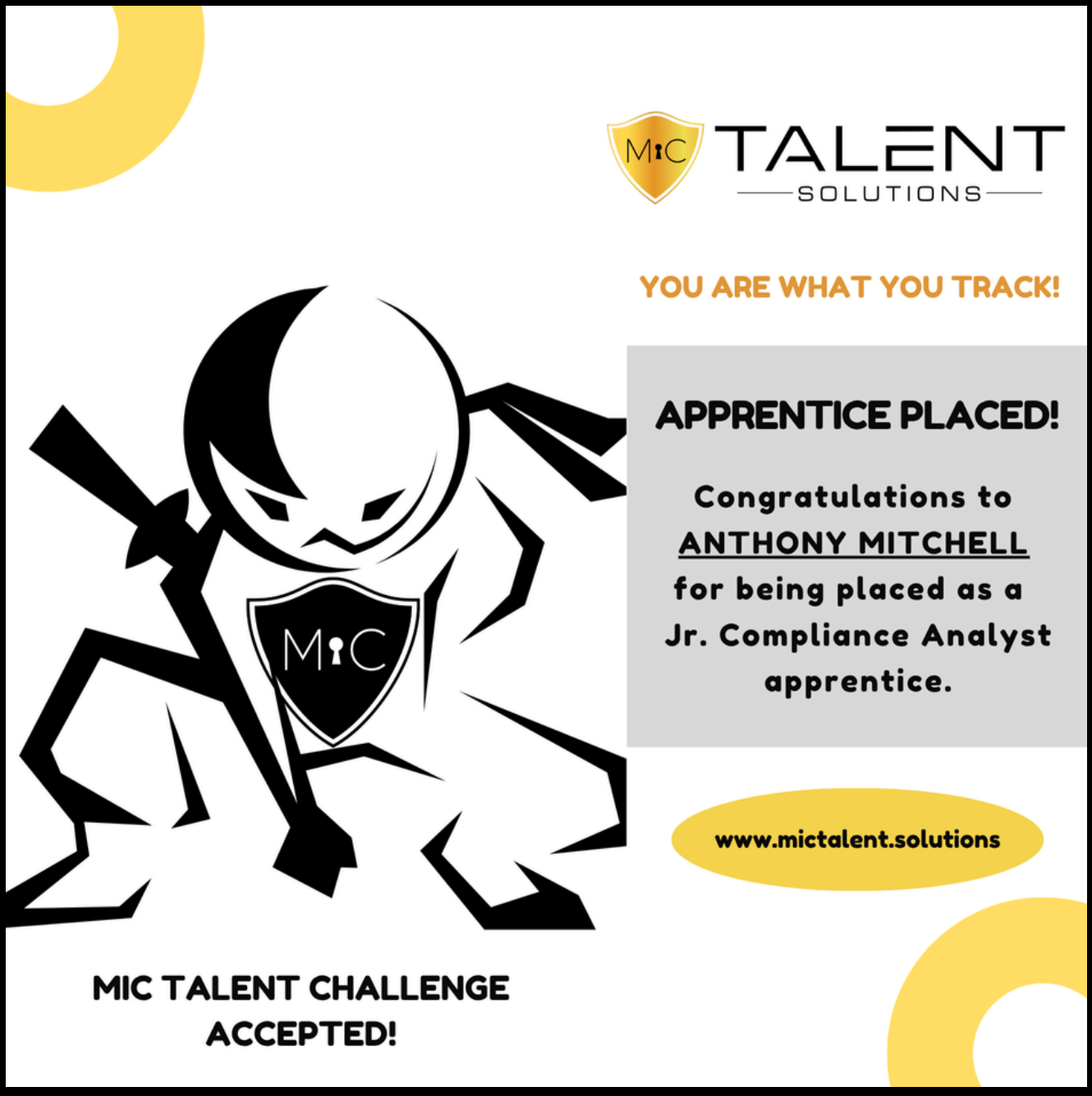
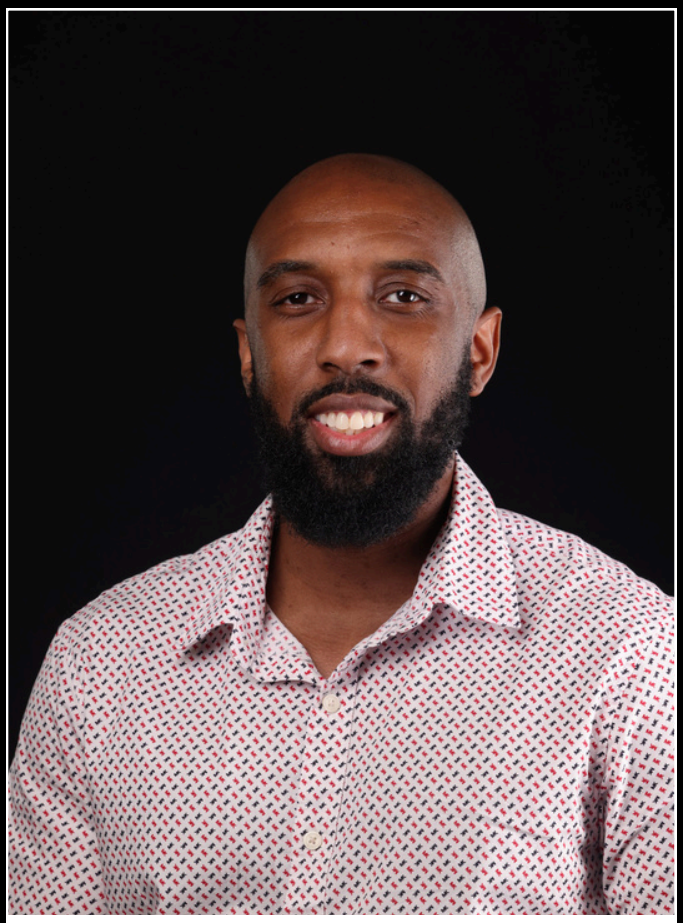
July 2025

MiC News



MEMBER SPOTLIGHT



ANTHONY MITCHELL

Tell us about yourself.

I am a curious person, a life learner, and a go getter. I find excitement in figuring out problems and how things work. I pride myself in knowing that I don't give up easily even in difficult times. I find solace in structure comes from my military service and upbringing. This is what I believe to be why felt this field was for me.

How did you first hear about MiC, and what was your experience like working with the team during your job search?

When transiting out of the service I wanted to also transition into the role or field where I would be a "*Lifer*". I started self studying and taking courses in Cybersecurity and eventually started looking more at jobs. As I ran into one obstacle after another I was advised to start looking into apprenticeships. I searched the DOL list of apprenticeships and found MiC. I reached out to Ms. Mary and she informed me of the next open application period. Once it opened I applied, interviewed, and once accepted I knew I had to focus because this what I wanted to do

You are now set to start your new job so what does being placed through MiC mean to you? How does this opportunity change things for you?

I have been searching for the opportunity to showcase my skills and efforts for 2.5 years now. This role is everything and it means more to me because I am not only displaying what my capabilities are, I am representing something bigger which is MiC.

What kind of preparation did you do for your interview? Any tips or strategies you found especially helpful?

While the coursework with the apprenticeship may have ended, I continue to seek information in this field where ever I can find it. I take courses I find through networking on LinkedIn but a lot of my preparation comes through YouTube. Il researched the company online and watched videos on their products. I also reviewed various topics based on the job description and practiced responses to normal questions.

Are there any resources or support from MiC that you found particularly valuable?

Each Sunday afternoon for the last 3 or 4 months I have met with fellow members from my cohort and the MiC community. The commitment to continued learning from this group is what has added value to not only my journey but others because you see that there is someone just like you, that is willing to put the hard work and time in. I also believe in the mentor program. My mentor Tyrone kept me on track. There was a time I felt defeated and was ready to bow out but he remined me of my purpose.

What advice would you give to other MiC Talent members who are currently looking for roles in cybersecurity?

Stay the course. It may get rocky, it may split into several different paths, and you feel there is no correct one that leads to success, but there is. If you have the time, enroll in courses, use YouTube University (this is a big one for me), and join The SOC Dojo group *(we meet on Sundays at 3:00 PM CT)*.

Any fun facts you'd like to share with our readers?

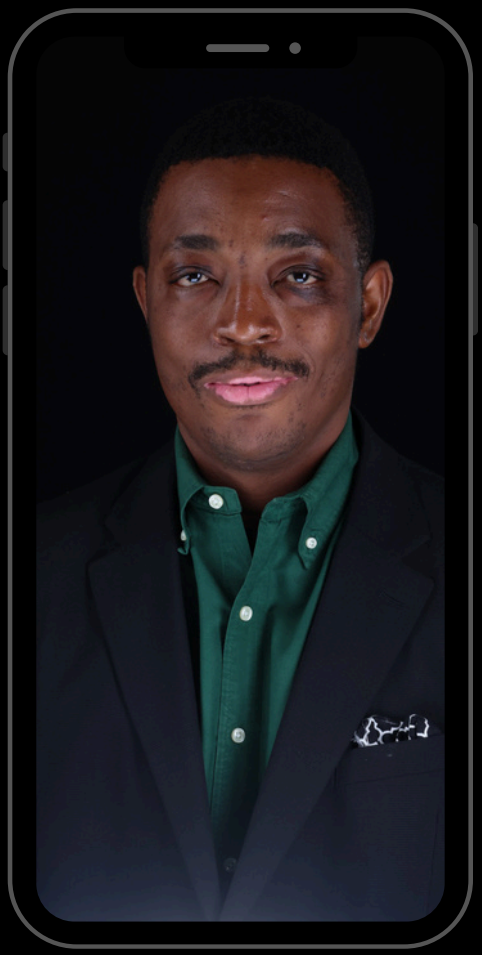
I enjoy working out because I believe maintaining a strong level of fitness is key to living a longer, more youthful life. For me, it’s not just about exercise — it’s about investing in my future self and staying sharp both mentally and physically.

A tip you’d like to share?

Keep pushing forward, ask questions, and don't run from the challenge.

Ghost Jobs: A Hacker's Harvesting Garden

by Ademola Olanrewaju



In the digital job market, not every opportunity is what it seems. "Ghost jobs"—positions posted with no intention of being filled—have become a deceptive norm. While job seekers waste time applying, hackers quietly reap the rewards. These phantom listings aren't just frustrating; they're fertile ground for data harvesting, social engineering, and identity theft.

What Are Ghost Jobs?

Ghost jobs are fake or outdated job postings that companies leave online, either intentionally or through negligence. They might serve various purposes, such as building a pipeline of resumes for future hiring, creating the illusion of company growth, or even collecting personal data for marketing. However, when these listings are exploited by malicious actors, they become more than just misleading; they become harvesting gardens for hackers.

Why Hackers Love Ghost Jobs

Every resume submitted to a ghost job is a potential payload. Think about the wealth of information typi-

-cally included: full names, phone numbers, email addresses, employment history, education, certifications, references, and sometimes even home addresses. This data can be used to craft highly targeted phishing campaigns, impersonate professionals, or even brute-force access to corporate systems. Because applicants believe they're engaging with a legitimate employer, they're often less guarded, making them easier targets.

The dangers posed by ghost job data harvesting are not theoretical. Several major breaches mirror the kind of exploitation that can occur:

- **LinkedIn Scraping Incident (2021):** This incident impacted 700 million users when a hacker scraped public profiles using LinkedIn's API. The collected data included names, emails, phone numbers, and geolocation. Although LinkedIn argued it wasn't a "breach," the leaked data was more than enough to fuel phishing and impersonation attacks—precisely what ghost job scammers aim for.

- **Real Estate Wealth Network Breach (2023):** A misconfigured database exposed a staggering 1.5 billion records. This data included property histories, financial records, and personal information of both celebrities and everyday users, even tax IDs and court judgments information often found in resumes submitted to high-level job listings.

How then do you Protect Yourself:

If you're on the job hunt, it's crucial to treat every application like a potential exposure point:

1. Verify the listing:

Always check the company's official website to confirm the job opening exists there.

2. Limit sensitive documents:

Avoid uploading sensitive documents unless absolutely necessary and you've verified the legitimacy of the request.

3. Use a separate email:

Consider creating a dedicated email address solely for job applications to compartmentalize your personal information.

4. Be sparse with personal details:

Limit personal details on your resume. There's no need to include your full address or birthdate.

5. Ask questions:

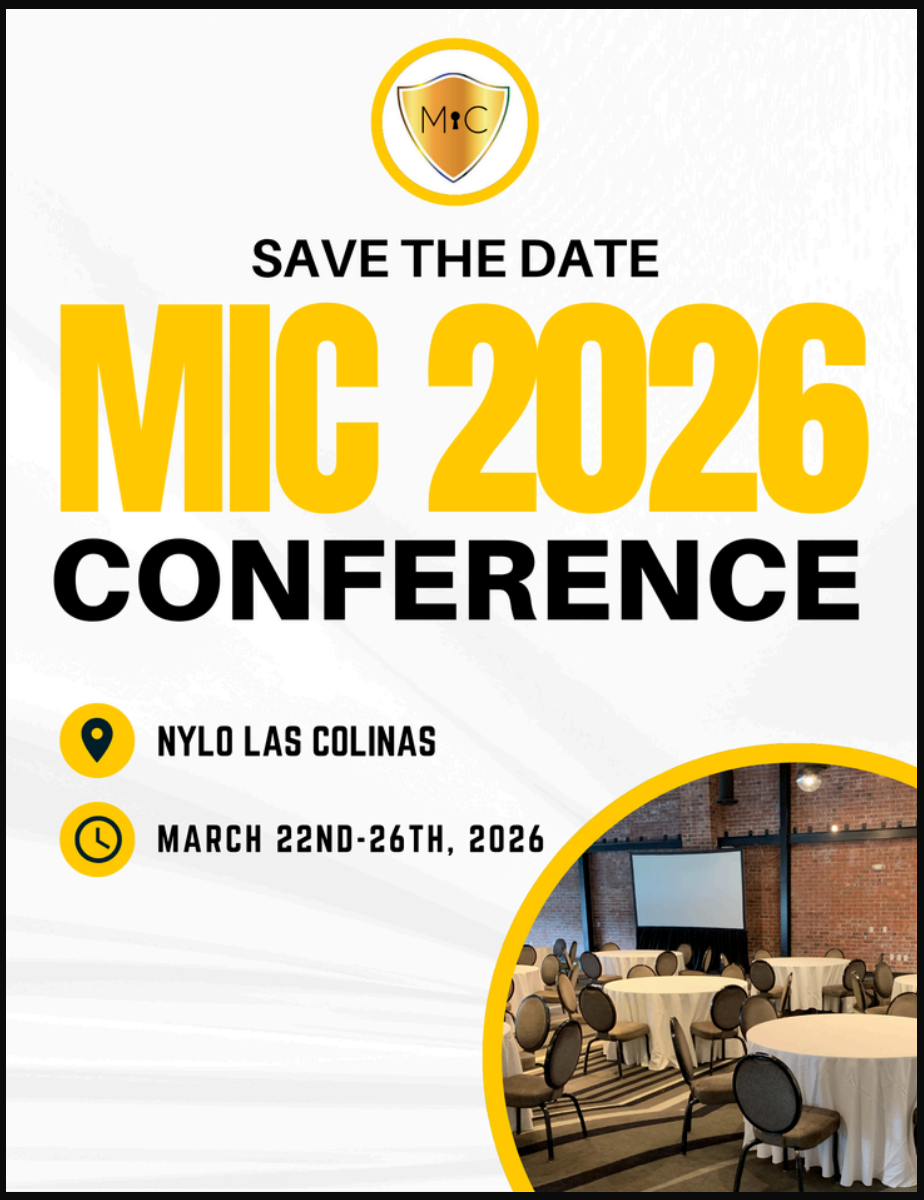
If a recruiter is vague, evasive, or seems to rush you, trust your instincts and walk away.

In conclusion, Ghost jobs may seem harmless, but they're often the first step in a chain of exploitation. Hackers don't need zero-day vulnerabilities when they can harvest data from hopeful professionals. In this landscape, cybersecurity isn't just about firewalls; it's about foresight.

Have you encountered a ghost job, or do you have tips for spotting them? Share your thoughts!

MiC Announcements

IT'S HAPPENING!



MiC LEAD Aspirers™
Coming up on:
August 08, 2025

MiC Drop Prep™ Sessions
Coming up on:
August 05, 2025