Mobile & IoT Security Essentials

Best For

This program is ideal for:
Early to mid-career professionals
Employees using mobile devices for work
Professionals working in hybrid and remote environments
Organizations managing mobile, connected, and smart devices

Delivery Style

The learning experience is practical, awareness-driven, and focused on helping professionals use mobile and connected devices securely in everyday work without technical complexity.

Outcome Level

Participants develop stronger awareness of mobile and IoT-related security risks, improved device-handling discipline, and the ability to reduce exposure to threats created by connected technologies.

Program Positioning

Mobile devices and Internet of Things (IoT) technologies are now deeply embedded in modern workplaces. Smartphones, tablets, wearables, smart office devices, and connected tools improve efficiency — but they also introduce new security vulnerabilities when not handled properly.

Many security incidents occur because mobile and IoT devices are poorly secured, shared, lost, or misused. This program is designed to help professionals understand **how everyday use of connected devices affects organizational security**, and how small actions can significantly reduce risk.

The content reflects current workplace realities across the USA, Canada, Australia, and global organizations where mobile and IoT security awareness is increasingly essential.

✅ Ideal for professionals with 0–15 years of experience
✅ Ideal for organizations managing connected-device risk

LEARNING STRUCTURE (8 HOURS)

Block 1 — Understanding Mobile & IoT Security Risks

This session builds a strong foundation by explaining how mobile and connected devices introduce unique security challenges in the workplace.

It covers:

- What mobile and IoT devices are in work environments
- Why connected devices increase attack surfaces
- Common security risks associated with mobile usage
- Shared responsibility for device security

✅ **Outcome:** Clear understanding of mobile and IoT security fundamentals.

Block 2 — Securing Mobile Devices for Work

This session focuses on protecting smartphones and tablets used for professional tasks.

It covers:

- Locking and securing mobile devices
- Managing device settings responsibly
- Risks of lost or stolen devices
- Safe use of personal devices for work

✅ **Outcome:** Improved mobile-device security habits.

Block 3 — App Usage, Permissions & Updates

This session helps participants understand how apps and software choices affect device security.

It covers:

- Risks of unverified or unnecessary apps
- Managing permissions responsibly
- Importance of updates and patches
- Avoiding malicious or fake applications

✅ **Outcome:** Safer app usage and update discipline.

Block 4 — IoT Devices & Smart Workplace Technology

This session introduces IoT devices commonly found in modern workplaces and explains their security implications.

It covers:

- Smart office devices and connected tools
- IoT risks beyond traditional IT systems
- Shared and unmanaged device risks
- Responsible interaction with smart technologies

✅ **Outcome:** Improved awareness of IoT-related security concerns.

Block 5 — Network & Connectivity Awareness

This session focuses on secure connectivity practices for mobile and IoT devices.

It covers:

- Risks of public and unsecured networks
- Safe connectivity practices
- Avoiding unsafe Bluetooth and Wi-Fi usage
- Understanding network exposure risks

✅ **Outcome:** Stronger connectivity and network awareness.

Block 6 — Data Protection on Mobile & IoT Devices

This session strengthens awareness of how data is stored, accessed, and shared through connected devices.

It covers:

- Protecting sensitive data on mobile devices
- Avoiding data leakage through apps
- Secure file access and sharing
- Responsible data handling across devices

✅ **Outcome:** Improved data protection on connected devices.

Block 7 — Responding to Mobile & IoT Security Issues

This session focuses on what to do when a device-related security issue occurs.

It covers:

- Recognizing signs of compromise
- Responding to lost or stolen devices
- Reporting issues promptly
- Supporting incident containment

✅ **Outcome:** Faster and more confident response to device-related incidents.

Block 8 — Mobile & IoT Security Action Plan

This final session helps participants apply secure device practices consistently.

It covers:

- Identifying personal device-related risks
- Strengthening secure usage habits
- Applying awareness daily
- Creating a personal mobile and IoT security action plan

✅ **Outcome:** Clear, practical plan for secure use of mobile and IoT devices.

✅ What You Will Walk Away With

Participants complete the program with:
Stronger awareness of mobile and IoT security risks
Improved device-handling discipline
Reduced exposure to connected-device threats
Greater confidence using mobile technology securely
A structured approach to mobile and IoT security
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 mobile and connected-device scenarios
Skill-focused learning with immediate application
Programs designed specifically for modern professionals

Copyright

© Knowledge Que. All rights reserved. No part of this material may be reproduced, distributed, or transmitted without prior written permission.