EC-Council

" Changing the narrative with regard to building a holistic cybersecurity workforce is crucial to addressing the talent shortage crisis. A cybersecurity team with diverse skill sets is better prepared to deal with evolving threat patterns proactively and effectively. While competent leadership is crucial from a strategic point of view, it is only the tip of the iceberg. To drive and execute cybersecurity programs successfully, organizations must also consider the competence of first-line responders and those in supporting roles. The C|CT scholarship by EC-Council represents a milestone in helping eager, aspiring professionals take their vital first steps in building entry-level cybersecurity skills. With fresh talent joining this field, we will soon see a brighter future. "

- **Jay Bavisi, President and CEO of the EC-Council Group**

With increasingly sophisticated hacking tactics creating complex cybersecurity issues, security strategies must adapt to meet these challenges. Because such cyber threats have vast potential to disrupt operations and continuity, organizations must stop seeing cyber attacks as an afterthought and uphold a comprehensive vision for successful prevention instead of mere mitigation. Relying on technology and disregarding other factors limits organizations to a single-dimensional approach that is not enough to effectively address the evolving cyber threats.

Hackers leverage proximity or social engineering tactics to bypass technology and exploit insiders to carry out their attacks. To stay ahead of the curve, organizations must consider human, social, cultural, and governance factors to implement a robust cybersecurity strategy. Only when organizations employ a multi-protection system, invest in rigorous cybersecurity training, and practice an optimal use of security tools and technologies can they sustain a secure environment.

EC-Council's March Cyber Brief edition keeps you updated on the latest cybersecurity trends and challenges with exclusive stories, engaging webinars, and video testimonials while offering critical insights into the current technologies and security best practices to combat emerging cyberthreats.

Access Previous EC-Council Cyber Brief Issues   »

Cybersecurity Technician

EC-Council pledges $3.5 million to help career starters begin their journey in cybersecurity with the C|CT Scholarship. Take the first step toward joining the cybersecurity workforce.

Apply Today

Insights

READ MORE
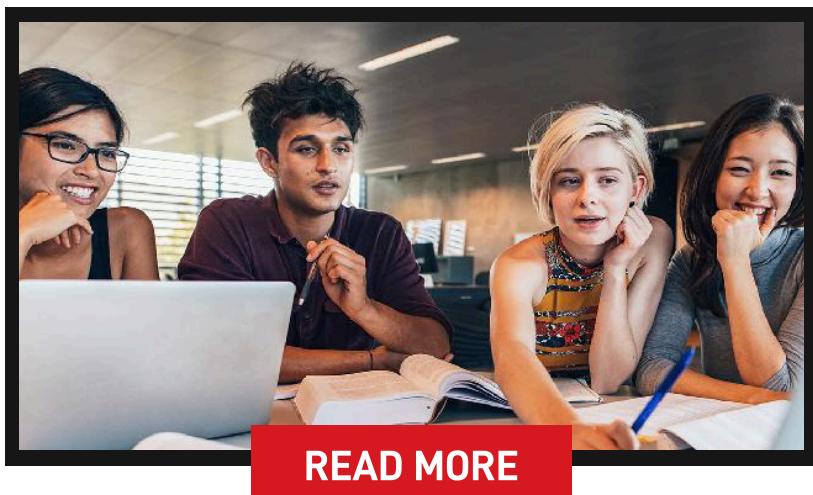
How Do I Begin My Career with a Cybersecurity Scholarship in 2023?

How to Begin a Career in Cybersecurity with World's Unique Entry Level Course | EC-Council CCT

Kickstart Your Cybersecurity Career with EC-Council's $3.5 Million C|CT Scholarship Program

Ethical Hacking

Impact of the C|EH – Hall of Fame Report 2023

READ MORE

READ MORE

C|EH Compete – April Challenge

C|EH Global Challenge
April 2023: Social
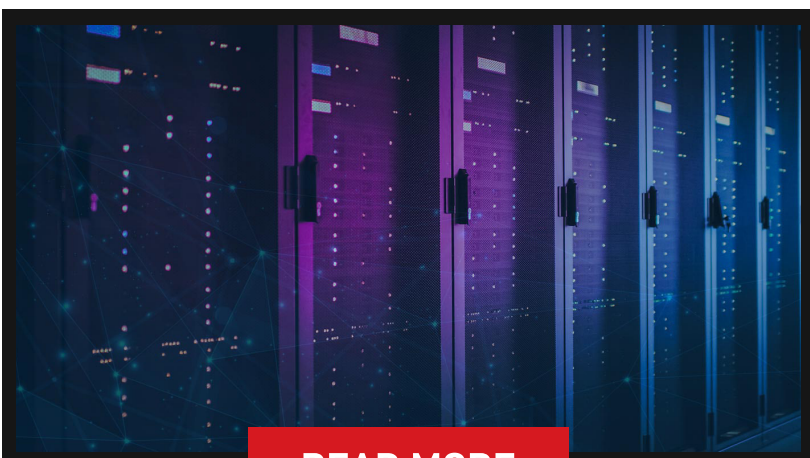Engineering / Phishing
Attacks | Certified
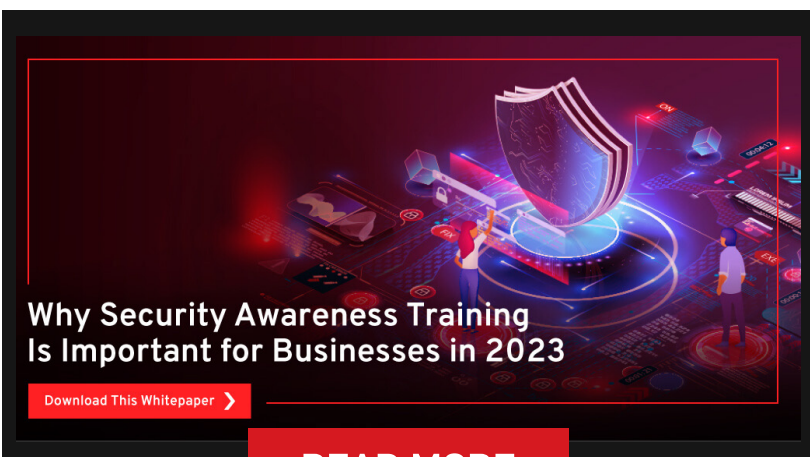Ethical Hacker
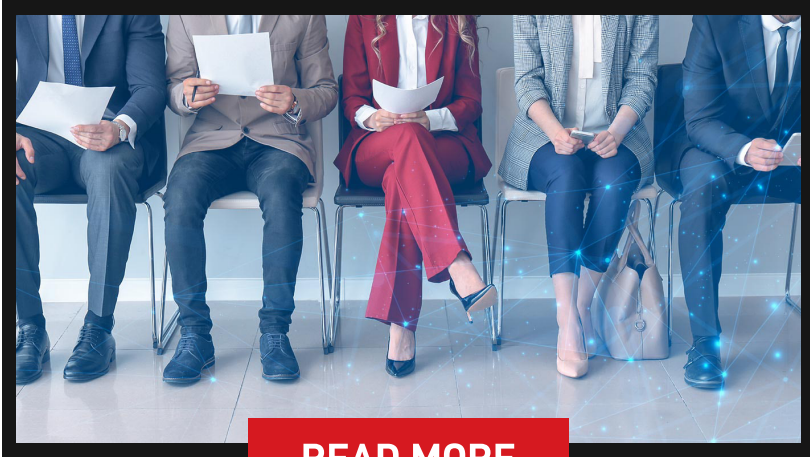
READ MORE

C|EH Opens Doors to Multiple Job Roles in Cybersecurity
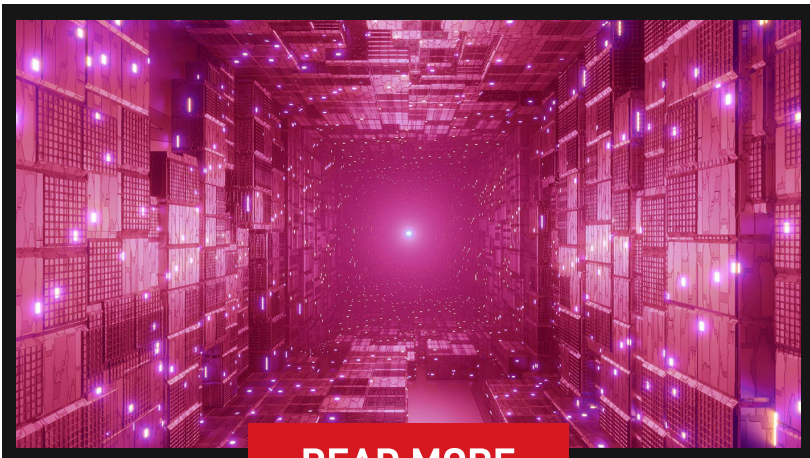
READ MORE

What Is Fog Computing? Importance, Applications, and Everything You Need to Know (C|EH)

READ MORE

C|EH Compete (CTF) A Practice Ground for Ethical Hackers

Why Security Awareness Training Is Important for Businesses in 2023

Download This Whitepaper

READ MORE

Why Security Awareness Training Is Important for Businesses in 2023

Governance, Risk Management, and Compliance in the Cybersecurity Framework

READ MORE

EC-Council

ETHICAL HACKING V/S PENETRATION TESTING

Penetration testers assess the security of a specific aspect of an information system according to an outlined scope. Ethical hackers carry out many types of cyberattacks on an entire system using multiple attack vectors without being restricted by a scope document.

Penetration testers carry out a one-time, limited-duration engagement. Ethical hackers have a continuous engagement that generates more in-depth and comprehensive results.

Penetration testers need a robust knowledge of the domain or area that their penetration tests will target. Ethical hackers need detailed knowledge of hacking tactics, techniques, and procedures so that they can imitate a cybercriminal's steps.

Penetration testers are not responsible for the client's security configuration and incident handling. Ethical hackers are required to assist blue teams and incident handling teams in incident containment and validation for different types of cyberattacks.

Penetration testers must be proficient in writing foolproof reports. Ethical hackers generally do not need to be well versed in report writing.

www.eccouncil.org

Understanding and Responding to Ransomware Attacks by Jerry Bowman

CEH Opened a Variety of Job Opportunities | Mahmoud Embaby
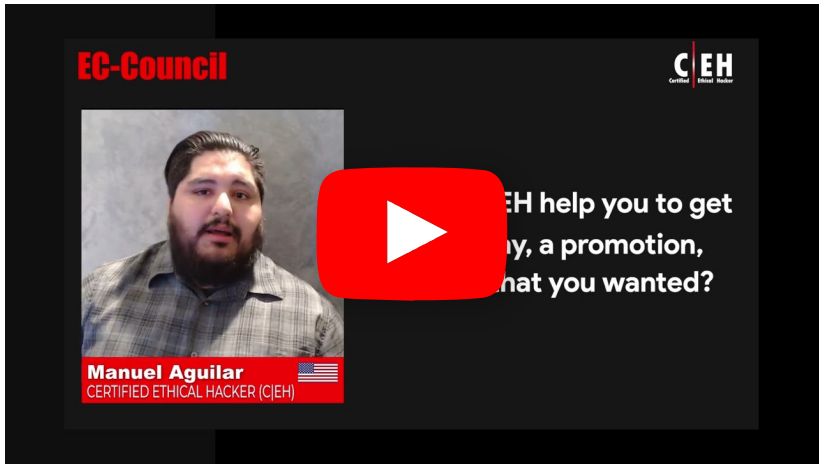

C|EH Helped Me with Skills & Knowledge to Improve Cybersecurity Posture | Jaren Painter
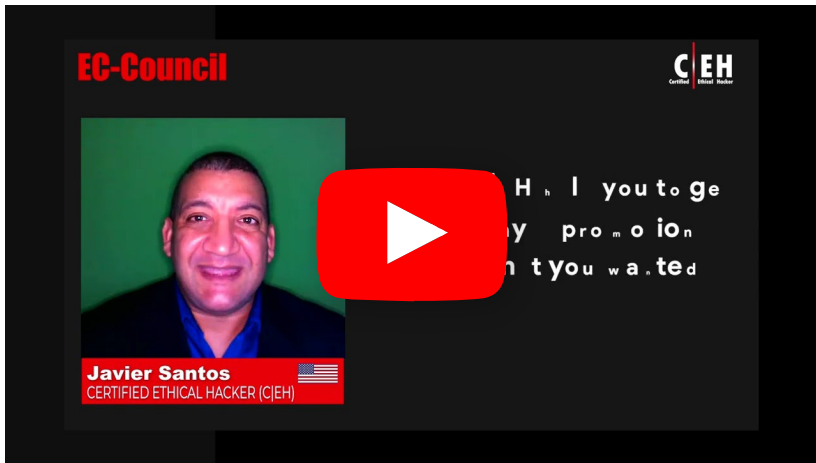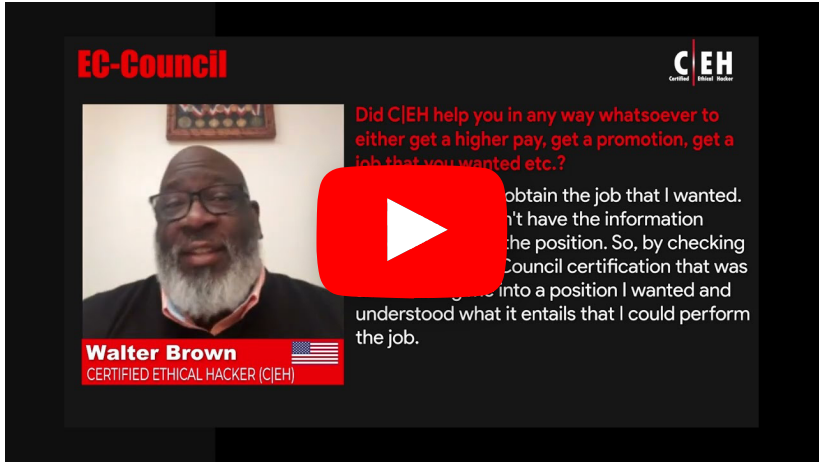

C|EH Helped Me Get a Job & a Promotion | Javier Santos

How C|EH Helped Me Gain Knowledge and Promotion | Mary Moore

From EMT to Cybersecurity Professional with C|EH (Inspiring Career Journey)

How the C|EH Enhanced My Knowledge and Helped Me Get My Dream Job | Walter Brown - USA
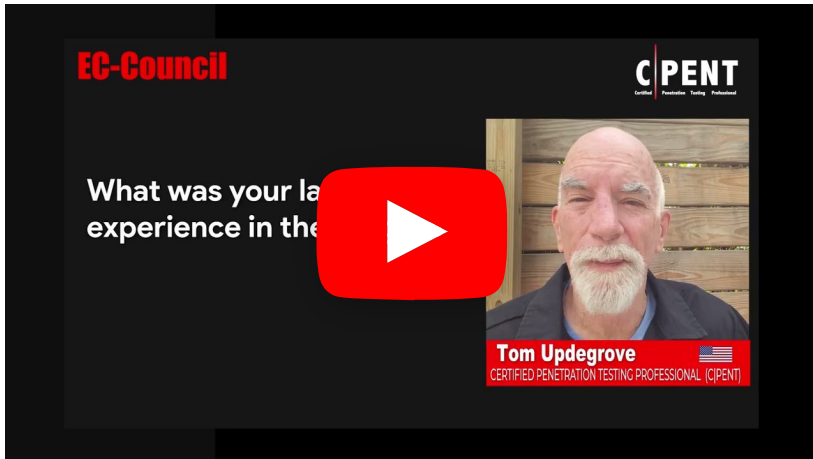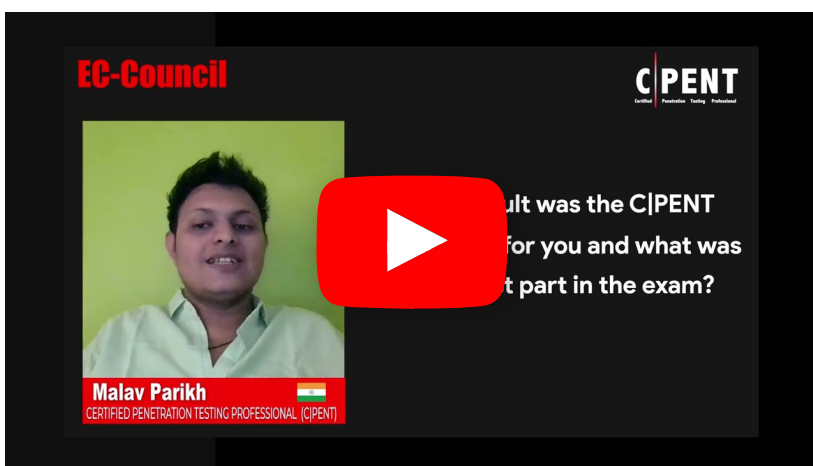
Penetration Testing

Insights

READ MORE

What is Privilege Escalation? Attacks, Understanding its Types & Mitigating Them

READ MORE

Buffer Overflow Attack Types and Prevention Methods

How C|PENT Helped Me Acquire New Invaluable Skills | Tom Updegrove

Penetration Testing Course C|PENT is Best in Class, it Help Me Outshine at Work & Career
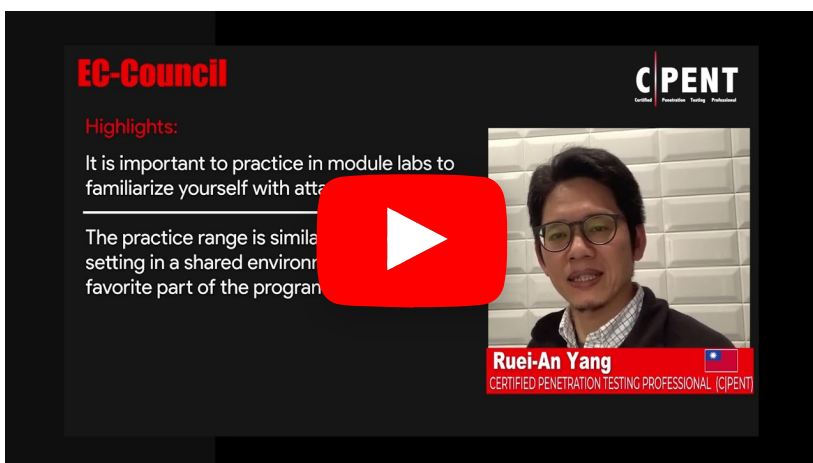
How Labs and Practice Range Helped Me Crack C|PENT Exam | Ruei-An Yang
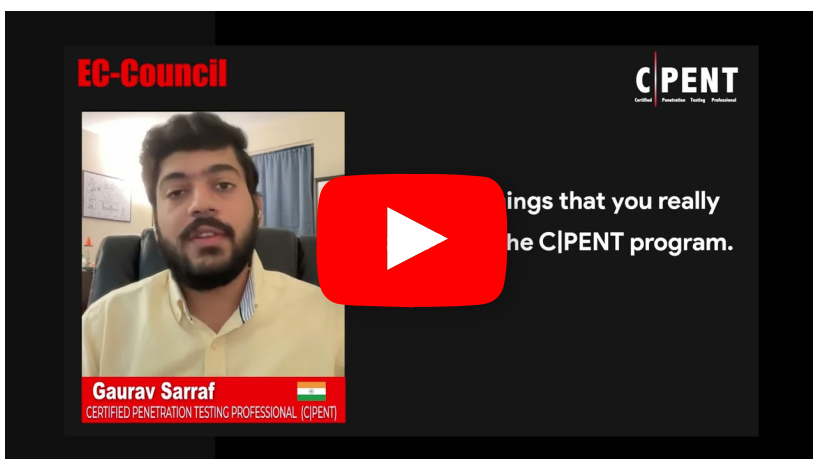
Why C|PENT Is a Must-take Course for Cybersecurity Professionals | Gaurav Sarraf

Career and Leadership
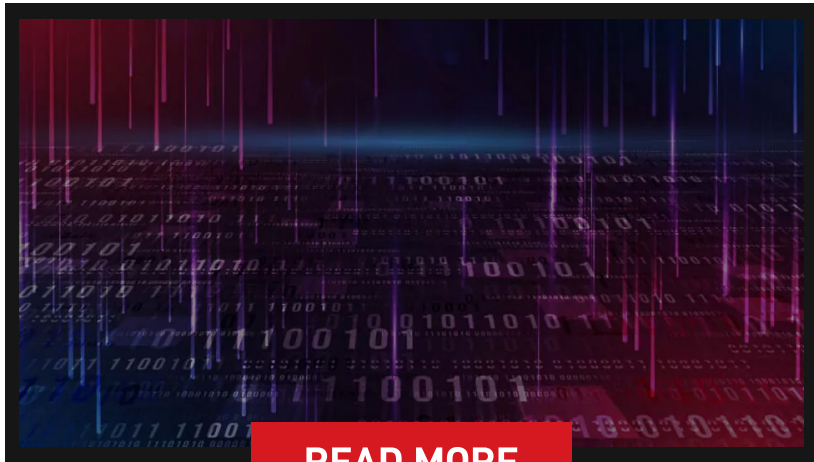
READ MORE

KPIs for a Chief
Information Security
Officer (CISO)

READ MORE

Essential CISO
Learnings

Cloud Security
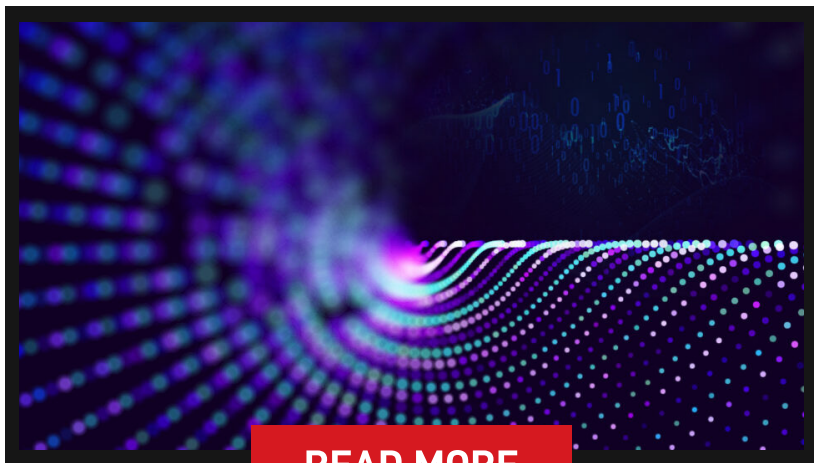
READ MORE

6 Common Cloud
Security Mistakes and
How to Avoid Them
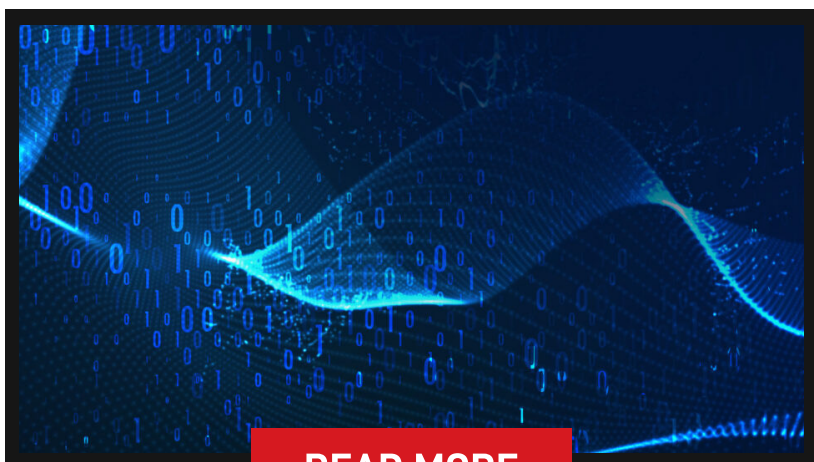
READ MORE

The Blueprint for
Securing the Hybrid
Cloud: Essential Cloud
Security Training

The Ultimate Guide to Cloud Security Certifications in 2023

READ MORE

Cyber Talks

Webinars

Webinar Recordings

Understanding the Difference Between Digital Security and Data Privacy

Introducing Novel Technologies for Effective Threat Hunting

Future Skills: Sustaining Women in Cybersecurity

Penetration Testing Challenges for Cloud-Based Applications (IaaS, PaaS, SaaS)

Monitoring Threats in All Types of Cloud Environments

Why You Should Learn Ethical Hacking, Network Security, Digital Forensics, and SOC for a Perfect Launch Pad into Cybersecurity

Upcoming Webinars

Identity-Driven Security: The Key to Zero Trust

REGISTER

Ethical Hacking for Cloud Security: Best Practices and Tools

REGISTER

How Penetration Testing Helps Secure Web Applications

REGISTER

EC-Council in the News

EC-Council Announces $3.5Million Scholarship to Spark New Cybersecurity Careers Globally

READ MORE

Chuck McGann Appointed as a Master Certified EC-Council Instructor (CEI) for C|CISO

READ MORE

Ethical Hacker from Brazil Tops in the EC-Council's February C|EH Compete Challenge

READ MORE

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Cybersecurity in the Age of IoT: Challenges and Solutions for Students and Professionals

READ MORE

Cybersecurity Consultants: The Role They Play and How to Become One
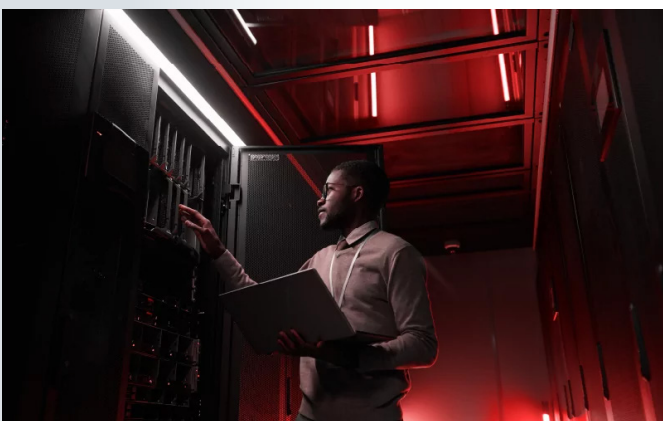
READ MORE

How to Secure Your Home Wi-Fi Network from Hacker

READ MORE

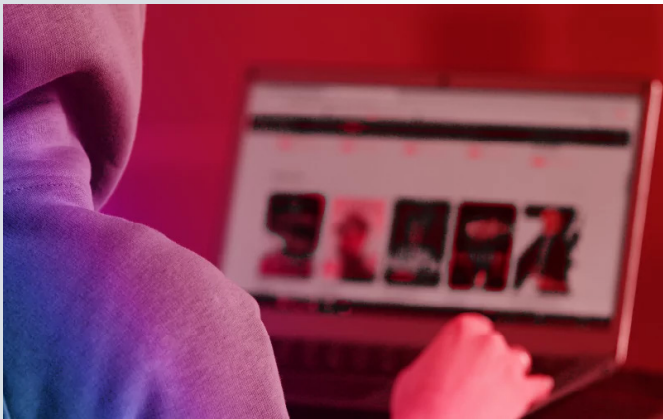## Don't Be the Bait! Phishing Scams: How to Keep Your Online Identity Safe

READ MORE

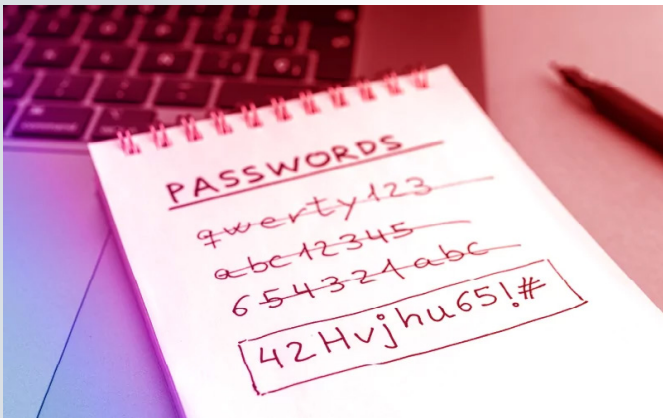## Networking: Critical for Career Development in Cybersecurity

READ MORE

Top Skills Required for a Career in Cybersecurity

READ MORE

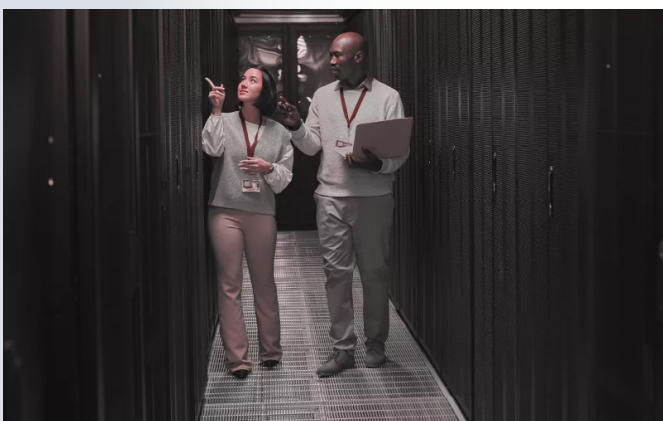## Exploring the Dark Web and Its Dangers

READ MORE

The Importance of Strong Passwords and How to Create Them

READ MORE

Artificial Intelligence and Cybersecurity: The Future is Now

READ MORE

How to Develop a Comprehensive Cybersecurity Strategy

READ MORE