IT-säkerhet för personalen

KURSPLAN

Kapitel 1: Introduktion till IT-säkerhet

- ✓ Vad är IT-säkerhet? – Grundläggande principer och betydelse
- ✓ Identifiera våra motståndare – Hot och deras motiv
- ✓ Ditt värde som medarbetare i säkerhetskedjan
- ✓ Organisationens värde och exponering
- ✓ Övningsuppgifter

Kapitel 2: Förstå och förebygga cyberhot

- ✓ Olika typer av attacker – Botnet, ransomware, social engineering, phishing
- ✓ Hur attacker sker – Taktiker och mål
- ✓ Medarbetarnas identitet och integritet
- ✓ Insikter i hur phishing-företagsbedrägerier begås och hur man upptäcker dem
- ✓ Övningsuppgifter

Kapitel 3: Teknik och säkerhet i praktiken

- ✓ Uppdatera och säkra datorer och programvara
- ✓ Skapa och underhålla säkra lösenord
- ✓ Tvåfaktorsautentisering och dess betydelse
- ✓ Molntjänster – Säkert datautbyte och datalagring
- ✓ Sociala mediers roll och påverkan på säkerheten
- ✓ Övningsuppgifter

Kapitel 4: Modern teknik och riskhantering

- ✓ Hantera filterbubblor och kritiskt tänkande
- ✓ Säkert använda smartphones och tablets i och utanför arbetet
- ✓ Upptäcka och rapportera säkerhetsincidenter i tid
- ✓ Säkerhetskopiering – Effektiva rutiner och strategier för återställning
- ✓ Övningsuppgifter

Kapitel 5: Flexibilitet och framtida säkerhetsutmaningar

- ✓ Skydda företaget mot ransomware och andra aktuella hot
- ✓ Policys och bästa praxis för distansarbete
- ✓ Skapa en hållbar säkerhetskultur
- ✓ Uppdaterade trender och framtida utmaningar inom IT-säkerhet
- ✓ Övningsuppgifter