Cybersecurity

THREATS & MITIGATIONS FOR GOVERNMENT ACCOUNTING PROFESSIONALS

Agenda

- Disclaimers
- Objectives
- Top Threats to Individuals & Companies
- Top New Threats
- Examples
- Best Practices & Summary
- Q&A

Disclaimers

- I am <u>not</u> a licensed cybersecurity professional
- My experience and research
- This is a highly dynamic environment
- You will have homework
- I will include a pointless pie chart

Objectives

- Enhance Awareness of Evolving Cyber Threats
- Deepen Understanding of Targeted Attack Vectors
- Identify and Implement Effective Defense Mechanisms
- Promote Cyber Hygiene Best Practices
- Empower Attendees to Apply Knowledge Practically

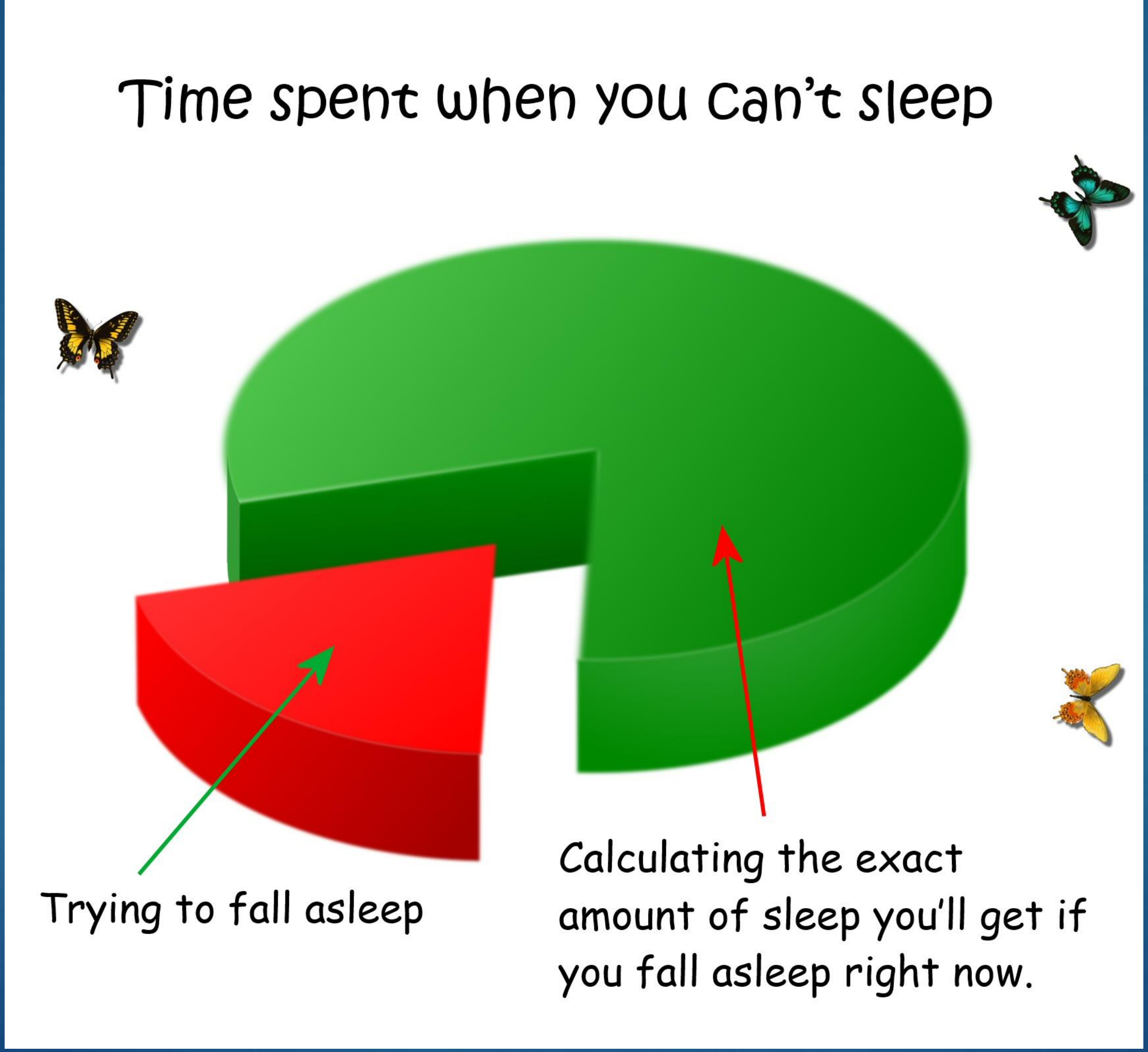
Top Threats to Individuals

- Phishing and Social Engineering
  - Mitigations: Awareness Training, Verification Steps, Use Anti-Phishing Tools
- Malware
  - Use Reliable Antivirus Software, Regular Updates to OS and applications, Avoid Suspicious Links and Downloads
- Ransomware
  - Regular Backups, stored offline, Training on phishing, Endpoint Protection Solutions
- Mobile Device Vulnerabilities
  - Use Multi-Factor Authentication (MFA), Only Download Apps from Trusted Sources, Use Secure Networks or VPNs
- Man-in-the-Middle
  - Use Encrypted Connections (HTTPS), Avoid Public Wi-Fi for Sensitive Transactions, Use VPN Services

Top Threats to Companies

- All of the Above
- <u>Supply Chain Attacks</u>
  - Vendor Risk Management, Network Segmentation, Continuous Monitoring
- <u>Insider Threats</u>
  - Access Control based on roles, Employee Monitoring, Regular Audits

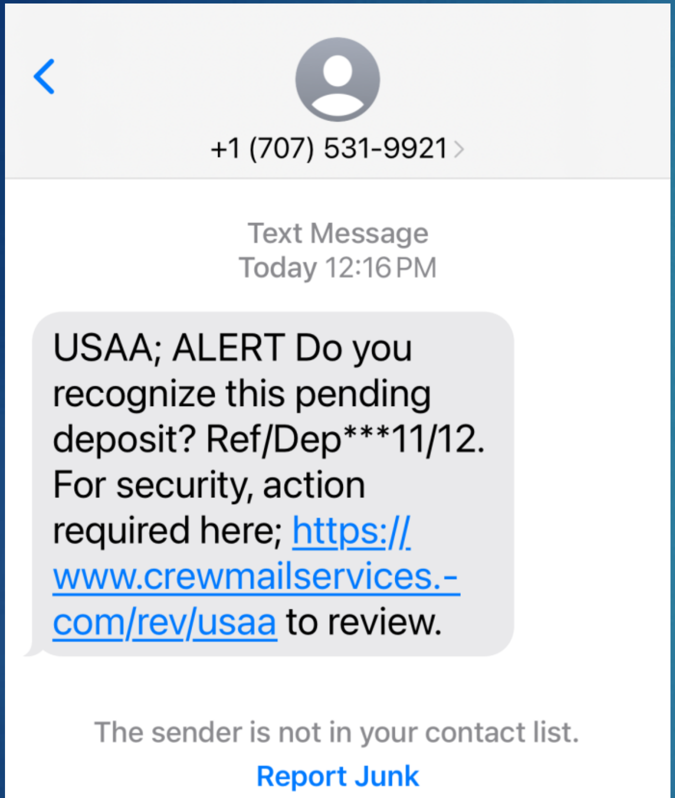
Pointless Pie Chart



Top New Threats

- Advanced Persistent Threats (APTs)
  - Network Security Measures, Patch Management and Vulnerability Mitigation, Access Control and Privilege Management
- Identity-Based Threats
  - Strong Authentication (MFA), Regular Identity Verification, Zero Trust Security Model
- Evolving Social Engineering Tactics
  - Continual Training on new tactics, Behavioral Analysis Tools, Enhanced Communication Verification
- AI-Driven Attacks
  - Enhanced Security Training, Advanced Detection Tools with AI, Regular System Updates

Examples

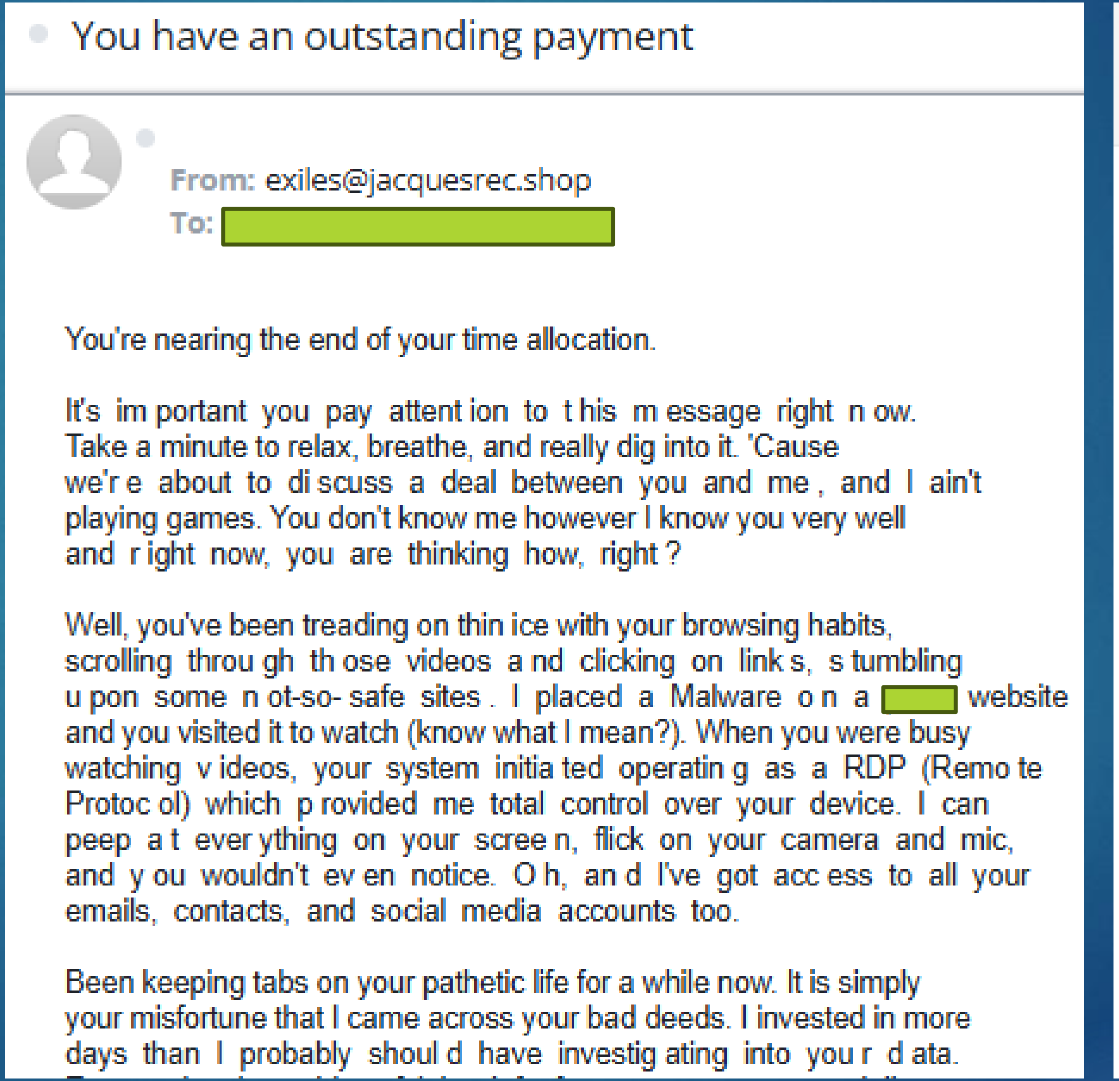

+1 (707) 531-9921

Text Message
Today 12:16 PM

USAA; ALERT Do you recognize this pending deposit? Ref/Dep***11/12. For security, action required here; https://www.crewmailservices.-com/rev/usaa to review.

The sender is not in your contact list.

Report Junk


You have an outstanding payment

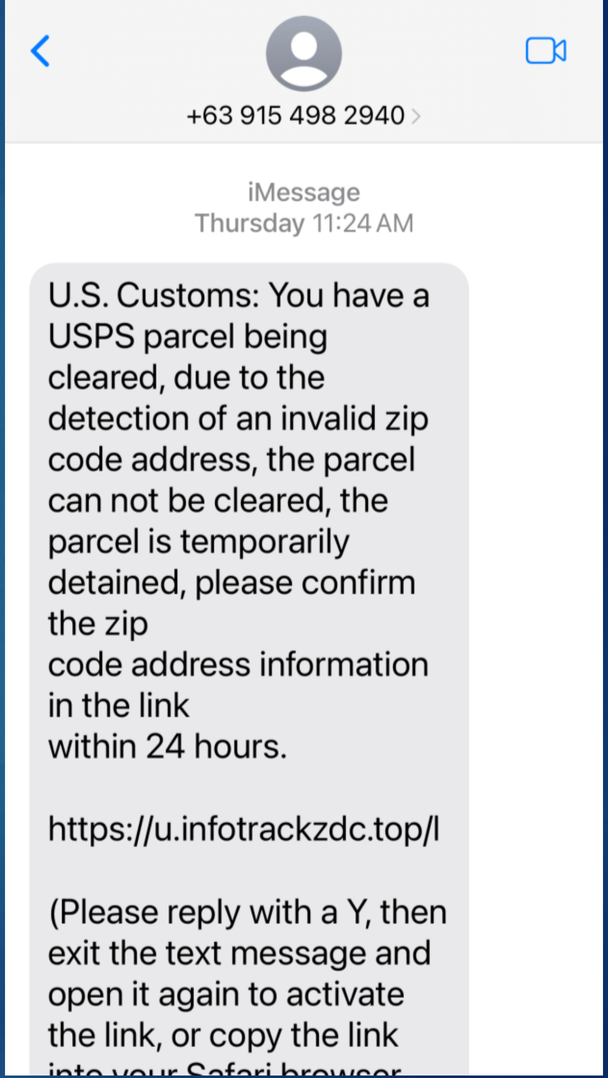
From: exiles@jacquesrec.shop
To: [redacted]

You're nearing the end of your time allocation.

It's important you pay attention to this message right now. Take a minute to relax, breathe, and really dig into it. 'Cause we're about to discuss a deal between you and me, and I ain't playing games. You don't know me however I know you very well and right now, you are thinking how, right?

Well, you've been treading on thin ice with your browsing habits, scrolling through those videos and clicking on links, stumbling upon some not-so-safe sites. I placed a Malware on a [redacted] website and you visited it to watch (know what I mean?). When you were busy watching videos, your system initiated operating as a RDP (Remote Protocol) which provided me total control over your device. I can peep at everything on your screen, flick on your camera and mic, and you wouldn't even notice. Oh, and I've got access to all your emails, contacts, and social media accounts too.

Been keeping tabs on your pathetic life for a while now. It is simply your misfortune that I came across your bad deeds. I invested in more days than I probably should have investigating into your data.


+63 915 498 2940

iMessage
Thursday 11:24 AM

U.S. Customs: You have a USPS parcel being cleared, due to the detection of an invalid zip code address, the parcel can not be cleared, the parcel is temporarily detained, please confirm the zip
code address information
in the link
within 24 hours.

https://u.infotrackzdc.top/l

(Please reply with a Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser

Best Practices

- Be suspicious and alert
- Regular Training on the latest tactics
- Up-to-date Detection/Prevention Software
- Multi-Factor Authentication (MFA)
- Endpoint and Network Security
- Backups and Data Protection
- Continuous Monitoring

Summary

- Cyber threats require *proactive* and *adaptive* security measures
- Greatest risk → Carelessness
- Human Awareness – Auditor Mentality
- Homework: Find and report a threat

Q&A

Thank You!

TRAILBOSS@THEDATACOWBOY.TECH (WORK)

ANDREWMCLEANGIBBS@GMAIL.COM (NON-WORK)

HTTPS://WWW.LINKEDIN.COM/IN/ANDREWMGIBBS/

The Data Cowboy LLC delivers tangible value to clients by providing decades of data and technology expertise combined with timeless cowboy values.

Our Services:

- Data & AI Consulting
- Program Management
- Keynote Speaking
- Professional Education

TDC™

The Data Cowboy™