NEWSLETTER

# MIC NEWS

October 2026



# MEMBER SPOTLIGHT:

## EBONEE MCCORVEY



EBONEE MCCORVEY

**Tell us about yourself.**

I have worked in food service and nutrition for over 15 years. My work experience includes training kitchen directors and managers on components of food safety, menu planning, fiscal management, and federal child nutrition regulations. Even while I was still a Nutrition Consultant for an education training center, I was learning more about technology in my spare time.

**What first sparked your interest in cybersecurity? Was there a particular experience, person, or moment that inspired you to explore this field?**

I used to do web admin work as a side duty to a previous job I had. For our team I would update our website as needed, and with that responsibility I had to attend classes hosted by the technology department on web accessibility and other technical regulations. I would always want to learn more than what was required when it came to the backend of the technology. I was first interested in learning CSS and what is in the frontend stack. That transferred over into cyber--security after I had to take a course while in my master's degree. My professor consulted in cybersecurity, and I loved learning about different cases he would mention. From there I found a never-ending desire to learn more about the industry until I made the decision to steer my career to cybersecurity.

**What motivated you to apply to the MNC-CTC Cybersecurity Residency Program? What stood out to you about the opportunity?**

Finding an opportunity to learn cybersecurity and gain leadership skills in a focused, holistic manner was unique to me. It is even better that I can access the Cybersecurity Resource Center (CRC) locally since I live in Dallas. What stood out was the absence of the sales pitch about how easy or fast I could land a job in cybersecurity. I have seen online plenty of bootcamps that make hyperbolic statements about their ability to train you to prepare for a career in 6 weeks to 6 months. MNC-CTC is about giving you the best foundation to enter a career in cybersecurity, not just land a job.

**What has been the most valuable thing you've learned since joining the program? This could be a technical skill, a professional lesson, or something you've discovered about yourself.**

Ms. Mary always says that working in cybersecurity is about continuous learning. Since we have started with MNC-CTC there have been a major intrusion by autonomous AI (Hugging Face), critical vulnerabilities that affect majority of existing websites (PHP2Shell), leaks of employee data of an intelligence organization (FBI), and thousands of other cybercrimes worldwide. If you are not constantly learning and practicing, or engaging with other cyber professionals, you may fall behind in this industry. We know that vicious ransomware incidents can be costly to an organization, but depending on the industry you work in, falling behind on knowledge or technical skills could also cost lives. And as complex this industry is, there are no shortages of blogs, magazine, podcast, videos, Discord chats, and conferences to learn from. It is up to you to get the information you need and dig in.

**How has being part of the Minorities in Cybersecurity (MiC) community influenced your cybersecurity journey?**

We began our process in June this year in the pre-apprenticeship phase. I can see a marked difference in my knowledge, mindset and dedication to learning this industry. I do not feel as lost as I have in the previous years I have been doing self-studying. The coursework helps to sharpen my understanding of technical terms that I have heard many times from experts. The seminars and leadership sessions give me a realistic view of what working in cybersecurity from a variety of perspectives. Being involved keeps me motivated to keep learning and growing.

**What has your experience been like attending the MNC-CTC seminars? Is there a particular seminar, topic, or discussion that resonated with you?**

It is hard to choose! I have truly appreciated all of the seminar for very different reasons. All of the experts that imparted wisdom to us really gave me a different perspective of working in cybersecurity. My top favorite seminars were Ademola Olanrewaju “Cybersecurity as a Sales Accelerator” and Eunice Roberts “Study Like a Cyber Pro”. Both were insightful for me as someone that has worked in sales, and as person that did not start really learning how to study until college.

**What are your career goals in cybersecurity? Is there a particular area of the field you're most excited to explore?**

Because I have worked in hospitality and k-12, I think I would be interested in exploring how cybersecurity can serve these industries. I am most excited to gain more technical experience to carve out if I want to specialize in penetration testing, malware analysis or threat research.

**What advice would you give to someone who is interested in cybersecurity but isn't sure where to begin?**

Write down what kind of work you want to do in cybersecurity then do research to find the jobs that align with what you want to do. If you enjoy crime or hacker tv shows and movies, write down the things that make them interesting to you and find career paths that can realize your vision.

**Any fun facts, favorite tech hobbies, or a professional 'manifestation' you’re currently working toward?**

In my personal life, I will always have a love of cooking, creating recipes and learning global cuisines. A tech project I am working on is building a personal website that will showcase my creative ventures, track my technical learning journey and share more about my personality and professional skills.

# AWARENESS IN ACTION 20+ YEARS LATER

## EBONEE MCCORVEY



EBONEE MCCORVEY

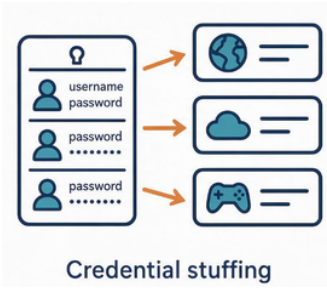
October for some information security and cybersecurity professionals means sifting through newly released annual reports, like the Microsoft Digital Defense Report, which codify trends and threats as the year begins to wind down. This year it also means celebrating 22 years of Cybersecurity Awareness Month. Every year on LinkedIn, I see a good number of posts on the good and bad of awareness training in organizations. After listening to a few podcasts about the repetitive, disengaging nature of cybersecurity awareness trainings and how Sys Admins continue to see "P@SSWORD1" used in the wild, I began to wonder: How did we get here?

In 2001, while the devastation of 9/11 was still fresh in the minds of America, the Department of Homeland Security (DHS) initiated a partnership with the National Cybersecurity Alliance (NCA) to change how we address digital threats. This collaboration was a challenge at reducing the nation's cyber risk by focusing on educating businesses and people about cybersecurity. It was the beginning of public-private partnerships of government agencies, tech companies, and society. In October 2004 Cybersecurity Awareness Month was formally launched as a national initiative. The early focus was on keeping every American safe online by raising awareness of basic cyber hygiene, password security and phishing scams. There was a push to engage with k-12 and small businesses in addition to volunteer-based outreach opportunities to spread awareness to communities. Later the National Coordinator for Critical Infrastructure Security and Resilience, CISA, joined the collaboration alongside NCA.

Microsoft has reported in its latest Digital Defense Report 2026 that password weakness still leads in 99% of initial access to cloud-based identities. These vulnerabilities usually lead to further identity credentials being stolen. Attack techniques like password spraying, credential stuffing, and AI-assisted social engineering coupled with password cracking (brute force) can cause significant harm to you or your organization. Darkweb vendors sell large datasets of breached data. Stolen datasets with millions of credentials in the hands of threat groups targeting everyday American businesses like Bank of America or Walmart is a useful weapon. They will attack many accounts at once, spraying them with the passwords (a) acquired on the darkweb to see where they can gain access. Threat actors can also use your previously breached password to get into other accounts you own (b) or leverage agentic AI to social engineer a personal email in a phishing campaign then unleash relentless bots to crack your password (c).




(a)




(b)




(c)

*"Every small choice you make adds up. Cybersecurity is a daily practice, not a one-time fix," said Lisa Plaggemier, Executive Director of the National Cybersecurity Alliance.*

We can all do something to better protect ourselves. Passwords are used to access almost every account that we have registered to use for daily life such as email, productivity apps, games, shopping sites, traveling, paying utilities, and filing taxes and more. Hackers are betting that you will be overwhelmed with the number of passwords you have to keep up with. They are hoping that you do not update your passwords so that your data that was scraped in a previous breach can still be used to get into your bank account, your email, and possibly takeover your identity. This is why **password entropy**, the complexity and randomness of a password, **2FA** (multi-factored authentication), and warning people of the **dangers of reusing** passwords are still a part of every cybersecurity awareness training to this day.

*Happy Cybersecurity Awareness Month to every expert, practitioner, student and enthusiast that rise to the challenge to make life online safer. Cheers to another year for the opportunity to make a greater impact for good.*

*-Ebonee McCorvey*

*Sources:*
*https://www.staysafeonline.org/cybersecurity-awareness-month | Cybersecurity Awareness Month*
*https://www.youtube.com/watch?v=E4sSzj2Ap4U | 20 Years of Cybersecurity Awareness Month Kick-off*
*https://cybersecpods.com/podcasts/the-cyber-threat-perspective/replay-painfully-persistent-problems-weak-passwords/ | Cyber Threat Perspective - Podcast*
*https://www.microsoft.com/en-us/corporate-responsibility/topics/cybersecurity/reports/microsoft-digital-defense-report/ | MICROSOFT*
*https://www.nist.gov/cybersecurity-awareness-month | NIST*
*https://www.cisa.gov/news-events/news/cisa-launches-cybersecurity-awareness-month-securing-next-250 | National Coordinator for Critical Infrastructure Security and Resilience*

# MIC ANNOUNCEMENTS

## CRC IS NOW OPEN




The Cybersecurity Resource Center is now open Saturdays from 10:00 AM - 4:00 PM CT, and we invite anyone who needs cybersecurity assistance to visit ineedcyberhelp.org to schedule a session!

*Learn more here: ineedcyberhelp.org*

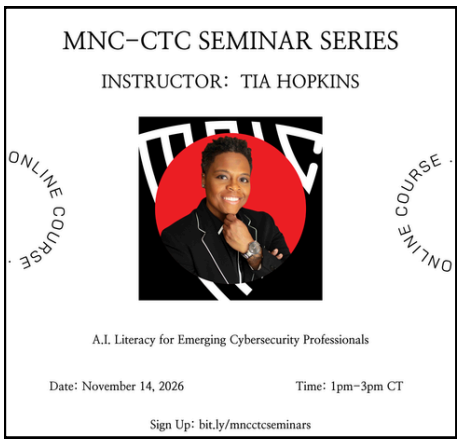
## REGISTER FOR MIC2027




Registration for the 2027 MiC Annual Conference is now open! Join us March 21–25, 2027, as we celebrate five years of leadership, community, and impact. Secure your spot today!

*Learn more here: ineedcyberhelp.org*

## UP NEXT: THE MNC-CTC SEMINAR SERIES




The 12th installment of MNC-CTC Seminar Series kicks off on November 14, 2026.

Join us for our next session, **"A.I. Literacy for Emerging Cybersecurity Professionals,"** featuring guest speaker Tia Hopkins.

*bit.ly/mncctcseminars*

## GET INVOLVED

**Make A Donation**

bit.ly/micdonation

**Join The Community**

$49 Student Membership
bit.ly/JoinMiC

**Become A Mentor**

2 years of IT or Cybersecurity Experience
bit.ly/micmentors