



# Introductory Security Awareness Training

**Session Overview:** A concise 30-minute session designed for everyone, all roles, as a introduction and/or review of the fundamentals of cybersecurity risk and safe practices in the Primary Care Network environment.

These sessions are intended to support your PCN and the roles within it. Should you want to modify any of the agenda below, please share that information with your trainer.

## Agenda:

- **Welcome & Introduction (5 min):** Overview of why cybersecurity matters in Primary Care Network. You're the Shield!
- **Core Topics (15 min):**
  - Recognizing phishing attempts: Email, Social Engineering, Malware, Mobile Devices, etc.
  - Basics of strong password practices
  - Physical security and device management, data security
  - Reporting Incidents overview
- **Interactive Q&A (5 min):** Open discussion for immediate questions.
- **Wrap-Up & Key Takeaways (5 min):** Summary of practical tips for daily use and next steps.

## Benefits of Attending:

- Understand the importance of cybersecurity in safeguarding patient data and confidential information.
- Learn simple, actionable steps to enhance personal and organizational security.
- Empower yourself to recognize and report potential cyber threats, reducing human risk.





# Intermediate Security Awareness Training

**Session Overview:** A 60 to 90-minute interactive training session as the next step expands on the introductory concepts, expanding on the Security Mindset, developing a Security Culture, with an added high-level review of Incident Response Plans (IRP).

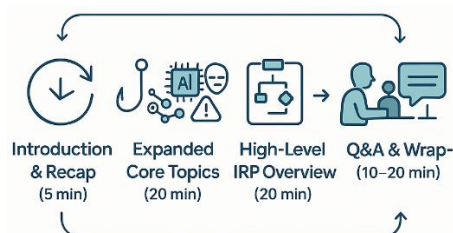
These sessions are intended to support your PCN and the roles within it. Should you want to modify any of the agenda below, please share that information with your trainer.

## Agenda:

- **Introduction & Recap (5 min):** Quick refresh of the basics covered in the Introductory session.
- **Expanded Core Topics (20 min):**
  - Exploring different types of phishing, social engineering, malware awareness, security terms, and secure work practices.
  - How AI could lead to greater security risk now and in the future?
  - Deepfake technology overview; potential use and abuse.
  - Review and deeper dive into recognizing and reporting security incidents
- **High-Level IRP Overview (20 min):**
  - What is an Incident Response Plan?
  - Key roles and responsibilities
  - Overview of critical response steps in an IRP
- **Interactive Case Study (15 - 25 min):** Optional. Role-playing exercise to practice identifying and responding to potential threats.
- **Q&A and Wrap-Up (10 - 20 min):** Discussion of best practices and lessons learned, key takeaways and what's next.

## Benefits of Attending:

- Enhance your understanding of common cybersecurity threats and risk mitigation strategies. Discuss ways to increase security and promote data security.
- Further develop you PCN's Security Maturity; enhance your Security Culture.
- Gain exposure to the basics of Incident Response Planning, crucial for immediate risk management.
- Participate in interactive exercises that simulate real-world scenarios, reinforcing learning through practice.





# Advanced Security Awareness Training

**Session Overview:** A comprehensive 3-hour training session designed for groups that have completed previous training modules OR are interested in furthering their Security Maturity. This session covers foundational topics as a review, an in-depth review of Incident Response Plans, and explores emerging cybersecurity threats with interactive exercises. This session is intended to assist PCN's on determining where they are and what their next steps could be. If you want to modify any of the agenda below, please share that information with your trainer.

## Agenda:

- **Introduction & Recap (15 min):** Overview of cybersecurity fundamentals and recent threat trends that are newsworthy.
- **In-Depth Cyber Threat Analysis (30 – 45 min):**
  - Detailed discussion on phishing, social engineering, malware, and other attack vectors the office has seen. Video demonstrations available.
  - Review of current threat landscape specific to Primary Care Network.
- **Detailed Incident Response Plan (IRP) Deep Dive (60 min):**
  - Step-by-step exploration of IRP components; update personal IRP document specific for your office.
  - Roles and responsibilities during a cyber incident
- **Emerging Threats & New Ideas (30 min):**
  - Introduction to innovative security strategies and proactive measures
  - Discussion on future cybersecurity trends and technologies (e.g., AI in cybersecurity)
- **Interactive Group Exercise (45 min):**
  - Tabletop exercise simulating a cyber incident scenario
  - Collaborative discussion and problem-solving
- **Final Q&A and Takeaways (15 min):** Recap, closing discussion and next steps.

## Benefits of Attending:

- Obtain an in-depth, practical understanding of advanced cybersecurity concepts tailored for the Primary Care Network.
- Develop, implement, and manage an effective Incident Response Plan.
- Engage in interactive exercises designed to foster collaboration and enhance real-world readiness against cyber threats.

