2025 Spring Conference at Rocky Gap Resort
Flintstone, Maryland
Cybersecurity at Work and at Home

Michael Lopez

May 8, 2025

BIOGRAPHY

- Information Security Officer for Queen Anne’s County since January 2025
- Moved to Maryland’s Eastern Shore in 2024 after supporting NASA’s Armstrong Flight Research Center in California for nearly 20 years, wearing nearly every hat in IT.
- xxxxxxxxxxxxxxx

ABSTRACT

Cybersecurity at Work and at Home

List brief overview of presentation in bulletized format

- High level Cybersecurity overview, touching on everyday threats to our data (at work and at home) and the influence of emerging threats, such as AI.
- I'll be providing professional and personal examples of the threats to demonstrate the importance of staying vigilant at home, as well as at work.
- Specific topics will include: Phishing, Ransomware, Software vulnerabilities and end-of-life software, Multifactor authentication, and AI.

What are the goals of cybersecurity?

C.I.A.

- Confidentiality
  - Do you keep unauthorized people out of the data?
- Integrity
  - Are you sure the information is accurate?
- Availability
  - Can you get to the information you are authorized for?

Threats to be aware of in 2025

- Phishing / Spear-phishing / Smishing
- Ransomware
- Software vulnerabilities
  - 0-Days
  - End of life software
  - IoT
- Multi-factor Authentication
- Artificial Intelligence (LLMs)

Phishing

- Messages intended to get information from you.
- Often contain links that will try to get you to log into something that looks real, but is stealing your password.
- May be spread in a wide net to catch as many as possible.
- May be customized to target you specifically.
- We mostly know about email phishing, but these attempts can be made through any communication system, such as text, social media, or phone call.

C.I.A.

Ransomware

- Malware that may be contained to a single device, or may spread to other devices on a network.
- Usually release ransomed data.
  - It’s good for business.
- Double-ransomware becoming more common.

C.I.A.

Software Vulnerabilities

- Patch Tuesday
- Out of band
- PCs, Macs, Linux, UNIX, Android, iPhone, Alexa, Routers, Raspberry Pis
- IoT Devices: Refrigerators, doorbell cameras, alarm systems, wastewater treatment sensors, power monitors, HVAC controls

C.I.A.

End of Life Software

Product	End of Life Date
Microsoft Windows 10	14 Oct 2025
Microsoft Office 2016 & 2019	14 Oct 2025
Apple MacOS 13	TBD
Apple iPhone iOS 17.x	19 Nov 2024
Apple iPhone iOS 18.x	TBD
Google Android OS 13 (“Tiramisu”)	TBD
Adobe Reader 2020	30 Nov 2025
Python 3.9.xx	31 Oct 2025
Red Hat Enterprise Linux 8.x	31 May 2029
Jira 9.9.x	02 Jun 2025

Multifactor Authentication

- Something you know
  - Username, Password, Security questions
- Something you have
  - Smartcard, App, FOB
  - Commonly use SMS/Text for a verification code
- Something you are
  - Finger print, Iris pattern, DNA

Ransomware

- Current uses:
  - Finding patterns in data
  - Generating custom text, computer code, images, audio, and videos
- Use concerns:
  - Storing and misuse of your data
- Cybersecurity concerns:
  - Phishing (text, photo, audio, and video)
  - Vulnerability exploitation with fast adaptation and pattern finding

QUESTIONS?

Contact:

Michael Lopez
Queen Anne's County
Phone: 410-758-6607 x2157
E-mail: mlopez@qac.org