Greene County Information Systems

Cybersecurity in a World of Growing Threats

Greene County Information Systems

IS Security Mission Statement:

Ensure confidentiality, integrity, and availability of county information and assets through a balanced, multilayered, threat informed strategy.

We’re going to talk about

- Current Threats
  - Who
  - What
  - Why
  - How
- What we are doing
  - Protections in place
  - Upcoming projects
- What you can do to help

Current Threats: Who

Opportunistic vs Targeted threat actors

- Opportunistic: spray and pray, sending out phishing emails to a list of addresses, hoping someone will take the bait
- Targeted: a motivated actor who is going after a specific person or organization

Organized crime

- Opportunistic and targeted
- Run like a business – Ransomware as a service, Initial access brokers, call centers

Nation state

- Targeted
- Well funded and well trained – APT (advanced persistent threat)

Current Threats: What

- Data Breach
  - PII
  - Financial information
- Disruptive/Destructive attacks
  - DoS, malware, wipers, OT (water treatment, pipelines, electrical grid)
- Ransomware
  - Form of disruptive attack
  - Malware that encrypts your data that is then held for ransom

Current Threats: Why

INFORMATION = MONEY

VERIZON BREACH REPORT FOUND 95% OF DATA BREACHES ARE FINANCIALLY MOTIVATED

RANSOMWARE – ABOUT $900 MILLION IN 2023

Current Threats: How

- Stolen Credentials
  - 49% data breaches involved use of stolen credentials
  - Breaches to steal credentials!
  - Phishing emails
  - Credential harvesting websites

Current Threats: How

Email security

- Phishing -> biggest risk
- Don’t click links, unless you have to

Attachments are still a risk

- Html/url stuffing
- Malware
- Ransomware

How has AI changed the game

- ChatGPT
- Microsoft Copilot baked in
- More realistic and natural sounding emails

Current Threats: How

Updates

- Patching is so important – Vulns a factor in 38% ransomware events for local government ransomware events in 2023
- Bad guys don't need a critical vulnerability anymore
- String together several small vulnerabilities to compromise a machine

Restart your machine

- At least once per week
  - Apply the updates/patches
- Good rule of thumb, Friday before you leave

What you can do

- Trust but verify
  - Trust your Spidey senses
  - Ask to see badges
  - Call trusted numbers to verify requests, especially via email
- Suspicious email program
  - Keep sending in those suspicious emails
  - Helps the whole county!
- How to spot AI phishing?
  - Ask Copilot

What you can do

You
”What are some tips to recognize AI generated phishing emails?”

Copilot

- **Phishing emails**—those cunning attempts to trick you into revealing sensitive information or downloading malicious files—are becoming more sophisticated, thanks to the use of **AI**. Here are some tips to help you recognize these AI-generated phishing emails:

1. **Compare with Previous Communications**: Pay attention to the **formatting and design** of the email. Compare it with any previous communications you've received from the supposed sender. **Inconsistencies in tone, style, or vocabulary may indicate a phishing attempt1**.
2. **Content Quality**: AI-generated phishing emails may still use **generic greetings** like “Dear user” or “Dear customer” instead of addressing you by name. **Look for poorly written content or typos1**.
3. **Unexpected Attachments**: If an email contains an **attachment** you weren't expecting, exercise caution. **If you know the sender but doubt the content, verify it through an alternate communication method1**.

- Remember, AI-powered phishing emails can be highly convincing, so stay vigilant and follow these guidelines to protect yourself online! 🛡️ 📧

What we’re doing

People-centric cybersecurity strategy

- You all are our greatest assets!
- Everyone of you is a sensor in the field

Talk to you guys

- Cyber awareness training - Sharing is caring
  - Understand your business – Protect to enable
  - Talk Tech – so much cool stuff going on, but can we use any of it?

Cisco Duo -> game changer!

- Dramatic reduction in compromised accounts
- If you get locked out of Duo, without logging in, let us know!

Suspicious email program

Upcoming Improvements

Arctic Wolf - allows us to dramatically up our security game!

- 24/7 SOC monitoring
- Vulnerability scanning
- Cyber awareness training

Network Segmentation

- Compartmentalize department data networks
- Reduce spread of malware

Thank you!

Helpdesk

417.868.4031 or
x4031

helpdesk@greenecountymo.gov