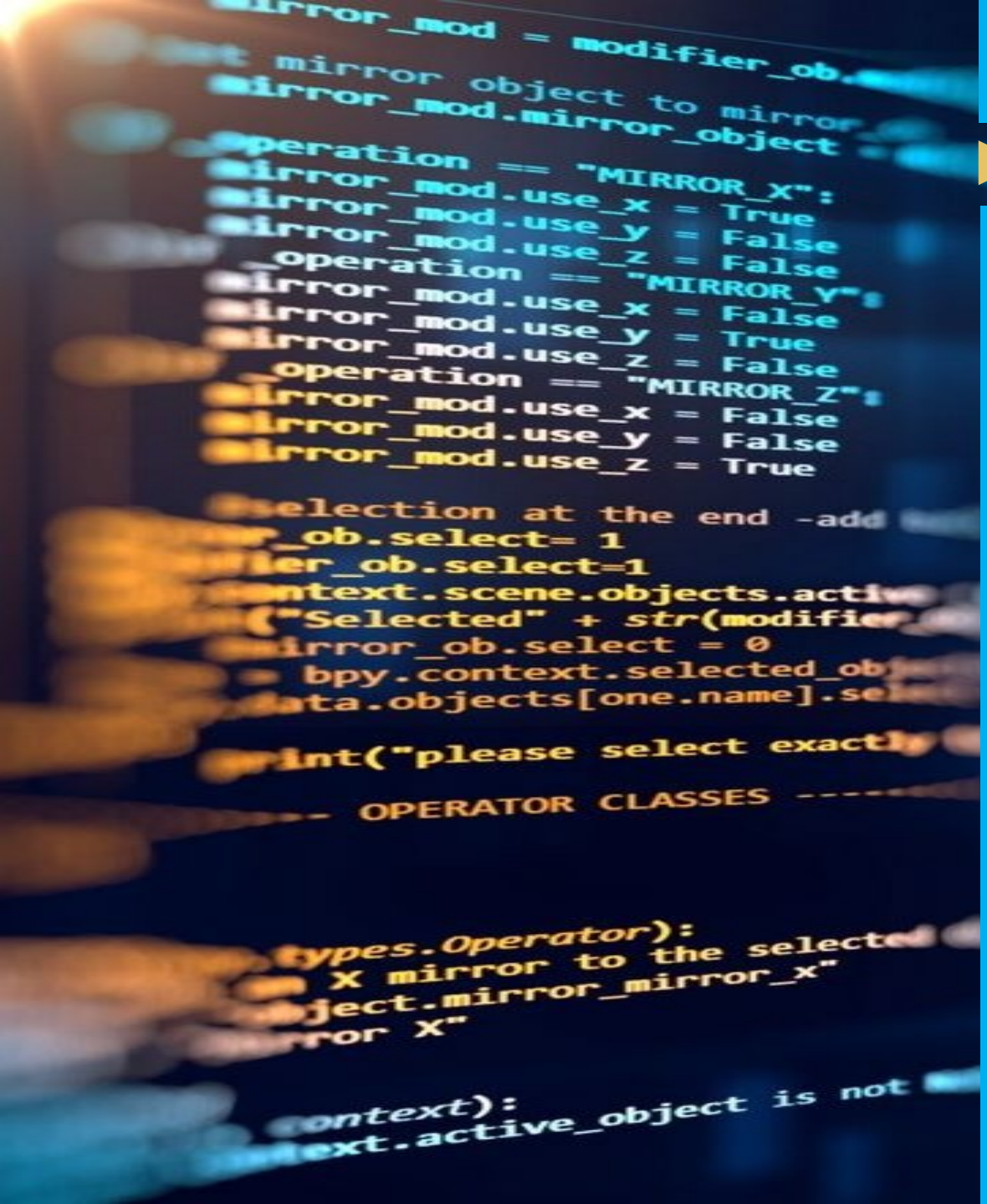


AN OFFERING IN THE BLUE CYBER SERIES

Protecting Against Social Engineering and Phishing

By Anna Etheron

Cybersecurity & Infrastructure Security Administration

26 September 2023

BLUE CYBER EDUCATION SERIES

Protecting Against Social Engineering and Phishing

A simple, proactive approach to securing your small business

What are we covering today?

- Target audience
- Creating a culture of cybersecurity
  - Defending against social engineering
  - Creating strong passwords
  - Securing your devices
  - Reporting incidents
- Free trainings, tools, and other resources

Quick about me

- Anna Etherton, Phishing Team Lead
- Anna Etherton is the Phishing Campaign Lead at the Cybersecurity and Infrastructure Security Agency (CISA). For seven years, she has provided Phishing Simulation services to State, Local, Public, and Private organizations. Her role involves overseeing the Phishing Campaign Assessment (PCA) team, which measures user responses to phishing emails mimicking real threats. Anna has also conducted Cyber Hygiene Workshops and Tabletop Exercises in Indonesia, Thailand, and the Philippines.
- Previously, Anna served as Program Manager and Government Lead for the Network Security Information Exchange (NSIE) Committee, collaborating with domestic and international members to share threat information. Prior to that role, she was part of the Pentagon's Computer Incident Response Team (PENTCIRT), working closely with CYBERCOM, DISA, and Army Commands to investigate cyber security violations inside the Pentagon.
- Anna has served overseas for over 6 years as is a US Army Combat Veteran and civilian contractor, overseeing satellite operations, Blue Force Tracking, network infrastructure, and IT security compliance.
- Anna loves skydiving, ziplining, riding her motorcycle, and teaching Cyber Awareness to local charity organizations. Her favorite pastime is attending the Marine Corp Marathon, simply to watch from the sidelines.

Target audience – you!

- “Cyber rich, resource poor”
  - Fewer than 20 employees
  - No in-house, dedicated information technology staff
- Ideal Future State vs Current State
  - Burden of cybersecurity
  - Tools, people, and processes
  - Better than nothing, then building too optimal

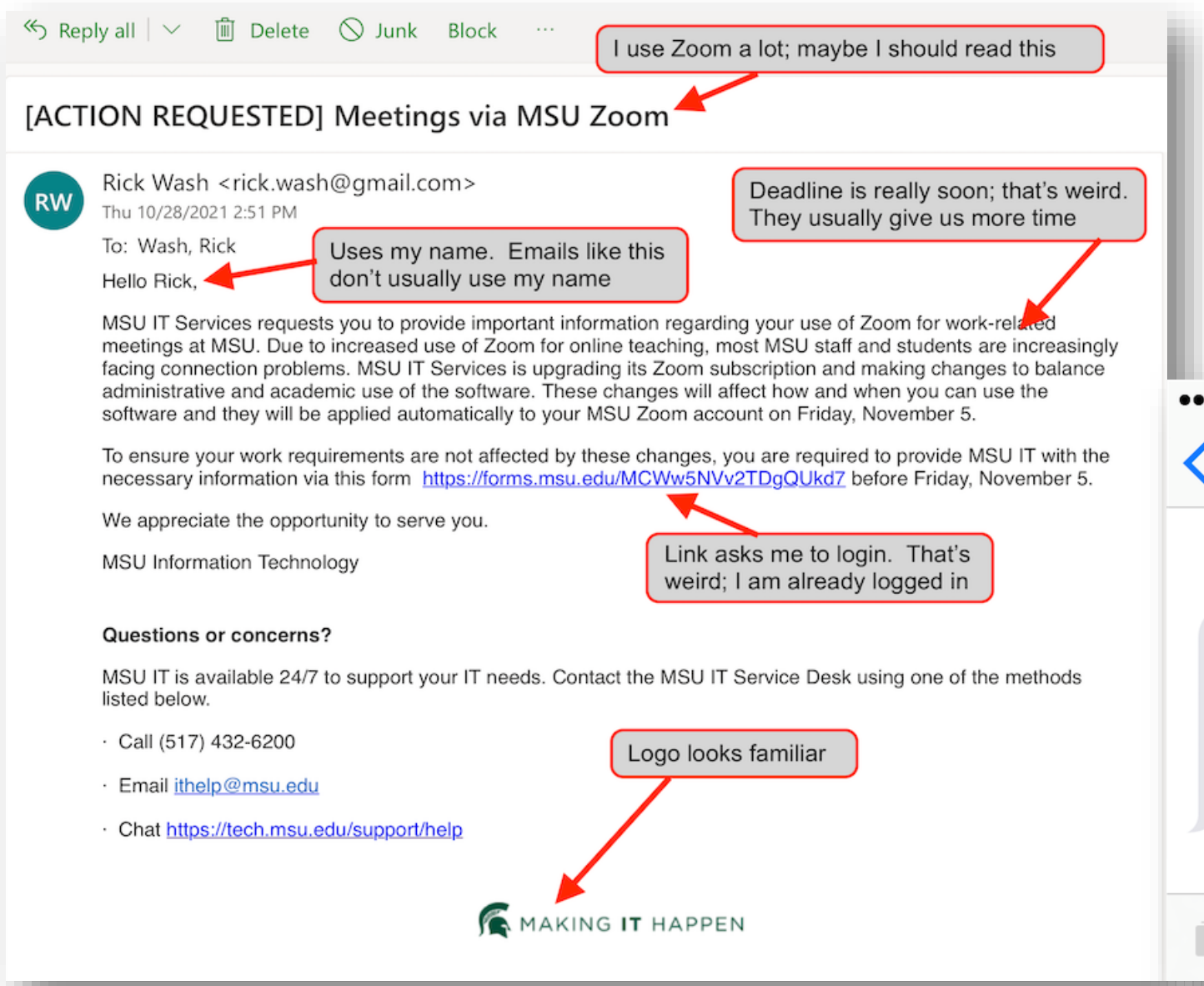
Culture of Cybersecurity

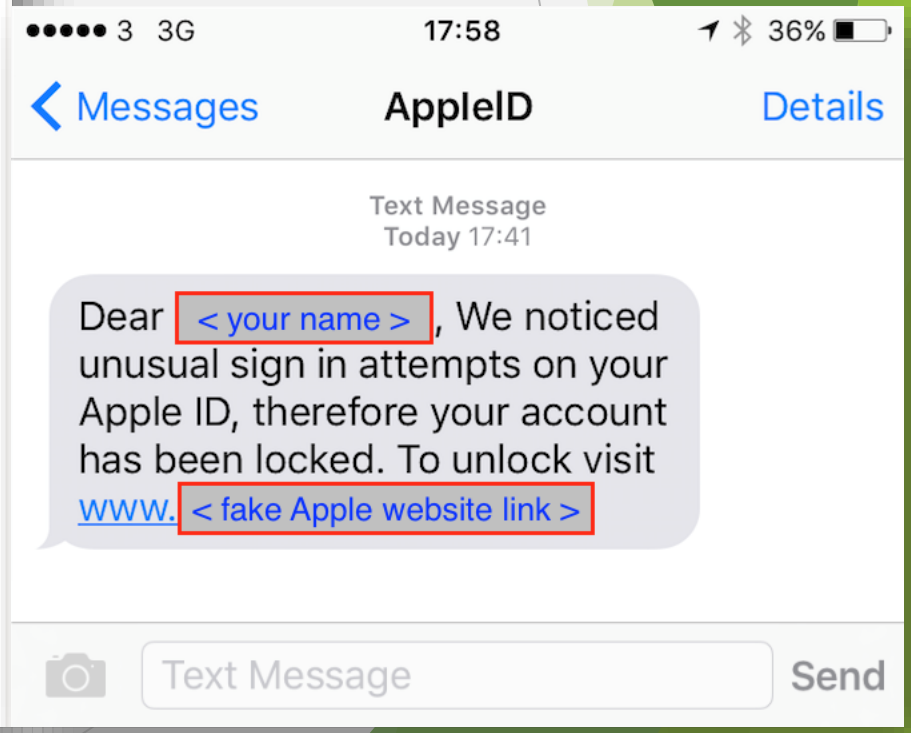
- Starts at the top
  - Lead by example
  - No shame
  - Share personal experience on incidents
- Gamification, because games are fun!
  - Positive behavioral reinforcement
  - Security Champions
- Home life and work life
  - Good and bad behaviors can flow both ways
  - Train positive behaviors at work

Phishing Defense

- **Types of Social Engineering: Phishing, Vishing, Smishing…**
  - Result is most commonly credential theft or malware deployment
- **Understanding indicators**
  - Trigger strong emotions (anger, fear, urgency, curiosity)
  - Sender's email and presumed identity
- **I think this is phishing, what do I do?**
- **I clicked, now what?**

Adapting and Staying Relevant



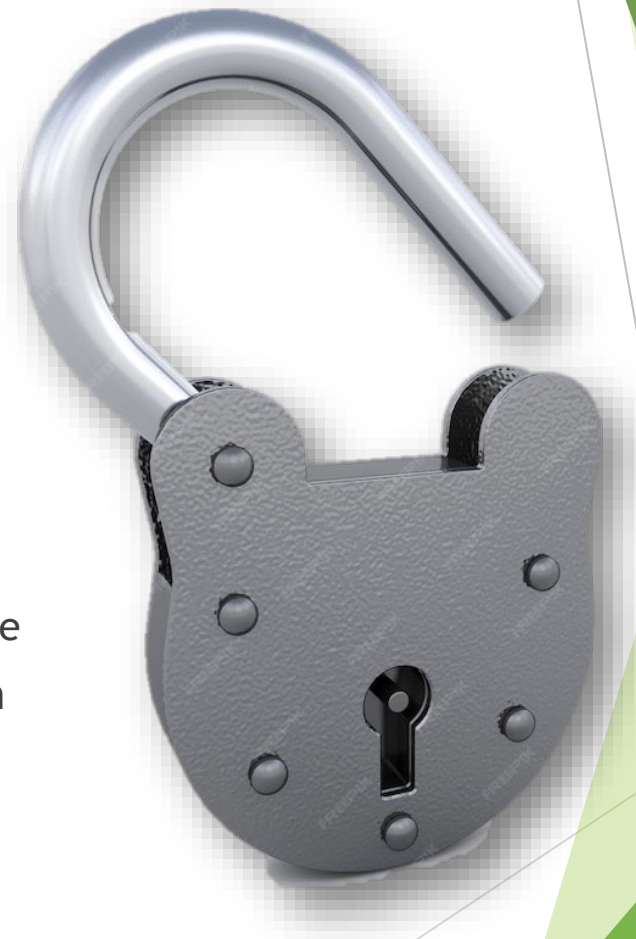


What’s Your Password?

https://www.youtube.com/watch?v=opRMrEfAIiI start at 40 seconds

Strong Passwords

- **What makes for a good password?**
  - Long – at least 15 characters
  - Unique – never used anywhere else
  - Randomly generated – usually by a computer or password manager.
    - They're better than humans at being random!
- **Use a password manager!**
  - Reputable app (with a strong primary password!)
  - Stored in browser (but watch who has access to that device!)
  - Otherwise, use a memorable passphrase that is long and unique
- **Multi-Factor Authentication is *optimal*, but not always an option**
- More great tips: https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords



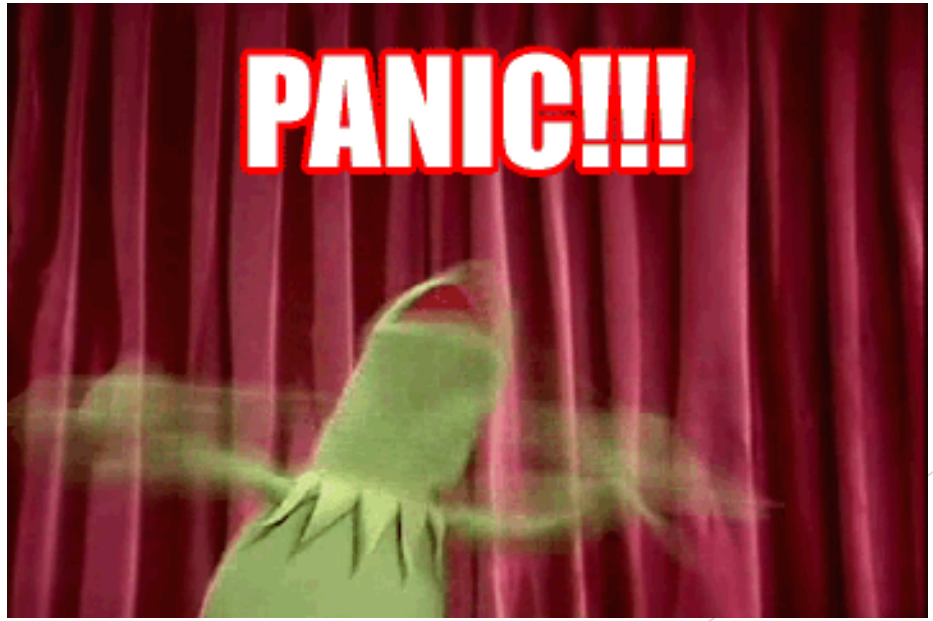
Device Security

- Train folks on what a “device” is
- Keep your software and app up to date
  - Better yet, enable auto updates!
- Download with caution
  - Use official app stores with reputable developers
  - Avoid unknown or 3rd party applications
- Treat your device like a wad of cash– would you leave that unattended?
  - Locking your screen
  - Be aware of your surroundings-- OpSec!

Incident Reporting

- **Something will happen! Are you prepared?**
  - Act quickly to limit damage
  - Report it, even if you think someone else already has
  - There's no shame if you caused an incident, report it!
  - Speak up if you see security policies or processes that don't work

- **Finally, organizations should report anomalous cyber activity and or cyber incidents 24/7 to:**
  - report@cisa.gov
  - (888) 282-0870



Free Resources!

- Visit our Small and Midsize Business webpage for resources to help your business recognize and address cybersecurity risks https://www.cisa.gov/cyber-guidance-small-businesses
- Create a custom cybersecurity plan for your small business with the Federal Communication Commission's (FCC) Small Biz Cyber Planner 2.0 -- https://www.fcc.gov/cyberplanner
- Learn about compliance resources on collecting sensitive data from consumers and employees from the Federal Trade Commission (FTC) -- https://www.ftc.gov/business-guidance/privacy-security
- Safeguard your business, employees, and customers from online attacks, data loss, and other threats with resources from the National Cyber Security Alliance (NCSA) https://staysafeonline.org
- Videos
  - Simple Cyber Safety Steps https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe
  - Enabling MFA https://youtu.be/gj14IzfpFXs

Questions?