CyberSecurity

Senior Professional

Become a **White Hat Hacker** and Defend your Data!

New Horizons®

Learn What Earns

5 Reasons Why the I.T. Industry Is a Great Career Choice

If you're looking into possibilities for a new profession or a career change, the I.T. industry might be at the top of your list. It's one of the fastest growing sectors worldwide providing jobs full of opportunities for professional success. And if you're willing to accept the challenge it is highly rewarding throughout life. To help you make your decision, here are five reasons to start a career in I.T.:

1. Quick Employment

Tech companies are looking to hire I.T. professionals because demand is high and there aren't enough qualified workers to fill the gap. And the trend won't end anytime soon, as the tech industry is set to grow another 22-38% by 2020. The demand is so high, that certified professionals can easily find work even without a college degree.

2. A Variety of Career Opportunities

Information Technology is not an isolated industry. It overlaps with every other sector, which makes it a versatile career opportunity. From healthcare to agriculture, digital transformation is driving change in all spheres of business which allows I.T. professionals to choose a career that aligns with their interests.

3. Easy Career Growth

As technology improves, I.T. professionals evolve alongside it. But with the constant pursuit of knowledge, it allows them to grow their careers much faster and easier than in other industries. It is not unheard of for tech professionals to start at entry level, and move to a mid-level managerial position within a few years.

4. It Pays Well

Tech professionals are esteemed for their unique skill sets. That makes them invaluable assets in any business. Therefore, when it comes to their financial compensation for their work, it is substantially higher than the average norm even at junior or entry-level positions.

For example, depending on the industry and location a software engineer (with experience) can earn an average salary of around $83,000, which is considerably more than the national average in the United States.

5. A Reasonable Education

Every job in the I.T. industry requires a unique set of skills. To qualify for a position, candidates usually have to demonstrate the right amount of technical expertise and provide proof of education and some experience.

However, what skilled professionals don't necessarily need is a 4-year university degree. If they have the right certification and display an aptitude for completing tasks, they usually receive an entry-level position.

And when it comes to certification training programs, they are faster and far less expensive than a full degree in Computer Sciences. So, anyone with enough desire can pursue a career in I.T. even when you start from scratch.

Senior Cybersecurity Professional

What if you could spend all day hacking and get paid for it? Take the Certified Ethical Hacker course and you can help the good by behaving like the bad. This course will teach you all the tricks of the trade that you can then use for a fun, engaging career of finding vulnerabilities in systems. Learn how to network scan, evade IDS, hack mobile platforms and more. As cybersecurity continues to grow as a threat, Certified Ethical Hackers are in demand to help protect companies from security threats. In just one week, you can learn what you need to help protect the company at your next career!

What will you do with it? You'll be set free to attack systems just like malicious hackers do, in order to find and fix weaknesses in your company's and client's systems. Your work will help develop security policy, identify technology trends and keep data safe. In addition to testing computer systems, you'll document operational procedures, monitor platforms and train users for security compliance.

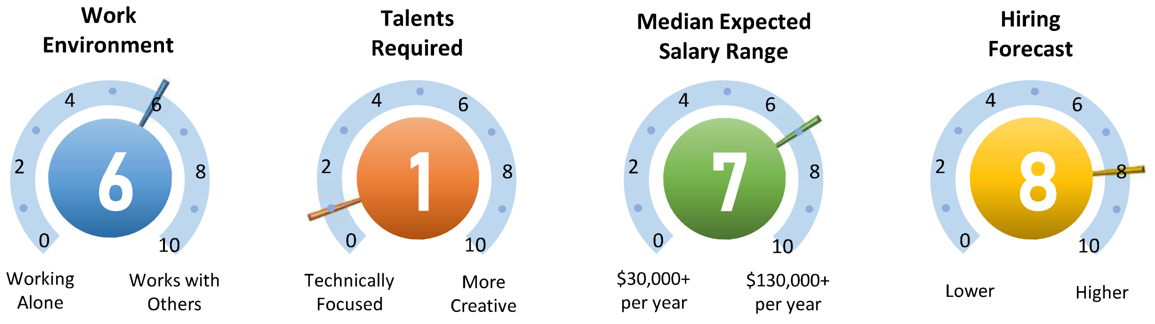
Personal Skills Needed

- Complex Problem Solving
- Critical Thinking
- Reading Comprehension
- Active Listening
- Monitoring

Students will learn how to scan, test, hack and secure target systems. The course covers the Five Phases of Ethical Hacking: Diving into Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and Covering your tracks.

Does this job fit you?

FUTURE AT A GLANCE*



* According to the U.S. Department of Labor. A proud partner of the americanjobcenter network.

Other Career Paths Available But Not Limited To:

- Computer and Information Systems Managers
- Information Security Analysts
- Computer Systems Analysts
- Chief Information Security Officer
- Forensic Computer Analyst

Program Includes:

- 40 hours of live Certified Ethical Hacker Certification Training (with free re-take option)
- Preparatory Materials for the Certification Exams (1)
- Practice Exams for the Certification Exams (1)
- Certification Exams: *CEH Exam (312-50)*
- 35+ Hours of Bonus Material, such as:

Certified Information Systems Auditor (CISA)

Certified Information Security Manager (CISM)

CompTIA Advanced Security Practitioner (CASP+)

Successful Completion of this Program Includes:

- Learning the skills needed to become a critical asset to any company in the Security profession
- Earning the CEH Certification Designation
- Learning a multitude of interpersonal, professional, and security skills to help you become successful in your new career!
- (Program includes access to over 2,800 self-paced certified On-Line Anytime (OLA) Courses and Modules to assist you even after you are employed in your new career.)

Program Format: Online, in person and self-study

Time: 4 Weeks
Cost: $6,690

Classes and materials provided by New Horizons of Wisconsin, the state’s largest technology and business skills training organization. All classes are certified and/or authorized by the developer.

This program is approved by the Wisconsin Department of Workforce Development and is listed on the Eligible Training Provider List (ETPL) Portal. (Note:A/O 2/5/20, Application in Process)

The Top 5 Reasons You Should Consider a Career in Cybersecurity

1. You'll Be a Part of an Exciting, Challenging Field

The internet touches almost all aspects of daily life. In our digital age, cybersecurity plays an essential role in ensuring online safety, as well as the safety of the essential systems that support our daily lives, including electricity, transportation, and financial institutions. As a cyber security professional, you'll be working daily to keep critical infrastructure secure, and will constantly be facing new, engaging challenges.

2. You Will Find More Job Opportunities

Because cybersecurity is such a fast-growing field, there's a high employer demand for qualified professionals. Between 2007 and 2013, postings for cyber security jobs grew 74%, and according to the Bureau of Labor Statistics, employment in the field is projected to grow 18% from 2014 to 2024 - much faster than the average for all occupations. In other words, there are a lot of cybersecurity jobs to be filled, and demand doesn't appear to be slowing any time soon.

3. You Can Earn Higher Pay

The average salary in a job that requires information technology (IT) skills is 50% higher than the average private-sector American job. In 2016, the median pay for a cybersecurity job was $92,600 per year, as compared to a median annual wage of $37,040 for all workers.

4. You'll Be Able to Choose an Industry That Interests You

One of the most appealing aspects of a career in cybersecurity is that the field can be applied to many different industries, from government to nonprofit to private sector. The highest demand for cybersecurity workers are in industries that manage high volumes of consumer data, such as finance, health care, and retail trade.

5. You Can Use Your Entire Skillset

Cybersecurity is a dynamic field, attracting people from all different types of work backgrounds. This means that within the broad field of cyber security, there's an opportunity to differentiate yourself by drawing on your skillset from prior jobs, such as information technology, administration, or accounting, while also building new cybersecurity skills.

National Cybersecurity Awareness Month
(Own + Secure + Protect) + IT
Get Trained, Be Informed and Stay Ahead of the Cybersecurity Curve

Certified Ethical Hacker (CEH)

Certified Ethical Hacker training and certification at New Horizons will help you learn to stop hackers by thinking and acting like one. The CEH training immerses students in an interactive environment where they will learn how to scan, test, hack, and secure their own systems. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. The CEH certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators and anyone who is concerned about the integrity of the network infrastructure.

Benefits of the CEH Certification

As more and more businesses adopt technology in storing data and expanding their market, the number of hackers has also increased. This has prompted the EC Council to put forward ethical hacking as a concept. Ethical hacking acts as a bodyguard to computer and network systems.

Protecting your business: Your business is prone to cyber-attacks and you need trained and certified employees that can think like hackers to protect your assets from hackers. CEH certified employees are permitted to hack into an organization's network to perform essential tests that are meant to protect it from illegal hacking.

Makes the transition to the cloud easier: More and more businesses are transitioning to the cloud and this has led to increased levels of threats. Due to the fast-growing IT world and complex security requirements, hacking techniques are always evolving and only CEH certified employees can help overcome this challenge.

Penetrative testing knowledge: Also referred to as pen testing, employees with this knowledge will help identify system vulnerabilities that hackers can use to attack your systems. There are different penetrative testing methods that you will learn including targeted testing, external testing penetration of all external systems such as DNS and web servers, internal testing, and blind testing which simulate actual attacks from hackers.

Prepare your business for a real attack: cyber-attacks are inevitable regardless of how fortified your computer systems are. Eventually, a hacker will find vulnerabilities and attack your computer assets. However, this doesn't mean that you should stop bolstering your security systems. Because cyberattacks have always been evolving, the only way to minimize or prevent attacks is by being well-prepared. One of the best ways to be prepared against potential attacks is by allowing your CEH certified ethical hackers to identify vulnerabilities beforehand.

Get equipped with real hacking tools: Regardless of how curious you may be, you may not be able to identify the right hacking tools without formal in-depth training that is needed to use the complex hacking tools. However, through the CEH certification, you will learn how to use these tools themselves.

This is the outline for your 5 day LIVE class with an expert to prepare you for a career in CyberSecurity. You will need be serious about your career and prepared to learn. We will train you on everything below!

COURSE OUTLINE
PAGE 1

1 - Introduction To Ethical Hacking

Overview Of Current Security Trends

Understanding Elements Of Information Security

Understanding Information Security Threats And Attack Vectors

Overview Of Hacking Concepts, Types, And Phases

Understanding Ethical Hacking Concepts And Scope

Overview Of Information Security Management And Defense-In-Depth

Overview Of Policies, Procedures, And Awareness

Overview Of Physical Security And Controls

Understanding Incidence Management Process

Overview Of Vulnerability Assessment And Penetration Testing

Overview Of Information Security Acts And Laws

2 - Footprinting And Reconnaissance

Understanding Footprinting Concepts

Footprinting Through Search Engines

Footprint Using Advance Google Hacking Techniques

Footprint Through Social Networking Sites

Understanding Different Techniques For Website Footprinting

Understanding Different Techniques For Email Footprinting

Understanding Different Techniques Of Competitive Intelligence

Understanding Different Techniques For Who Is Footprinting

Understanding Different Techniques For Network Footprinting

Understanding Different Techniques Of Footprinting Through Social Engineering

Footprinting Tools

Footprinting Countermeasures

Overview Of Footprinting Pen Testing

3 - Scanning Networks

Overview Of Networking Scanning

Understanding Different Techniques To Check For Live Systems

Understanding Different Techniques To Check For Open Ports

Understanding Various Scanning Techniques

Understanding Various Ids Evasion Techniques

Understanding Banner Grabbing

Overview Of Vulnerability Scanning

Drawing Network Diagrams

Using Proxies And Anonymizer For Attack

Understanding Ip Spoofing And Various Detection Techniques

Overview Of Scanning And Pen Testing

4 - Enumeration

Understanding Enumeration Concepts

Understanding Different Techniques For Netbios Enumeration

Understanding Different Techniques For Snmp Enumeration

Understanding Different Techniques For Ldap Enumeration

Understanding Different Techniques For Ntp Enumeration

Understanding Different Techniques For Smtp And Dns Enumeration Countermeasures

Overview Of Enumeration Pen Testing

5 - Vulnerability Analysis

Vulnerability Of The Management Life Cycle

Understanding Various Approaches To Vulnerability Analysis

Tools Used To Perform The Vulnerability Assessments

Vulnerability Analysis Tools And Techniques

6 - System Hacking

Overview Of Ceh Hacking Methodology

Understanding Different Techniques To Gain Access To The System

Understanding Privilege Escalation Techniques

Understanding Different Techniques To Create And Maintain Remote Access To The System

Overview Of Different Types Of Rootkits

Overview Of Steganograpy And Steganalysis

Understanding Techniques To Hide The Evidence Of Compromise

Overview Of System Hacking Penetration Testing

7 - Malware Threats

Introduction To Malware And Malware Propagation Techniques

Overview Of Trojans, Their Types, And How To Infect Systems

Overview Of Viruses, Their Types, And How They Infect Files

Introduction To Computer Worm

Understanding The Malware Analysis Process

Understanding Different Techniques To Detect Malware

Malware Countermeasures

Overview Of Malware Penetration Testing

8 - Sniffing

Overview Of Sniffing Concepts

Understanding Mac Attacks

Understanding Dhcp Attacks

Understanding Arp Poisoning

Understanding Mac Spoofing Attacks

Understanding Dns Poisoning

Sniffing Tools

Sniffing Countermeasures

Understanding Various Techniques To Detect Sniffing

Overview Of Sniffing Pen Testing

COURSE OUTLINE
PAGE 2

9 - Social Engineering

Overview Of Social Engineering
Understanding Various Social Engineering Techniques
Understanding Insider Threats
Understanding Impersonation On Social Networking Sites
Understanding Identity Theft
Social Engineering Countermeasures
Identify Theft Countermeasures
Overview Of Social Engineering Pen Testing

10 - Denial-Of-Service

Overview Of Denial Of Service (Dos) And Distributed Denial-Of-Service (Ddos) Attacks
Overview Different Dos/Ddos) Attack Techniques
Understanding The Botnet Network
Understanding Various Dos And Ddos Attack Tools
Dos/Ddos Countermeasures
Overview Of Dos Attack Penetration Testing

11 - Session Hijacking

Understanding Session Hijacking Concepts
Understanding Application Level Session Hijacking
Understanding Network Level Session Hijacking
Session Hijacking Tools
Session Hijacking Countermeasures
Overview Of Session Hijacking Penetration Testing

12 - Evading Ids, Firewalls, And Honeypots

Understanding Ids, Firewall, And Honeypot Concepts
Ids, Firewall And Honeypot Solutions
Understanding Different Techniques To Bypass Ids
Understanding Different Techniques To Bypass Firewalls
Ids/Firewall Evading Tools
Understanding Different Techniques To Detect Honeypots
Ids/Firewall Evasion Countermeasures
Overview Of Ids And Firewall Penetration Testing

13 - Hacking Web Servers

Understanding Webserver Concepts
Understanding Webserver Attacks
Understanding Webserver Attack Methodology
Webserver Attack Tools
Countermeasures Against Webserver Attacks
Overview Of Patch Management
Webserver Security Tools
Overview Of Webserver Penetration Testing

14 - Hacking Web Applications

Understanding Web Application Concepts
Understanding Web Application Threats
Understanding Web Application Hacking Methodology
Web Application Hacking Tools
Understanding Web Application Countermeasures
Web Application Security Tools
Overview Of Web Application Penetration Testing

15 - Sql Injection

Understanding Sql Injection Concepts
Understanding Various Types Of Sql Injection Attacks
Understanding Sql Injection Methodology
Sql Injection Tools
Understanding Different Ids Evasion Techniques
Sql Injection Countermeasures
Sql Injection Detection Tools

16 - Hacking Wireless Networks

Understanding Wireless Concepts
Understanding Wireless Encryption Algorithms
Understanding Wireless Threats
Understanding Wireless Hacking Methodology
Wireless Hacking Tools
Understanding Bluetooth Hacking Techniques
Understanding Wireless Hacking Countermeasures
Wireless Security Tools
Overview Of Wireless Penetration Testing

17 - Hacking Mobile Platforms

Understanding Mobile Attack Platform Vectors
Understanding Various Android Threat And Attacks
Understanding Various Ios Threats And Attacks
Understanding Various Windows Phone Os Threats And Attacks
Understanding Various Blackberry Threats And Attacks
Understanding Mobile Device Management (Mdm)
Mobile Security Guidelines And Security Tools
Overview Of Mobile Penetration Testing

18 - Iot Hacking

Understanding Iot Concepts
Cryptography Tools
Understanding Various Iot Threats And Attacks
Understanding Iot Hacking
Understanding Iot Attacks
Iot Security Tools

19 - Cloud Computing

Understanding Cloud Computing Concepts
Understanding Cloud Computing Threats
Understanding Cloud Computing Attacks
Understanding Cloud Computing Security
Cloud Computing Security Tools
Overview Of Cloud Penetration Testing

20 - Cryptography

Understanding Cryptography Concepts
Overview Of Encryption Algorithms
Cryptography Tools
Understanding Public Key Infrastructure (Pki)
Understanding Email Encryption
Understanding Disk Encryption
Understanding Cryptography Attacks
Cryptanalysis Tools

CyberSecurity Professional Career Skills Program

This portion of your job skills program focuses on helping your personal improvement, which will help you succeed in the future. Here you will gain

skills such as:

Certified Information Systems Auditor (CISA)

Certified Information Security Manager (CISM)

CompTIA Advanced Security Practitioner (CASP+)

Below you will find the detailed listing of your classes, with approximately 35 hours of professionally created and delivered content will provide you with the additional skills that you will need to succeed at your new career!

This is your On-Line Anytime (OLA) library, and you will have access to these titles, and thousands more, for a full year!

Asset Type	Title	Code	Program Length
Courses	**Certified Information Systems Auditor (CISA) 2019: BCP & Network Security**	it_spcisa19_10_enus	69 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Continuous Monitoring**	it_spcisa19_14_enus	48 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Data Privacy & Risk**	it_spcisa19_03_enus	47 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Data Storage & Malware**	it_spcisa19_09_enus	66 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Digital Asset Protection**	it_spcisa19_08_enus	66 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Digital Evidence Gathering**	it_spcisa19_13_enus	35 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: IAM & Data Classification**	it_spcisa19_04_enus	73 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Information System Auditing**	it_spcisa19_01_enus	57 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: IT Management Frameworks**	it_spcisa19_02_enus	38 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Performance & Management**	it_spcisa19_05_enus	68 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: PKI & Data Protection**	it_spcisa19_06_enus	62 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Scenario-Based Practice**	it_spcisa19_15_enus	22 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: System Design & Analysis**	it_spcisa19_11_enus	59 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Testing & Vulnerability**	it_spcisa19_12_enus	65 Minutes
Courses	**Certified Information Systems Auditor (CISA) 2019: Virtualization & Cloud**	it_spcisa19_07_enus	69 Minutes
Courses	**CISM: Information Risk Management Part 1**	it_spcesm_03_enus	54 Minutes
Courses	**CISM: Information Risk Management Part 2**	it_spcesm_04_enus	53 Minutes
Courses	**CISM: Information Security Governance Part 1**	it_spcesm_01_enus	74 Minutes
Courses	**CISM: Information Security Governance Part 2**	it_spcesm_02_enus	71 Minutes
Courses	**CISM: Information Security Incident Management Part 2**	it_spcesm_08_enus	60 Minutes
Courses	**CISM: Information Security Program Development and Management Part 1**	it_spcesm_05_enus	53 Minutes
Courses	**CISM: Information Security Program Development and Management Part 2**	it_spcesm_06_enus	57 Minutes
Courses	**CompTIA CASP CAS-003: Applying Research Methods for Trend and Impact Analysis**	cs_casp_a16_it_enus	26 Minutes
Courses	**CompTIA CASP CAS-003: Business and Industry Influences and Risks**	cs_casp_a01_it_enus	48 Minutes
Courses	**CompTIA CASP CAS-003: Conducting Security Assessments**	cs_casp_a09_it_enus	52 Minutes
Courses	**CompTIA CASP CAS-003: Implementing Cryptographic Techniques**	cs_casp_a14_it_enus	59 Minutes
Courses	**CompTIA CASP CAS-003: Implementing Incident Response and Recovery**	cs_casp_a10_it_enus	43 Minutes
Courses	**CompTIA CASP CAS-003: Implementing Security Activities across the Technology Life Cycle**	cs_casp_a17_it_enus	43 Minutes
Courses	**CompTIA CASP CAS-003: Integrating and Troubleshooting Advanced AAA Technologies**	cs_casp_a13_it_enus	40 Minutes
Courses	**CompTIA CASP CAS-003: Integrating Cloud and Virtualization Technologies in the Enterprise**	cs_casp_a12_it_enus	44 Minutes
Courses	**CompTIA CASP CAS-003: Integrating Hosts, Storage, and Applications in the Enterprise**	cs_casp_a11_it_enus	50 Minutes
Courses	**CompTIA CASP CAS-003: Interacting across Diverse Business Units**	cs_casp_a18_it_enus	30 Minutes
Courses	**CompTIA CASP CAS-003: Organizational Security and Privacy Policies**	cs_casp_a02_it_enus	40 Minutes
Courses	**CompTIA CASP CAS-003: Secure Communication and Collaboration Solutions**	cs_casp_a15_it_enus	31 Minutes
Courses	**CompTIA CASP+ CAS-003: Integrating Controls for Mobile and Small Form Factor Devices**	cs_casp_a07_it_enus	49 Minutes
Courses	**CompTIA CASP+ CAS-003: Integrating Network and Security Components, Concepts, and Architectures**	cs_casp_a05_it_enus	86 Minutes
Courses	**CompTIA CASP+ CAS-003: Integrating Security Controls for Host Devices**	cs_casp_a06_it_enus	48 Minutes
Courses	**CompTIA CASP+ CAS-003: Risk Metric Scenarios for Enterprise Security**	cs_casp_a04_it_enus	36 Minutes
Courses	**CompTIA CASP+ CAS-003: Risk Mitigation Strategies and Controls**	cs_casp_a03_it_enus	57 Minutes
Courses	**CompTIA CASP+ CAS-003: Selecting Software Security Controls**	cs_casp_a08_it_enus	42 Minutes

Notes:

Your New Career Starts Today!

New Horizons®

Learn What Earns