CYBER SECURITY
AWARENESS TRAINING
FOR EMPLOYEES MADE EASY!

ONLINE COURSE - WORK AT YOUR OWN PACE

CYBER SECURITY AWARENESS TRAINING INCLUDES:

- FULL Access to all Cyber Security Lessons
- **FREE** POPI Compliance Training Videos
- **FREE** POPI Compliance Toolkit
- **FREE** Cyber Security Printable Posters
- **FREE** Cyber Security Social Media Pack

eset Authorised Partner

TRAINING FOR EMPLOYEES

Introduction

We've listened to the hundreds of companies we have worked with over the last 20 years who wanted a solution to protect their valuable data. Over these two decades, we've worked with thousands of staff, training them and helping solve their IT technical issues. We prepared this course based on real life scenarios that users come across on a daily basis.

Cyber Security Awareness Training for Employees is not negotiable any longer. Every single day, we hear of companies being hacked and losing precious data – or being held to ransom by unscrupulous hackers.

Did you know that about **90% of cyber-attacks** infiltrates an organisation **via email?**

Yes! Just one single innocent click by any one of your staff can result in theft of your valuable data. For most businesses, this would be a catastrophe!

This course has been specifically designed to teach you and your staff how to avoid becoming a victim to these new cyber criminals that are constantly trying to break into your business.

Our course is completely user-friendly and will meet the needs of even the most novice end-user.

SA has the highest number of targeted ransomware, business email cyber-attacks in Africa!

South Africa has the third-highest number of cybercrime victims worldwide, costing the economy at least R2.2 billion a year.

Nearly all successful cyber-attacks worldwide are caused by human error. Clicking on an unsafe link or accidentally disclosing sensitive personal or financial information to a threat actor can lead to infected devices, being locked out of online accounts and even breaches of one's online banking profile.

eset Authorised Partner

JC AUDITORS ISO 9001 CERTIFIED

TRAINING FOR EMPLOYEES

Cyber Security Training

WARNING: VIRUS FOUND

Our Cyber Security awareness training is designed to educate you about matters relating to information security.

This training aims to raise awareness of the various potential internal and external security risks to your organisation, including email scams, malware, weak passwords, and insider threats. It will equip each employee to identify cyber risk and avoid exposing your business to criminals.

Our training has been designed with the non-technical person in mind, with amazing animation lessons and simple practical ways to keep you safe. Staff won't be happy if you dump another 20 hour training session onto them, that's why we kept each lesson short and informative. Long, lengthy lectures are often ineffective, that's why we kept each lesson short, crisp and infromative - delivering maximum impact.

Did you know that about 91% of successful data breaches started with a phishing attack ?

Lesson 1
What's wrong with using the same password EVERYWHERE?

Lesson 2
Has your password been leaked online?

Lesson 3
How to choose a password?

Lesson 4
Why you should STOP saving your passwords in your browser!

Lesson 5
Think Before You Share Your Password.

Lesson 6
What is Vishing?

Lesson 7
Callback Attacks

Lesson 8
What is a Password Manager and how to use it.

Lesson 9
What is Two-factor authentication (2FA)?

Lesson 10
Phishing Scenarios

Lesson 11
Travel Scams – Don't get caught!

OVER 35+ LESSONS
Cyber Security Training for Staff MADE EASY!

Validated by:

The course has been validated by the QMS experts at JC Auditors, an internationally accredited ISO 9001 certification body. So, you have peace of mind that the content is world class! To ensure that the course delivers maximum impact and value, we have used stimulating visuals, fun animated videos and real-life scenarios in a user-friendly interface.

eset Authorised Partner

TRAINING FOR EMPLOYEES

POPI Compliance Videos

POPI TRAINING

1. The Protection of Personal Information Act was introduced in 2013 and has seen a growth in its implementation in recent years.

2. The POPI Act requires every public and private body to provide staff with relevant necessary data protection training.

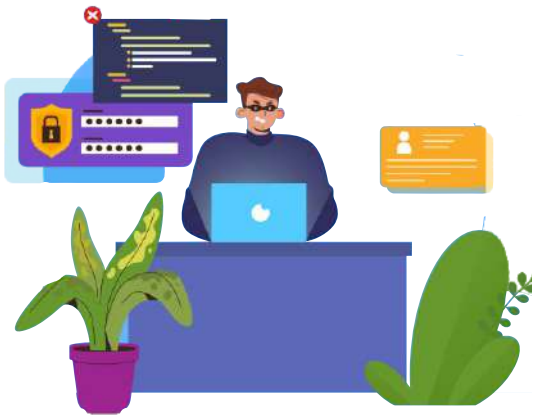
3. This training walks you throught the entire POPI Act without all the technical lingo, increasing your competency in interpreting and applying POPIA, developing the expertise to correctly implement POPIA, and growing your capability to better assist data subjects.

4. These training sessions have been developed to enable businesses to have a good understanding of the essential requirements of the POPI Act.

POPI TRAINING INCLUDES

What is the POPI Act all about?
Why do we need the POPI Act?
Who will be affected by the Act?

Chapter 1:	Definitions and Purpose
Chapter 2:	Lawful processing, Rights of data subjects and Exclusions.
Chapter 3:	Conditions for Lawful Processing of PI.
Chapter 4:	Exemptions
Chapter 5:	Supervision, Information Regulator and Information Officer.
Chapter 6:	Prior Authorisation
Chapter 7:	Codes of Conduct
Chapter 8:	Rights of Data Subjects: Direct Marketing.
Chapter 9:	Transborder Information Flows
Chapter 10:	Enforcement
Chapter 11:	Offenses, Penalties, and Administration Fines.
Chapter 12:	General Provisions



ESET Authorised Partner

Presented by:

JC AUDITORS ISO 9001 CERTIFIED

TRAINING FOR EMPLOYEES

FREE Course Material

1 FREE POPI TOOLKIT

The majority of South African companies/organisations are required to abide by the Protection of Personal Information Act (POPIA), often known as the POPI Act.

Under POPI, it is against the law to gather, utilise, or store a customer's or business's personal information unless it complies with the rules and prohibitions outlined in the Act. Our POPI Toolkit includes templates, policies, procedures, forms, and agreements required, along with step-by-step instructions and an action plan to make the POPI compliance process easier for you. You can save thousands in consultant fees, policy and contract writing time, and other costs by using the POPI Act Compliance Toolkit. The toolkit will be made available to you via a download link after you have completed your purchase of ANY of our cybersecurity courses.

Full editable POPI Documents

2 PRINTABLES POSTER + SOCIAL MEDIA KITS

Posters are an easy way to keep good digital habits top of mind, between awareness training courses.

Print them out and hang them up around the office and create a culture of security with awareness.

We also included the social media pack which includes posts that you can share on your social media networks, internal intranet and WhatsApp.

SAFETY STARTS WITH AWARENESS
AWARENESS STARTS WITH YOU...
DON'T GET HOOKED!

PROUD MEMBER PMCB PIETERMARITZBURG & MIDLANDS CHAMBER OF BUSINESS

eset Authorised Partner

TRAINING FOR EMPLOYEES

CHECK LIST
PROTECT YOUR PC AND MOBILE

Protecting your business PC is essential for several reasons:

Data security: A business PC often contains sensitive information such as financial data, customer information, and trade secrets. Protecting your business PC helps to prevent data breaches and leaks, which can result in significant financial losses and damage to your business reputation.

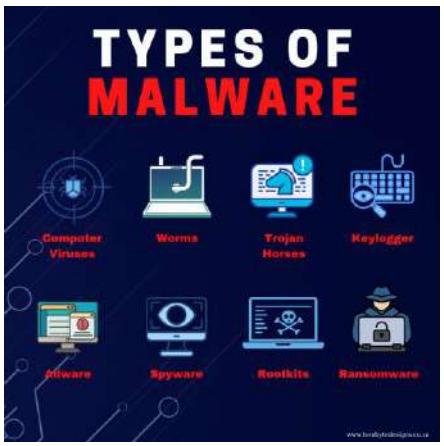
Productivity: Malware and other cyber threats can significantly impact the performance of your PC, resulting in lost productivity and downtime for your business.

Legal compliance: Depending on your industry, you may be required by law to protect certain types of data. Failing to adequately protect your business PC can result in legal and financial consequences, including fines and lawsuits.

Task	✓
Install an up-to-date Anti-Virus software: Make sure that you have an antivirus program installed and it is up to date with the latest virus definitions. We DO NOT recommend FREE Anti-Virus.	
Enable Firewall: Ensure that your firewall is enabled on your PC to block unauthorized access to your network.	
Keep the operating system up to date: Regularly install updates to your operating system and software to ensure that any vulnerabilities are patched.	
Setup passwords to access your PC or any biometrics.	
Use a VPN: Use a virtual private network (VPN) when accessing the internet on public Wi-Fi or other unsecured networks. (Example: SurfShark)	
Backup important files: Back up important files regularly and keep them in a safe location.	
Use Windows 10 or Higher - Putting off upgrading to the latest operating system can put you in a very vulnerable position as you will effectively raise a red flag to hackers who could potentially attack your device with ease remotely. Support for Windows 7 ended on January 14, 2020.	
Avoid downloading files from unknown or untrustworthy sources to avoid potential malware on your device.	
Do not connect unknown USBs or other devices to your computer.	
Never let kids or ANYONE use the same profile you use for business. Never let kids install games on a work PC.	
Before installing Apps on your mobile device consider whether it's reasonable for that application to have access to your personal information. (Photos, GPS, storage, etc.). Google "Apps Contain Malware".	
Shut down your computer if you are not using it for more than a day. (Saves energy and reduces your attack surface) (If they can't find you, they can't steal your data)	
Set up a separate email account for dating sites, mailing lists, coupons, etc. Never use your work email for personal use.	

CHECK LIST

PROTECT YOUR PC AND MOBILE



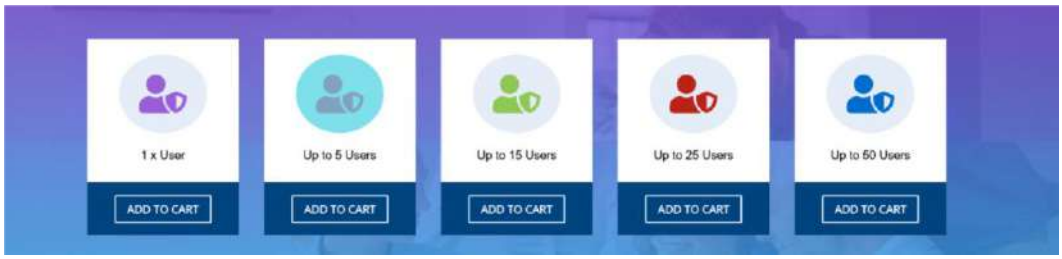
eset Authorised Partner

TRAINING FOR EMPLOYEES

GETTING STARTED

1 PLACE YOUR ORDER

Place your order at www.terabytedesigns.co.za or email info@terabytegroup.co.za



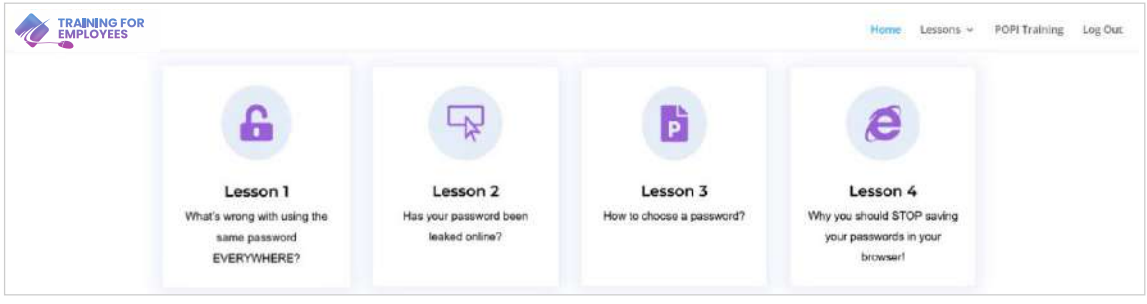
2 SIGN IN

Once your order is approved, your will receive a username and password.

https://www.terabytegroup.co.za/learn

3 START LEARNING

Select a lesson from the main menu or home page.



TRAINING FOR EMPLOYEES

T: 087 222 6877
E: info@terabytegroup.co.za
W: www.terabytedesigns.co.za

eset Authorised Partner

COURSE CHECK LIST

SECURE YOUR DIGITAL LIFE

Task	✓
I know why I should note use the same password EVERYWHERE	
I checked if my password has been leaked online	
I know how to choose a strong password	
I have removed my saved passwords from my browser	
I will not share my passwords with ANYONE	
I understand what Vishing and Callback Attacks	
I understand what a Password Manager is and how to use it	
I have setup 2-FA on all my accounts	
I have printed a set of Backup Codes for all my accounts	
I understand what Phishing is and how to identify these kind of e-mails	
I understand the concept of Malware	
I understand Business Email Compromise, and that I should never act without authentic confirmation.	
I understand how to stop a travel scam	
I understand what a VPN is and why I need it	
I know how to keep safe on social media	
I understand the importance of backing up my company data	
I understand the basics of keeping my PC safe	
I understand how and why I should keep my mobile safe	
When e-mailing I know how to use BCC and the danger of CC	
I understand the basics of the POPI Act	

eset Authorised Partner

TRAINING FOR EMPLOYEES