



Cyber Attack and Scam Awareness Training

The rise, in cybercrime is becoming a concern for organizations of all sizes. We use the internet every day often unaware of the risks involved. Cybercrime is. Can take on forms, such as data breaches or compromised customer accounts, which can cause financial havoc and directly impact your organization.

The 'Cyber Attack and Scam Awareness course aims to equip you and your employees with the knowledge to protect yourselves against cyber adversaries. This one-day training program will educate you on how hackers and malicious bots can infiltrate your systems and provide you with strategies to safeguard your information from fraud.

In today's business landscape it is crucial for companies regardless of their size to have an understanding of cybersecurity and its impact on operations. This course is tailored to strengthen you and your staff against the tactics used by cybercriminals. Your vigilance can act as a shield to protect your company's data from falling into the hands of cyber threats. Prepare yourself against the dangers that exist in the world.

Course Overview;

We will begin our journey with introductions, from participants and an overview of the workshop's agenda. Participants will also have an opportunity to outline their personal learning goals.

Throughout this workshop you will be guiding participants to;

- Understand their responsibilities and grasp the risks associated with cybercrime.
- Recognize potential threats that arise from cyber activities.
- Strengthen their network against malware intrusions by utilizing malware defenses.
- Explore the complexities of data access levels and limitations.
- Identify security measures, for remote or home-based work.
- Describe the security threats and the steps to counter them effectively.
- Identify vulnerabilities in their network or devices. Take appropriate remedial actions.

Targeted Email Phishing & Social Engineering;

In our segment we will uncover the tactics employed in targeted email phishing and provide participants with the ability to identify indicators to spot such deceptive emails in the future.

Email Compromise for Business;

This module delves into the manipulation tactics used by scammers to initiate data transfers equipping participants with skills to prevent attempts.

Phishing Attacks with Cybersecurity Awareness;

During this session participants will gain insights into strategies, for evading phishing attacks.

Instant Messaging;

This module explores how hackers can exploit messaging platforms using techniques to those used in phishing emails.

Smishing;

Participants will learn how to identify SMS messages and take countermeasures.

Red Flags;

In this session participants will learn how to recognize the emotions that social engineers use to manipulate them as gain knowledge on how to identify and respond to phishing attacks aimed at their computers.

Human firewall is the last line of defense;

Emphasizing the importance of cybersecurity defense strategies, for businesses the final session highlights that scammers and cybercriminals target both small enterprises equally.

Workshop Conclusion;

By the end of the course participants will have the opportunity to ask any remaining questions, for clarification and create a plan of action for implementing what they've learned.

Visit <https://paramounttraining.com.au> for more information or call 1300 810 725