ARGONAUT
Training & Consultants

BASIC CYBER SECURITY TRAINING

This is a two-day training designed for private individuals, businesses and organisations who require internet connectivity to conduct their daily work and home routine. The objective of this training is to enlighten and educate participants of the ever-evolving threat of cybercrime, how it affects individuals and businesses, why cybersecurity is a must, the proactive and reactive measures available.

We live in an ever-connected world where personal and company sensitive information has become currency for hackers and criminal groups. It is crucial to understand how to protect this information from being harvested and misused. This training will examine who are the likely targets of cybercrime, malware, social engineering, phishing and others cybercrime terminologies etc. Interactive Content include videos of live demonstration to make it more interesting and memorable for the trainee. We demonstrate how it's done, why it's done, and how a trained user might be able to spot the red flags in each of attacks methods.

INSIGHTS TO BE GAINED

- How to Identify social engineering red flags in emails, digital messages, over the phone and in-person attacks.
- How cyber criminals harvest sensitive information
- What they do with stolen information
- Identifying malicious malware
- How to protect personal and business information
- Preventing 'harvesting" during inflow and outflow of information

WHO SHOULD ATTEND

- Project Teams
- Accountants and Teams working in Finance
- Family, especially children
- Receptionists
- Support and administration staff
- Executives and managers

ABOUT THE FACILITATOR

George Paul de Lang is the CEO of Cyber Intelligence Systems, a managed security service provider based in Johannesburg. He is an expert in cyber security. He is passionate about sharing his knowledge of cybercrime and security. His focus is on, though not limited to, detecting and responding to advanced cyber security threats. He works with numerous local and international companies assisting them in developing and maintaining cyber security policies as well as conducting cyber threat analysis.

AGENDA

- ***Module One:* Exposition and context of Cyber Crime**
- Defining Cybercrime
- Recognising cybercrime methods
- Learning to identifying who and what type of information cybercrime targets
- Understanding how cyber criminals "harvest" sensitive information/data.
- Understanding how stolen information/data is used
- Understanding how cybercrime affects private individuals and organisations.

***Module Two:* The issue of Social Engineering**

- What is Social Engineering?
- Understanding Social Engineering tools
- Understanding how these tools operate
- Identifying ways to defend yourself from social engineering
- Proactive measures of defence
- Reactive measures

Module Three:
Case Study / Interactive session

- Exposition on cybercrime losses
- Question and answer session
- Practical work (if any/applicable)

***Module Four:* Scamming**

- What is scamming?
- Learning to recognise types and variation of scams
- Understanding scamming methods
- Learning how to avoid scams
- Understanding why scammers succeed
- Scamming terminologies
- Overview of a source code
- Learning how to identify a fraudulent source code

***Module Five:* Cybersecurity**

- Defining Cybersecurity?
- Understanding the necessity for cybersecurity awareness
- Understanding cybersecurity measures and advantages
- Learning how to incorporate a security policy for safe computing at home and organisations
- Components of a security policy
- Formulating and enforcing a security policy that fits
- User training
- Understanding security tests
- Monitoring techniques

***Module six:* Case study/Interactive session**

- Question and answer session
- Practical work (if any/applicable)
- Questionnaire