# Information Security Essentials for Corporate Users

*Skills and expertise to help you increase your users knowledge in the field of emerging security threats*

Education & Training Services

## About this workshop

In the era of digital transformation, the importance for having substantial knowledge on cybersecurity and information security is becoming essential skills to acquire for every corporate user. The reason behind is the protection of information and organizational reputational brand which is now considered as one of the critical function for all enterprises and as a part of their corporate vision and enterprise strategy.

Corporate end users are the first line of defense against cyberattacks that target your endpoints, such as phishing, malware, ransomware, or data breaches. If they are not aware of the signs and symptoms of these attacks, or how to respond to them, they can compromise your network, your data, and your reputation. Educating and training your end users on endpoint security awareness and best practices can help you reduce the likelihood and impact of these attacks, as well as improve your compliance and governance.

*An outsider's perspective can bring unexpected value to your organization*

In a nutshell, this workshop is mandatory for all back-office corporate users who are carrying corporate endpoint devices using corporate network accessing corporate data sensitive applications.

## After completing this workshop, you will be able to:

- Understand essential information security and cybersecurity concepts.
- Recognize malware analysis concepts and methodology used by hackers and classify types of different incidents.
- Distinguish system and application security threats and vulnerabilities.
- Be aware of the basic concepts, practices, tools, tactics, techniques and procedure used today by cybercriminals.
- Elaborate basic security principles, guidelines and procedures to safeguard data and know why data encryption tools are mandatory.
- Understand Identity Theft Protection and how Multifactor Authentication will reduce the overall implications with typical scenarios.
- Exploiting "Users" role in Information Security.

## Why this two-day workshop is important for your corporate users

Endpoint security is a critical aspect of IT security operations, as it protects the devices and data that your end users access and store on a daily basis. However, endpoint security is not only a technical matter, but also a human one. Your end users need to be aware of the threats and risks that they face, and the best practices that they can follow to prevent or mitigate them. In this two-day workshop, we will discuss how we can educate and train your end users on endpoint security awareness and best practices, and why it is important to do so.

## Workshop details:

### Unit 1 – Understanding the Role of Information Security and Cybersecurity

- World is getting instrumented, interconnected & intelligent.
- Exponential Data Growth – Some key facts and figures.
- The evolution of storage technology and future predictions.
- Assume a world without a security.
- Most Frequently Targeted Industries in 2018.
- Why a security is becoming a board room discussion.
- Key Security Concerns for the Executive Management.
- Security Vs. Safety in a view.
- How to avoid Social Engineering & Malicious Software.
- Hacker tricks to avoid – Recommendations.
- Understanding Cybersecurity and Cyberspace.
- Differences between Information Security and Cybersecurity.
- Multiple layers of protection offered by Security Solutions.
- Why securing your environment is important?
- What is Information Security.
- Why you need to make security a priority.
- Types of cybersecurity threats and Malware Detection.
- Why is Cyber Resilience needed.
- Top 11 ways poor security issues that can harm you.
- Security – Defense in depth.
- Cyber Security Awareness – The 6 Layers.
- Blueprint for Cybersecurity Success.
- What are the objectives of Cyber Security?
- How Web 3.0 will change our lives?
- Adoption of Cybersecurity best practices.
- Cybersecurity Awareness – Summary.
- 5 Questions you should ask your Services Provider.
- Careers in cybersecurity.
- Typical Cybersecurity roles in the industry.
- Unit 1 Assessment.

### Unit 2 – Essential Security Principles and Guidelines

- Why Data Protection is important?
- What are best practices, guidelines, frameworks and security controls.
- Understanding guidelines principles.
- Basic guidelines for setting up a user password.
- Tips for keeping your password secure.
- The top seven key security principles.
- Understanding Data Encryption and types of encryptions.
- Describing Symmetric and Asymmetric Encryptions.
- End–to–End Encryption Explained.
- The 8 Principles of Cybersecurity Laws.
- Goals and Principles of Cybersecurity – The larger picture.
- About National Response Center for Cyber Crime – Pakistan.
- Cybersecurity Standards, Frameworks Guidelines and Controls.
- Types of Cybersecurity Controls and their examples.
- Describing Identity Theft Protection.
- Understand Multifactor Authentication and scenarios.
- Unit 2 Assessment.

*Opportunities are made, not found*

# Information Security Essentials for Corporate Users

*Skills and expertise to help you increase your users knowledge in the field of emerging security threats*

TLC
Education & Training Services

## Target Audience for this workshop

Corporate users from business, finance, procurement, digital, application and database, audit, risk, compliance, IT operations, software development, project management, legal and HR professionals, including new fresh hires in these line-of-businesses with a familiarity of basic IT/IS concepts who want to;

- Learn new trends in information security and cybersecurity.
- Understand users role in information security.
- How deal with vulnerabilities, risk and threats.
- Security guidelines and principles.

**Security** is a team effort and a **shared responsibility** to **protect** your **brand**.

***"Endpoint users are usually found as a weakest link in Cybersecurity"***

## About the instructor

Training will be delivered by an experienced trainer with 25+ years of career experience imparting education and training services both locally and internationally and have served international enterprise technology vendors including IBM, Fujitsu, and ICL.

Our instructor holds various industry professional certifications in the space of enterprise servers and storage technologies, Information Security, Enterprise Architecture, ITIL, Cloud Computing, Virtualization, Blockchain, Green IT, IBM AIX and a co-author of 10 IBM Redbooks.

The training course flow will be a mix of lectures, classroom discussions and video demonstrations so that participants can have a detailed understanding of various components enabling them to maintain a cyber hygiene of there corporate devices to combat against cyber threats.

## Unit 3 – Dealing with Risks, Threats and Vulnerabilities

- Examining the Cost of a Data Breach.
- To address security threats, leaders must avoid following common myths.
- Use five fundamental security principles to help guide you.
- Juice Jacking Explained: Why You Should Avoid Public USB Ports.
- How to Identify False DNS-based Phishing Attacks.
- Understand Incidents, Breaches, Risk & Vulnerability.
- Types of Cybersecurity and their Specific Domains – Risk and Threats.
- Threats, Motives and Methods.
- Threats and security challenges faced today.
- Understand Threat management and Different threat levels and risks.
- Knowing security threats and their channels.
- Understanding Security Elements – The larger picture.
- Attack Progression Model used by Cybercriminals.
- Types of Cybersecurity Attacks.
- Risk Management: Know your risks.
- Understand the role of Risk Management.
- Defense Planning – Risk Analysis and Assessments.
- Risk Management Approach, key objectives and benefits.
- A small backdrop on ISO 27001.
- Qualitative Risk Assessment – Simple and Detailed Risk Assessment
- Possible vulnerabilities that one cannot ignore.
- Types of Comprehensive Vulnerability Assessments.
- Threat, Risk and Vulnerability – A High Level Summary.
- Unit Assessment 3.

## Unit 4 – Corporate Users Role in Information Security

- What do your device know about you.
- Assess and mitigate vulnerabilities in mobile systems.
- Endpoint security issues caused by users.
- Common Breach Vectors – Statistics that you cannot ignore.
- The Role of Authentication and Authorization.
- What is Role?
- Understanding "Users" role in Information Security.
- Differentiating between the role of Data Steward and Data Custodian.
- Users role in Information Security.
- Safeguarding Institutional Data.
  - Protecting Electronic Data, Safeguard your Passwords, Secure Your Computer, Protecting Physical Data, Disposing of Data (Data Sanitization).
- Safeguarding Electronic Communications.
- Understand Role Based Access Control.
- Traditional approach to UNIX Administration.
- RBAC Administration advantages.
- RBAC Framework.
- Understanding Roles & Authorization
- RBAC – A Generic Behavior.
- Avoid Risky Behavior Online.
- Block or allow pop-ups in your Web Browsers – An important step.
- Check and remove malware from your computer – Windows.
- Report any Suspected Security Breach.
- Adhere to the Computing Policy.
- Tips to help you stay more secure online – A Brief Summary.
- Additional Information – Guidelines.
- Typical Cybersecurity roles in the industry.
- Unit 4 Assessment.

## The importance of this workshop

Every business must confront the three major workplace security issues – staff safety, asset security, and the protection of data and other valuable information. These security issues require a robust workplace security system to avoid any risk to a business, which may be physical damage, robbery, theft, or system hacking. Both physical and logical security is arguably the most critical aspect of workplace safety. In this workshop, we will take a closer look at the importance of security in the workplace and expand upon some of the more important elements.

## Detail Information

| | |
|---|---|
| Course Code | : TN226 |
| Course Duration | : 2 Day Online Workshop |
| Course Location | : TLC, Customer On-site and Online. |
| Terms & Conditions | :100% payment in advance. |
| Course Deliverable | : Comprehensive Student Guide and Course Certificate |

For additional information, please write to us at: info@tlcpak.com

*Opportunities are made, not found*