Cyber Security Specialist

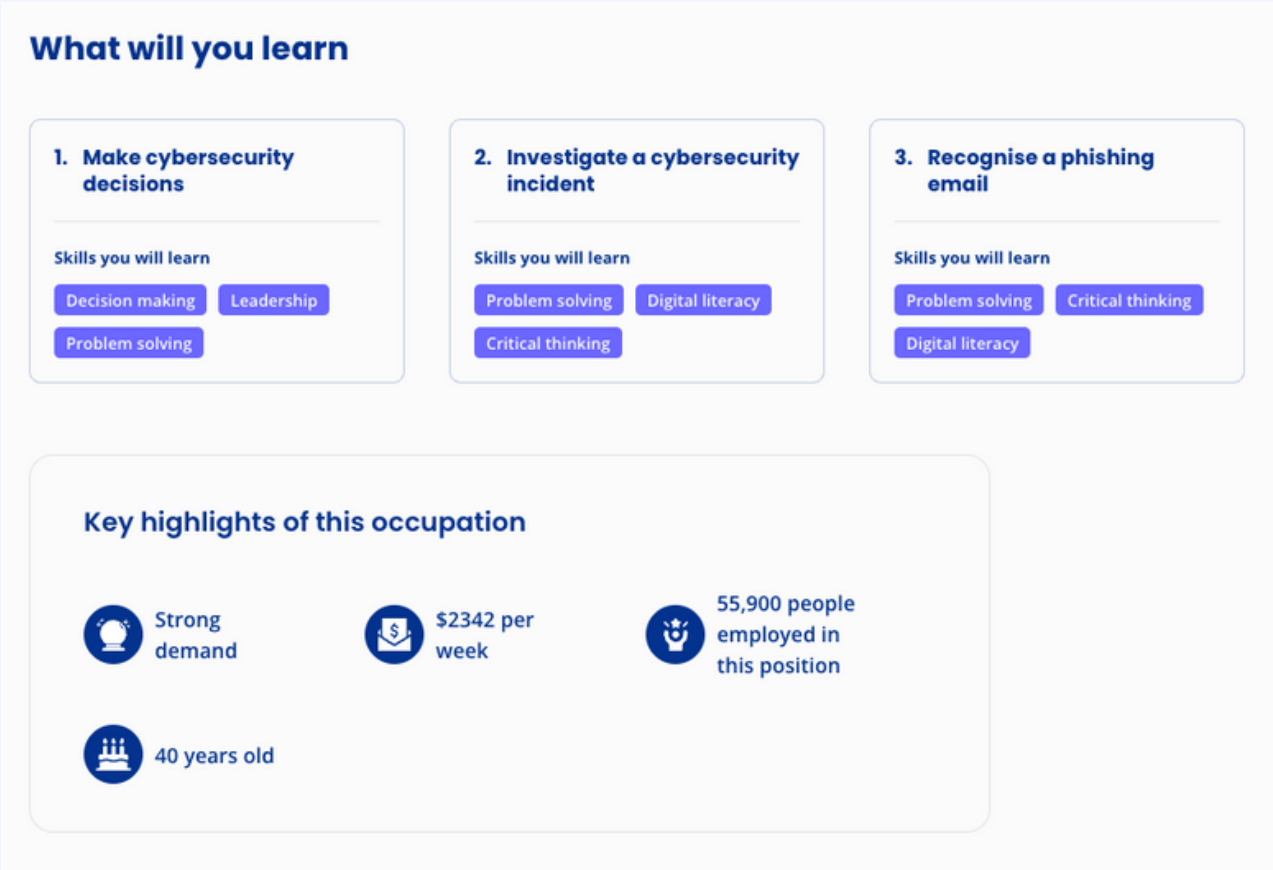
In collaboration with

Microsoft

Overview

A cyber security specialist is someone who helps protect computer systems, networks, and data from cyber threats like hacking, viruses, and cyber attacks. They use their knowledge of computer systems and software to identify vulnerabilities and weaknesses in security protocols and develop strategies to prevent cyber attacks from occurring.

Cyber security specialists work in a variety of workplaces, from the government and large corporations to small businesses and non-profits. They use specialised software and tools to monitor network activity and detect potential threats. They typically work closely with other IT professionals to ensure that systems are secure and up-to-date.



A Day in the Life

The tasks of a cyber security specialist can vary depending on your specific role and the organisation you work for. However, some typical duties may include:

- **Conducting security assessments: This involves analysing an organisation's computer systems and networks to identify potential security weaknesses.**
- **Developing security policies and procedures: Cyber security specialists create guidelines on how an organisation should handle sensitive data and respond to security incidents.**
- **Implementing security solutions: This involves configuring firewalls, encryption technologies, and other security measures to protect an organisation's networks and data.**
- **Monitoring network activity: Cyber security specialists use specialised software and tools to track network activity and detect potential threats, such as unauthorised access or malware.**
- **Investigating security incidents: If a security breach occurs, cyber security specialists investigate the incident to determine what happened and how it can be prevented in the future.**
- **Educating employees: Cyber security specialists often educate employees on best practices for cyber security, such as creating strong passwords and identifying phishing scams.**

Pathways


Bachelor's Degree in Computer Science, Information Technology or Cyber Security (3-4 years full time)
VET course such as a Certificate IV in Cyber Security (6 months full time)
Intensive Cyber Security Bootcamp (12-24 weeks full time)
Work placement or internship (typically 3 months)
Graduate/Entry role in Cyber Security
Progress into more senior roles
Security Manager
Security Architect
Chief Information Security Officer

Activities

Task 1: Recognise a phishing email

Introduction

Phishing emails are a form of cybercrime in which attackers pretend to be real organisations or people to deceive recipients into revealing valuable information, such as passwords, credit card details, or personal information. Sometimes these emails will attempt to have people click on a link that will download malware or take them to a malicious website. They pose a significant cybersecurity threat as they can often lead to financial loss, data breaches and identity theft. Detecting threats and training staff members to recognise suspicious emails are important parts of many cyber security roles.

Activity

In this task, you'll learn how to successfully identify a phishing email. To get started, visit the interactive quiz below and aim to get all 8 questions correct. You'll need to check for common signs of phishing, such as poor grammar, a suspicious email address, an unfamiliar or impersonal greeting, or requests for a transfer of funds or login credentials.. Often phishing emails will try to rush the recipients so they don't notice the warning signs of a scam – check for urgent language.

Activity Link

Conclusion

Cybersecurity professionals within organisations often work on strategies to prevent phishing attempts. This might include training for employees on how to detect malicious emails, or security solutions like blocking unknown email domains. Phishing can have a massive impact on businesses, no matter how large or small so being aware of phishing attempts is a must as a cyber security specialist. Start getting some phishing recognition practice in on the day-to-day by checking your personal emails for any suspicious signs of phishing – you could save yourself from an attack!

Task 2: Make cybersecurity decisions

Introduction

Decision-making is one of the most important skills for cybersecurity specialists. A good cybersecurity specialist is able to assess risks, decide how to respond to security incidents, choose the best security measures, and allocate resources effectively. They also have to make sure they follow laws and regulations, plus create long-term strategies to protect organisations. Good decision-making helps them identify and fix problems quickly, prevent attacks, and keep everything secure.

Activity

In this 'choose your own adventure style game', you'll get to decide how a company responds to real world security scenarios. These are the kinds of decisions you'll be able to impact in businesses as a Cyber Security Specialist. Head through to the Microsoft Training Arcade and select 'In The Crosshairs' to get started.

Conclusion

Effective decision-making is a crucial skill for cybersecurity professionals. When making decisions, they have to take into consideration multiple factors such as the interests of stakeholders, and the wider business impact. Security should always be the number one priority, even if finances and resources have to be sacrificed as a result.

Task 3: Investigate a cybersecurity incident

Introduction

When cybersecurity professionals investigate incidents, they follow a step-by-step process. First, they identify and report any suspicious activity or security breaches. Then, they work to contain the incident and limit any further damage. They make sure to preserve evidence, like logs and files, so they can analyse it later.

Next, they carefully analyse the evidence to understand how the incident happened and how extensive it was. They also search for any hidden threats or signs of ongoing attacks. They try to find the root cause of the incident, like a vulnerability or mistake that allowed it to occur.

Once they understand what happened, they develop a plan to fix the problem and make sure it doesn't happen again. They patch systems, update security settings, and provide training to help people stay safe. Throughout the process, they document everything they find and create a report to share what they learned and how to prevent similar incidents in the future.

Activity

In this task, you'll play an interactive game that simulates what it's like to investigate a cybersecurity crime.

The nation's largest e-retailer, Best for You Organics, is under attack! Gather clues and evidence to investigate a ransomware attack. Use Microsoft tools, like Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Purview compliance portal to find the culprit, configure compliance policies, remediate the attacks, and protect against future cybersecurity incidents.

Visit Microsoft's training arcade and select 'Keeping Up Appearances' to get started.

Conclusion

Just like in the game, real-life cybersecurity specialists often respond to ransomware attacks and suspicious web shell activity. Beyond investigating security breaches, it's important for cybersecurity professionals to document and learn from them so organisations can continue to strengthen their systems.

If you'd like to continue learning, Microsoft have another simulation called 'In the Crosshairs' which continues the cyber security work you undertook at Best for You Organic in a new cybersecurity attack. Just head back to Microsoft's training arcade and select 'In the Crosshairs' to get started. Don't forget to come back for your Cyber Security Specialist Virtual Work Experience certificate once you're done!