

Curso ATCS01 - Awareness em Cyber segurança para utilizadores

4,00 Horas

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.

Público-alvo

Este curso foi projetado especificamente para iniciantes e para aqueles que estão interessados em cargos de Especialista ou Analista de Cibersegurança

Quando completar o curso

Cibersegurança é a prática de proteger sistemas, redes e programas, contra ataques digitais. Esses ataques normalmente incluem interrupções nos negócios ou o roubo, adulteração ou destruição de informações sensíveis. Os ataques de ransomware estão em ascensão e prevê-se que custem às vítimas mais de 265 mil milhões de dólares (USD) anualmente até 2031. E isso é apenas um tipo de ameaça contra a qual todos precisamos de nos proteger. A necessidade de as organizações implementarem práticas de segurança eficazes nunca foi tão importante ou urgente.

Este módulo vai ensiná-lo das competências necessárias para identificar ameaças de segurança básicas e escolher as melhores práticas para enfrentá-las. Aprenderá a diferença entre dados, informações e insights e como as empresas utilizam os três para orientar as suas decisões de negócios. Vai aprender como manter a integridade dos dados e garantir que os dados se mantenham confidenciais. Também começará a aprender sobre os diferentes tipos de ataques e violações que ameaçam as organizações e os seus dados atuais.

Desde as pessoas, até os computadores, telefones móveis e a Internet das Coisas, tudo está conectado. Hoje, há mais dispositivos do que pessoas. Para alguns, os telefones móveis e tablets substituíram os computadores e portáteis



tradicionais. A web é onde as pessoas e as empresas fazem as coisas e está sempre ativa, 24 horas por dia. A Internet pode ser um lugar incrível para entretenimento, aprendizagem e outras experiências online. Mas a Internet não é segura. Hackers, phishing, roubo de identidade, fugas de segurança, questões de privacidade e muito mais são razões válidas para praticar constantemente uma navegação segura para se proteger. Aprenderá ainda, sobre as preocupações de segurança com aplicações e navegação pública, incluindo a gestão de plug-ins, extensões e barras de ferramentas. Vai aprender sobre as configurações de segurança dos navegadores web, cookies e caches de computador.

Pré-requisitos

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

Exames

(não existem exames)

Certificado

Este curso confere certificado de frequência a todos os participantes que frequentem no mínimo 80% das horas do curso.

Conteúdo 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 Ecosistema de Aplicações
- Riscos da Navegação Pública
- Plug-ins, Extensões e Barras de Ferramentas
- Técnicas de Navegação Segura

Redes Privadas Virtuais

Estudo de Casos