Cyber Hygiene & Safe Practices at Work

Best For

This program is ideal for:
Early to mid-career professionals
Non-technical staff across all departments
Professionals working in digital, hybrid, or remote environments
Organizations strengthening everyday cybersecurity awareness

Delivery Style

The learning experience is highly practical, awareness-focused, and designed to help professionals adopt safe digital behaviors as part of their daily work routines — without technical complexity.

Outcome Level

Participants develop stronger cybersecurity awareness, improved digital responsibility, and the ability to reduce everyday cyber risks through consistent, safe work practices.

Program Positioning

Most cybersecurity incidents do not begin with sophisticated hacking — they begin with everyday unsafe behaviors such as weak passwords, careless clicking, unsecured devices, or poor data handling. Cyber hygiene refers to the routine digital habits that protect individuals, teams, and organizations from preventable cyber threats.

This program is designed to help professionals understand **how their daily actions directly affect cybersecurity**. It focuses on practical awareness, risk recognition, and habit-building — rather than technical systems or IT controls.

The content reflects modern workplace realities across the USA, Australia, Canada, and global organizations, where cybersecurity is everyone's responsibility, not just the IT team's.

✅ Ideal for professionals with 0–15 years of experience
✅ Ideal for organizations building a strong cybersecurity culture

LEARNING STRUCTURE (8 HOURS)

Block 1 — Understanding Cyber Hygiene in the Workplace

This session builds a strong foundation by explaining what cyber hygiene means in everyday work contexts. Participants understand how routine digital behavior either strengthens or weakens organizational security.

It covers:

- What cyber hygiene means in simple terms
- Why small actions create big security risks
- Common causes of preventable cyber incidents
- Shared responsibility for workplace security

✅ **Outcome:** Clear understanding of cyber hygiene fundamentals.

Block 2 — Recognizing Everyday Cyber Risks

This session focuses on identifying common cyber risks that professionals encounter daily — often without realizing the danger.

It covers:

- Risky email and browsing behaviors
- Unsafe downloads and attachments
- Public Wi-Fi and unsecured networks
- Social engineering warning signs

✅ **Outcome:** Improved awareness of everyday cyber threats.

Block 3 — Safe Email, Messaging & Online Behavior

This session strengthens safe communication practices across email, chat, and online platforms.

It covers:

- Identifying suspicious messages
- Avoiding unsafe links and attachments
- Verifying unexpected requests
- Practicing cautious digital communication

✅ **Outcome:** Safer and more responsible online communication habits.

Block 4 — Device Security & Workspace Protection

This session focuses on protecting devices and digital workspaces from unauthorized access.

It covers:

- Securing laptops, mobiles, and tablets
- Locking devices and screens properly
- Safe use of removable media
- Preventing physical access risks

✅ **Outcome:** Stronger device and workspace security awareness.

Block 5 — Password Discipline & Access Awareness

This session introduces responsible access behavior without technical jargon.

It covers:

- Why weak passwords create serious risk
- Avoiding password reuse
- Protecting login credentials
- Understanding basic access responsibility

✅ **Outcome:** Better access discipline and password awareness.

Block 6 — Data Handling & Information Protection

This session helps participants understand how careless data handling exposes organizations to cyber risk.

It covers:

- Handling sensitive and confidential information
- Avoiding unsafe file sharing
- Recognizing data exposure risks
- Practicing responsible information management

✅ **Outcome:** Improved data protection habits.

Block 7 — Responding to Suspicious Activity

This session focuses on what to do when something seems wrong — and why early action matters.

It covers:

- Recognizing warning signs of compromise
- Reporting suspicious activity promptly
- Avoiding panic or cover-ups
- Supporting quick incident containment

✅ **Outcome:** Faster and more confident response to cyber concerns.

Block 8 — Cyber Hygiene Action Plan

This final session helps participants convert awareness into consistent behavior.

It covers:

- Identifying risky personal habits
- Strengthening daily cyber-safe routines
- Applying best practices consistently

- Creating a personal cyber hygiene action plan

✅ **Outcome:** Clear, practical plan for maintaining strong cyber hygiene.

✅ What You Will Walk Away With

Participants complete the program with:
Stronger awareness of everyday cyber risks
Improved digital safety habits
Reduced likelihood of preventable incidents
Greater confidence handling cyber concerns
A practical approach to workplace cyber hygiene
A Knowledge Que Course Completion Certificate (8 PDUs)

✅ Certification (Delivery-Neutral & Legally Safe)

On successful completion of the program, learners receive:
Knowledge Que – Course Completion Certificate
Recognition of 8 Professional Development Units (PDUs)
A digital certificate suitable for:
LinkedIn
Resume & Portfolio
Professional Profiles
Issued by Knowledge Que – Powered by Experts

✅ Why Knowledge Que

Expert-led, practical professional skills training
Real-world workplace scenarios
Skill-focused learning with immediate application
Programs designed specifically for modern professionals

Copyright