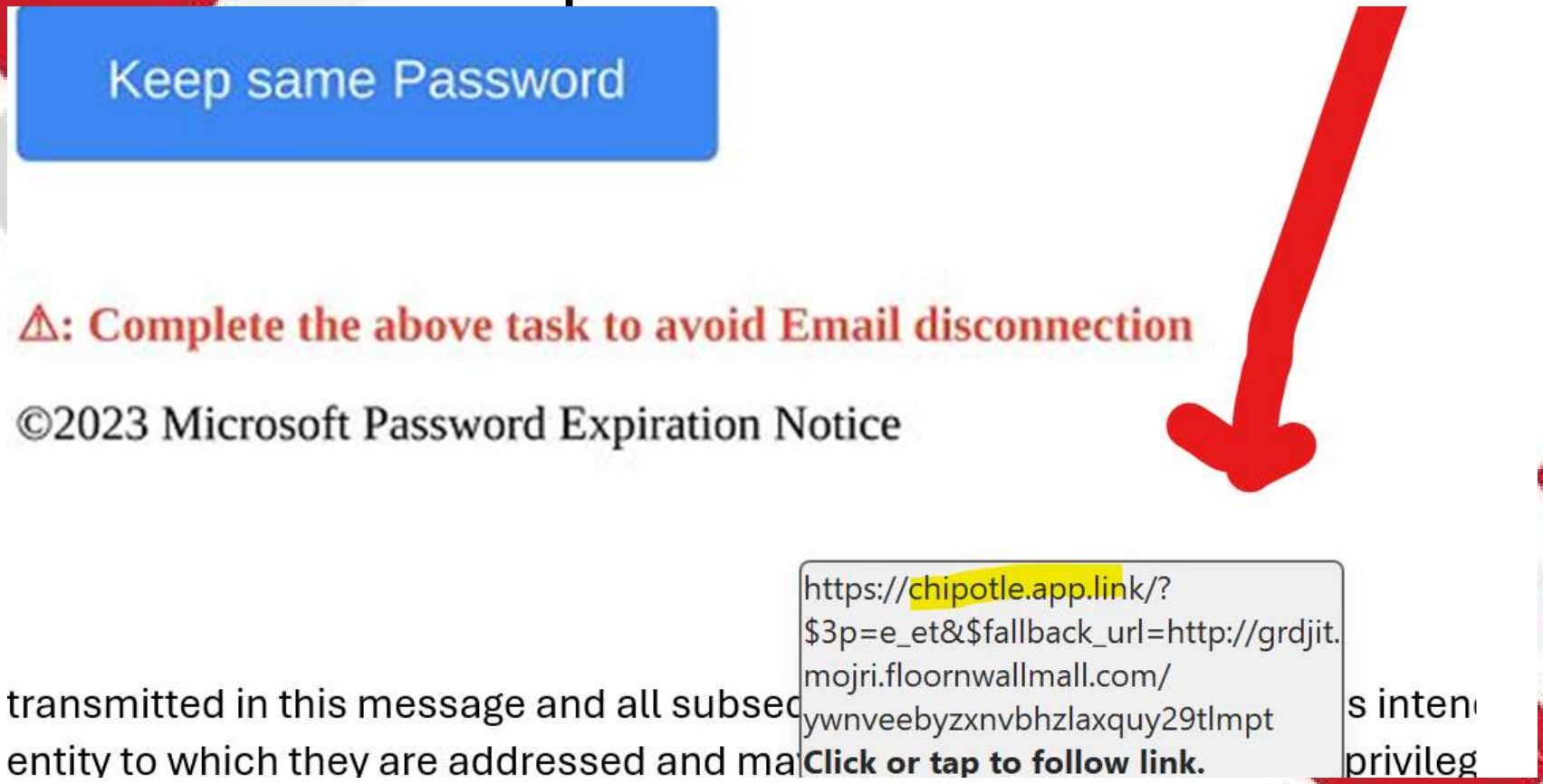
Example of an attack #2



Example of an attack #3



Example of an attack #3



Important **Terms to Know**

- Cyber Security
- Social Engineering
- Cyber Security Awareness

Get to Know these Terms

- Cyber Security
  - Proactive steps to prevent unauthorized access

Get to Know these Terms

- Social Engineering
  - Attackers exploit human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security.

Get to Know these Terms

- Cyber Security Awareness
  - Proactive measures aimed at educating end users on responsible use of information and communication technology, while also empowering them to protect themselves against cyber threats.

How can we **Fortify**?

1. Create a cyber security awareness training program
2. Mandate training (e.g. orientation)
3. Include cyber security awareness in performance appraisal
4. Conduct routine simulations

How can we **Fortify**?

5. Mandate multi-factor authentication
6. Use password manager
7. Use Single-Sign-On (SSO)
8. Create an incident response plan (IRP)
9. Create a backup and disaster recovery plan (BDRP)

Secret Sauce - **Culture of Security**

- Leadership commitment
- Encourage open communication channels
- Encourage incident reporting.
- Continuous Education and Training
- Reward Secure Behavior
- Empower employees with tools and technologies

Bonus – Fortifying Checklist

- ❑Vulnerabilities Assessment & Remediation
- ❑Implementing Security Measures
- ❑Creating a Culture of Security
- ❑Backup & Disaster Recovery Planning
- ❑Incident Response Planning
- ❑Testing & Simulation

Exercise #2

RESOLVE IT

This is your desktop

CCCU ANNUAL INTERNATIONAL CONVENTION
JUNE 21 - 26, 2024

Fortifying Your Data

Almando Cox

Are you **Ready for Duty**?

RESOLVE IT

Almando Cox | CEO

876-368-2154

acox@resolveit.com.jm

ResolveIT Limited

www.resolveit.com.jm

Schedule Time with Us

RESOLVE IT

http://bit.ly/3Cs7zbv