AMERICAN UNIVERSITY
W A S H I N G T O N , D C

Becoming a
Cybersecurity
Professional

American University Cybersecurity Professional Program

What Cybersecurity Is (and Isn't)

Welcome to the world of cybersecurity, a dynamic sector that beckons individuals from all walks of life.

Cybersecurity focuses on protecting digital systems, networks, and information from a variety of cyber threats. Professionals in this space utilize various strategies to detect vulnerabilities and risks, ensuring the security of our digital world.

Your unique background, skills, and perspectives are not just valued—they are essential to the cybersecurity industry. Whether you have a tech-savvy background or expertise from other areas, your contribution is key to building a defense against cyber risks.

There are *3.5 million* unfilled cybersecurity positions globally.

Source: [Cyberseek](#)

Cybersecurity *What* Is:

> **Protection:** Cybersecurity involves establishing measures to prevent unauthorized access to systems and data.

> **Detection:** It includes methods to identify potential threats and security breaches in real-time or after the fact.

> **Response:** Cybersecurity professionals react swiftly to security incidents, containing and mitigating the damage while recovering affected systems.

> **Education:** It involves educating employees and users about best practices.

> **Ethical Hacking:** Organizations use ethical hackers to identify vulnerabilities in their systems.

What Cybersecurity Isn't:

> **Solely About Technology:** Human behavior, policies, and processes are integral to a secure environment.

> **Static:** Cybersecurity is constantly evolving due to the ever-changing landscape of threats, technologies, and vulnerabilities.

> **Only for IT Professionals:** Collaboration across departments, including legal, management, human resources, and more, is essential.

> **One-Size-Fits-All:** Effective cybersecurity is tailored to an organization's unique needs.

> **Just About Computers:** It extends beyond computers to include all networked devices, including smartphones, IoT devices, and industrial control systems.
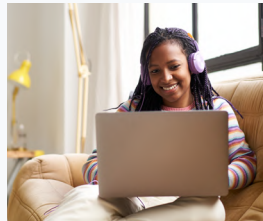
Theresa J.

Former Program Learner

★★★★★

I picked the American University cybersecurity course because it gives you actual hands-on knowledge of networking, Cisco security, and ethical hacking.

Decoding
Cybersecurity's Past

Throughout its history, cybersecurity has evolved from basic protection measures to a complex and multidimensional field, encompassing technical solutions and legal, policy, and ethical considerations. The ongoing evolution of technology and threats ensures that cybersecurity remains a critical aspect of modern society.

1970s-1980s:

Pioneering Days

The first computer viruses and worms: Creeper and Morris Worm

The concept of password security emerges
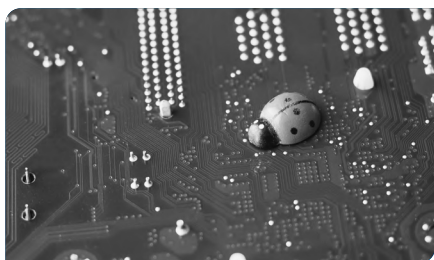
1990s:

Rise of Malware and Antivirus

> Malware attacks lead to the first commercial antivirus software

2000s:

Emergence of Cybercrime

Internet growth leads to phishing, identity theft, and credit card fraud

The need for improved security measures arises

2010s:

Advanced Threats and Nation-State Attacks

State-sponsored cyber attacks gain prominence ‹

Sophisticated and persistent data theft attacks appear ‹

Ransomware attacks surge ‹

2020s:

Continued Evolution

› Supply chain attacks and data breaches emerge

› Emphasis on cloud security, AI-driven threat detection

› Growing focus on regulations to address global cybersecurity challenges

Why You Should Work in the Tech Industry

Embrace the opportunity to learn, grow, and make a meaningful impact. Cybersecurity is a broad field with many career paths. Professionals in this field form a unique community to protect critical infrastructure, assets, and the public from cyber threats.

If you're passionate about protecting people and organizations from cyber threats, then a career in cybersecurity could be the perfect fit for you.

Cybersecurity Is Essential to
Our Way of Life

Cybersecurity professionals are a vital community of defenders. Their mission goes beyond safeguarding networks, data, and systems—they protect individuals, organizations, and societies from evolving cyber threats.

United by a common purpose, this community rises to challenges with unwavering determination. By decoding the hidden language of malware, dissecting the anatomy of breaches, and constructing barriers against cyberattacks, cybersecurity professionals enable us to thrive in a digital world full of smart devices.

Their commitment extends to crafting policies that preserve privacy, advocating for ethical digital practices, and empowering individuals with the knowledge to safeguard their digital footprints.

Cyber professionals are a collective force, pooling their diverse skills and perspectives to adapt to the evolving tactics of adversaries. As cyber threats grow in complexity, so does the unity of this community.

Norris P.

Former Program Learner

★ ★ ★ ★ ★

The instructors are very helpful... and you really come in not knowing much about the field as a novice, and they bring you up to speed in the introductory course.

Cybersecurity:
A Field of Opportunity

The demand for cybersecurity professionals spans every sector as the skills gap widens. Organizations continue to invest in faster, more advanced networks and technologies to manage their daily operations, creating a continuous need for trained cybersecurity professionals.

While AI has the potential to enhance various aspects of cybersecurity, human expertise remains crucial.

The bottom line is that there are too many open positions and not enough candidates to fill them. Companies have no choice but to entice potential employees by offering higher salaries. Companies are spending more on cybersecurity, and that trend is bound to continue.

There are nearly 500,000
open cybersecurity jobs needing to be filled.

Source: Cyberseek

$95,000/year is the
national average for entry-level cybersecurity salaries.

Source: Talent.com

Estimates suggest that by 2030 there could be a global talent shortage of more than *85 million workers.*

Source: Cyberseek

Employment of information security analysts is projected to *grow 33%* from 2023 to 2033, much faster than the average for all occupations.

Reference: U.S. Bureau of Labor Statistics

The Solution? *You.*

There are a number of ways to shrink the cybersecurity skills gap:

1 Reskilling

2 Boosting Diversity

3 Upskilling

Closing the cybersecurity skills gap is so crucial to organizations that recruiters are increasingly open to extending opportunities to candidates from a variety of backgrounds who may not follow the conventional trajectory of a cybersecurity professional. What's more, the Fortinet 2022 Cybersecurity Skills Gap Global Research Report reveals that providing training opportunities for individuals from underrepresented groups can significantly contribute to closing this skills gap.

Whether you are transitioning from another industry, have forged a unique career path, or belong to a traditionally marginalized group in the tech sector, the field of cybersecurity offers immense opportunities to welcome your own blend of diversity.

Jua J.

Former Program Learner

★ ★ ★ ★ ★

I've always sort of been tech-savvy. I wanted to dip my toes in the cybersecurity space because, as I said, I see that everything has become virtual...My thought process was these folks need to be protected, so I just started digging around. I saw the cybersecurity program at American."

It's a pivotal time for job seekers interested in learning new skills or changing careers. As employers move away from "traditional" candidates with a four-year degree in cybersecurity or related work experience, individuals willing to take the leap and reskill have more opportunities.

As cyber threats evolve, experienced professionals need to continually upskill in order to outsmart hackers. Existing security professionals can also close the skills gap with additional training and certifications as they seek advancement opportunities.

This means you no longer need years of experience or a highly technical background to train as a cybersecurity professional.

How You Can Make the Switch

If you're looking to start or advance your career in the cyber industry, a cybersecurity bootcamp is an investment that offers a high return in terms of career opportunities, skill development, and market relevance. It's a strategic move to capitalize on the increasing demand for cybersecurity professionals and secure a promising and dynamic career in an essential field.
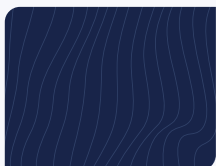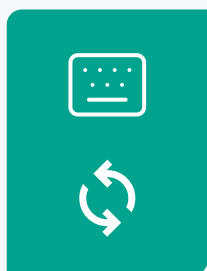
Be job-ready in under a year with the American University Cybersecurity Professional Program.

Our accelerated training offers:

> Rapid Skill Development

> Practical, Hands-On Learning

> Industry-Relevant Skills

> Networking Opportunities

> Proven Career Outcomes

Beyond
Accelerated Training

Cybersecurity certifications are highly sought after in the industry. In addition to gaining hands-on training, the American University Cybersecurity Professional Program provides foundational knowledge for several of industry-recognized cybersecurity certifications.* Boost your credentials with our in-depth resources and learn skills you can apply to the following certification exams:

- AWS Certified Cloud Practitioner

- Cisco Certified CyberOps Associate

- LPI Linux Essentials

- (ISC)2 SSCP**

- LPI Linux Essentials

- CompTIA CySA+

- CompTIA Network+

- CompTIA Security+

- (ISC)2 SSCP – Systems Security Certified

There are only enough cybersecurity workers in the United States to

fill 69% of the cybersecurity

jobs that employers demand.

Source: cyberseek.org

As part of the Complete Program offered by the American University Cybersecurity Professional Program, you can also take our **elective CompTIA® Security+ Certification Exam Prep Course,*** complete with a voucher for the CompTIA® Security+ certification exam.

Establishes the core knowledge required for any cybersecurity role

The only foundational cybersecurity certification that emphasizes hands-on practical skills

A globally recognized certification that establishes the core knowledge required in the cybersecurity industry and provides a springboard to intermediate-level jobs

*For details, please visit https://thrivedx.com/cybersecurity-program-disclaimers.
**Requires a minimum of one year of cumulative work experience in one or more of the seven domains of the SSCP Common Body of Knowledge (CBK) in order to be certified.

TDX

Contact or schedule a call with an advisor to learn more about how to launch your career in cybersecurity.