Curso ATCS01v2 - Cibersegurança | Sensibilização para utilizadores

Duração: 4h

Introdução

Este curso inicial permite adquirir as competências fundamentais de Cibersegurança que são cruciais para quem utiliza dispositivos informáticos e usa a Internet. Primeiro, aprenderá a reconhecer as ameaças e riscos de segurança comuns que indivíduos e organizações podem enfrentar, como roubo, manipulação e destruição de informações sensíveis. Em seguida, descobrirá as características dos ciberataques e aprenderá como pode aplicar as melhores práticas para se proteger contra eles. Depois, aprenderá as melhores práticas contra ciberataques. Estas incluem o uso de palavras-passe fortes, uma boa gestão de palavras-passe e autenticação multifatorial. Vai aprender formas de fortalecer o seu plano de segurança com técnicas como endurecimento de dispositivos, criptografia e muito mais. Em seguida, aprenderá sobre práticas seguras de navegação. Vai compreender porque é crucial praticar navegação segura para se proteger contra hackers, phishing, roubo de identidade, fugas de segurança, questões de privacidade e muito mais. Também explorará métodos para proteger e gerir informações confidenciais. Depois, descobrirá como configurar os navegadores para ajudar a reduzir as falhas de segurança.

Nas entidades abrangidas pela NIS2 (Decreto-Lei n.º 125/2025, Regime Jurídico da Cibersegurança), este curso pode integrar a sensibilização periódica de todo o pessoal, que as medidas mínimas do Regulamento n.º 756/2026 pedem no controlo PR.FC-1 do Quadro Nacional de Referência para a Cibersegurança. O certificado de formação e o registo de presenças documentam a participação de cada pessoa.

Público-alvo

Este curso destina-se a todos os utilizadores de tecnologias de informação que pretendam reconhecer as ameaças mais comuns e adotar boas práticas de segurança no dia a dia, e serve também de primeiro passo a quem esteja interessado em funções de especialista ou analista de cibersegurança.

No final do curso

Após a conclusão deste curso, os formandos deverão ser capazes de:
• Explicar os princípios de confidencialidade, integridade e disponibilidade da informação.
• Reconhecer os tipos de ameaças e de ataques mais comuns, incluindo o phishing, a engenharia social e o malware.
• Identificar tentativas de phishing e de malware no email e gerir o spam.
• Criar e gerir palavras-passe fortes e usar a autenticação multifator e o início de sessão único (SSO).
• Proteger os dispositivos com controlo de acesso, firewalls, endurecimento e conceitos básicos de criptografia.
• Navegar na Internet com segurança: configurar o navegador, gerir plug-ins e extensões, e conhecer os riscos das redes públicas e o papel das redes privadas virtuais (VPN).
• Aplicar estas boas práticas no dia a dia, a partir de estudos de caso.

Pré-requisitos

Conhecimentos gerais de informática, ser um utilizador de tecnologias de informação

Exames de certificação

www.actualtraining.pt
Tel: +351 217 158 018

(não existem exames)

Conteúdo programático em detalhe

Introdução
Confidencialidade, Integridade e Disponibilidade
Segurança e Privacidade da Informação
Ameaças e Violações
Tipos de Ameaças
Phishing, Engenharia Social e Outros Ataques
Técnicas de Gestão de Palavras-Passe
Autenticação e SSO
Ameaças de Segurança
• Controlo de Acesso, Autorização e Autenticação
• Endurecimento de Dispositivos
• Validação e Uso de Dispositivos
• Conceitos de Criptografia
Gestão de E-mail e Spam
Firewalls
Identificar Tentativas de Phishing e Malware
Práticas de Navegação Segura:
• Segurança no Ecossistema de Aplicações
• Riscos da Navegação Pública
• Plug-ins, Extensões e Barras de Ferramentas
• Técnicas de Navegação Segura
Redes Privadas Virtuais
Estudo de Casos