# *Cybersecurity: Fundamentals for Employees*

**Course Description**

Cybersecurity: Fundamentals for Employees explores the world of cybercrime. This one-day course will ensure that staff gain an appreciation of company-wide measures to protect against cyberattacks and their own role in the success of these defense measures.

Most importantly, it will help staff recognize phishing attacks and understand what steps to take to mitigate the effect when a cyberattack has been successful. It emphasizes the importance of practicing safe social media behavior to prevent cyber criminals from mining sensitive personal and company data.

**Course Outline**

**Session One: Course Overview**
Course Overview
Learning Objectives
Pre-Assignment
Pre-Course Assessment

**Session Two: The State of Cybercrime**
History of Cybercrime
Recalling Cybercrimes
Historical Examples of Cybercrime
Cost of Cybercrime

**Session Three: Types of Cyberattacks**
Types of Attacks

**Session Four: Role of Human Error**
The Role of Human Error
Opening Email

**Session Five: What Can a Company Do?**
Company-wide Defenses
Other Company-wide Defenses
Focus on Social Media
Create a Social Media Policy

**Session Six: Best Practices for Remote or Travelling Employees**
Out of Office Protections

**Session Seven: Scenarios**
Scenario: Malware
Scenario: Potential Data Breach

**Session Eight: Cyberattacks on Individuals**
Cyberattacks to Obtain Sensitive Information
Malware (Malicious Software)
Social Media
Social Media Scams

**Session Nine: Recognizing Phishing Attacks**
The Giveaway Clues to Phishing Attacks
Spot the Clue
Phishing Emails

**Session Ten: What Can a Person Do?**
Supporting Company Efforts
Social Media
Focus on Spear Phishing
How to Protect the Organization
Social Media Safety

**Session Eleven: Creating a Personal Cybersecurity Plan**
Cybersecurity Starts with You!
Personal Action Plan
Course Summary
Recommended Reading List