

COURSE OUTLINE

Securing Your Digital Presence Online



Securing Your Digital Presence Online

Duration: One day (9:00 AM to 5:00 PM)

Method: Instructor-led

Mode: Physical/Virtual

Level: Beginner

Instructor: Ali Reza Azmi

Overview

This one-day course empowers participants to understand and implement practical strategies to protect their digital presence. Designed for professionals and individuals concerned about online privacy and cybersecurity, this course covers essential topics such as secure browsing, managing passwords, identifying threats, and protecting personal and organizational data from cyberattacks.

By the end of the course, participants will be equipped with the knowledge and tools to safeguard their digital identities and minimize risks in an increasingly interconnected world.

Course Objectives

- Explain the fundamentals of online security and why it is critical in today's digital age.
- Provide actionable tips for protecting personal and professional information online.
- Help participants identify and mitigate potential cybersecurity threats.
- Introduce tools and best practices for managing digital privacy and security.

Who This Course Is For

This course is designed for:

- Professionals and individuals who want to protect their personal and professional digital presence.
- Business leaders seeking to implement secure practices for their teams and organizations.
- Anyone interested in understanding online risks and how to stay safe in the digital world.

Prerequisites

- No prior knowledge of cybersecurity or IT systems is required.
 - Basic familiarity with using the internet and common digital tools is recommended.
-

Module 1 — Understanding the Risks to Your Digital Presence

Overview:

- What is a digital presence? Why does it matter?
- Common threats: Phishing, malware, ransomware, and data breaches.
- Real-world examples of cybersecurity incidents and their impacts.
- The importance of proactive digital security in daily life.

Practical Activity:

- Group exercise: Analyze a simulated phishing email to identify red flags.

Learning Outcome:

Participants will understand common digital threats and their potential consequences, enabling them to take proactive steps to mitigate risks.

Module 2 — Strengthening Your Digital Defenses

Overview:

- Secure browsing practices: Using HTTPS, avoiding public Wi-Fi, and using VPNs.
- Password management: Creating strong passwords and using password managers.
- Multi-factor authentication: What it is and why it's essential.
- Safe file sharing and email practices.

Practical Activity:

- Interactive demo: Participants will evaluate password strength using a tool and set up multi-factor authentication for an account.

Learning Outcome:

Participants will learn and practice basic strategies for protecting their accounts and devices from unauthorized access.

Module 3 — Protecting Your Personal Data Online

Overview:

- Managing social media privacy settings.
- Recognizing oversharing and its risks.
- Understanding terms of service and app permissions.
- Protecting sensitive information from social engineering attacks.

Practical Activity:

- Hands-on session: Review and adjust privacy settings on a social media account or app.

Learning Outcome:

Participants will learn to safeguard their personal information and maintain privacy across various platforms.

Module 4 — Staying Vigilant Against Emerging Threats

Overview:

- Identifying suspicious activity: Warning signs of hacking attempts.
- Keeping your devices secure: Software updates, firewalls, and antivirus tools.
- Avoiding scams: Spotting fake websites and fraudulent links.
- Cybersecurity trends: What to watch out for in the future.

Practical Activity:

- Group discussion: Share common scams or suspicious activities participants have encountered and analyze how they could have been avoided.

Learning Outcome:

Participants will be equipped with the knowledge to detect and respond to emerging digital threats effectively.

Closing Remarks

- Summary of key lessons.

- Open Q&A session for addressing participants' specific concerns.
- Recommendations for further resources and tools to enhance cybersecurity.



HARMONIZING OUR SKILLS WITH YOUR ASPIRATIONS

CONTACT US

Fahim Zulkafli

Business Operations Manager

✉ fahim@twenty-four.io

☎ +60 13 526 6350

Scan the QR code or register via:
<https://twenty-four.io/contact/>



Twenty-Four Consulting PLT
(202404000540)

No. 8, Jalan Yap Kwan Seng,
31st Floor, Menara Ambank
50450 Kuala Lumpur
W.P. Kuala Lumpur

Our webiste:
twenty-four.io

Follow us here:



COURSE OUTLINE

twenty-four.io