CYBER SECURITY AWARENESS

LEARNING OUTCOMES

By the end of this course participants will be able to:

* Describe what cybersecurity is and why it is important to be aware of it.
* Understand what the risks are with using computers
* Identify the different forms of cybersecurity attacks and incidents.
* Understand how cyberattacks occur.
* Identify suspicious activity
* Describe different actions to protect both personal and work from cybersecurity incidents.
* **Increase** overall awareness

BUSINESS OUTCOMES

By implementing this course an organisation can:

* Ensure all workers have a sound knowledge of how to prevent a cybersecurity incident
* Ensure any cybersecurity incident is deal with efficiently and effectively
* Apply knowledge and methods provide to avoid incidents from eventuating
* Protect against negative consequences of a cybersecurity incident.

PREREQUISITES

None

DURATION

2 hours

COURSE OUTLINE

* History of computers and cyber-crime
* What is Cyber-Crime?
* What are the risks?
* How does it happen?
* Identification of phishing attempts and other forms of cyber-crime
* Australian regulations regarding email and cyber security and legal obligations
* Consequences of a cybersecurity breach
* Limiting the risk within organisations
    - Password security
    - Software updates
    - Vigilance
    - Protecting client data
* Case studies
    - Top hacks of the past year
    - Phishing email – case study
    - Viewing of live internet traffic