

Lernmodul 5 - Cyber-Sicherheit

Einführung

Bei der Cybersicherheit geht es um die Risiken und Gefahren des Online-Geschäfts. Es ist für jeden Kleinstunternehmer von entscheidender Bedeutung zu wissen, was zu tun ist, um Cyber-Bedrohungen zu minimieren. Dieses Modul zielt darauf ab, Ihnen das Wissen, die Fähigkeiten und die Einstellungen zu vermitteln, die notwendig sind, um sowohl Ihre persönlichen Daten als auch die Daten Ihrer Kunden zu schützen und zu sichern, Risiken zu eliminieren und vor Cyber-Angriffen geschützt zu bleiben. Es soll Ihnen helfen, die relevanten Risiken, Bedrohungen und Sicherheitsprobleme beim Zugriff auf Internet Anwendungen und -dienste zu verstehen und Schwachstellen Ihrer informationstechnologischen Systeme zu erkennen.

Ziel dieses Moduls ist es ...

1. Ihnen zu helfen, die Sicherheitsfragen zu verstehen, die sich bei der Nutzung von Computersystemen und elektronischen Diensten stellen,
2. Kleinstunternehmern für die relevanten Risiken und Bedrohungen zu sensibilisieren,
3. Ihnen helfen, Schwachstellen ihrer informationstechnologischen Systeme zu erkennen,
4. Maßnahmen auf der Grundlage bewährter Verfahren anzuwenden, um die Risiken zu beseitigen und ihre Unternehmen vor Cyberangriffen zu schützen und
5. ein Bewusstsein für verschiedene Praktiken und Werkzeuge, die Sie zur Verteidigung gegen eine Vielzahl potenzieller Bedrohungen einsetzen können, zu schaffen.

Erwartete Lernergebnisse

Wissen

Nach Abschluss dieses Moduls werden Sie ...

1. Schlüsselkonzepte im Zusammenhang mit Cybersicherheit kennen,
2. verschiedene Software-Tools wie Viren- und Spyware-Schutz, Anti-Phishing, Anti-Spam, Anti-Ransomware, Firewalls, Schutzschilde, Blocker und Webfilter kennen,

3. wissen wie starke Authentifizierung, Zugriffsmanagement, Datenverschlüsselung, Schutz vor Datenverlust, Zertifikate, sichere Authentifizierung, Cloud-Sicherheit und mobile Sicherheit implementiert werden können.

Kompetenzen und Fertigkeiten

Nach Abschluss dieses Moduls werden Sie ...

1. sich der Risiken und Bedrohungen bewusst sein,
2. die Schwachstellen Ihrer Informationstechnologie-Systeme erkennen,
3. Ihre informationstechnischen Systeme vor unberechtigtem Zugriff schützen können,
4. den Wert von Cyber-Schutztechnologien verstehen,
5. wissen, was man tun und was man nicht tun sollte, um nicht Opfer von Cyberkriminalität zu werden,
6. "Cybervertrauen" in Ihr Unternehmen bekommen und
7. eine integrierte Cybersicherheitsstrategie auf Ihr IT-Ökosystem (Netzwerk, Endpunkt, E-Mail, Cloud, Anwendungen, Identität) anwenden.

Curriculum

Modul 5 ist in 4 Einheiten unterteilt:

Einheit 1: Cybersicherheit definieren

Einheit 2: Grundsätze der Cybersicherheit

Einheit 3: Arten von Cyber-Angriffen

Einheit 4: Werkzeuge und bewährte Praktiken

Darüber hinaus gibt es ein Multiple-Choice-Quiz zur Lerneinheit.

Dauer des Moduls: ungefähr 180 Minuten