专科文凭
通信信息安全

tech 科学技术大学

tech 科学技术大学

专科文凭
通信信息安全

- 模式:**在线**
- 时间:**6个月**
- 学历:**TECH科技大学**
- 时间:**16小时/周**
- 时间表:**按你方便的**
- 考试:**在线**

网络访问: www.techtitute.com/cn/information-technology/postgraduate-diploma/postgraduate-diploma-computer-security-communications

目录

01

介绍

未经授权和不正当使用网络是用户可能面临的主要问题之一。鉴于大量的私人和机密信息通过互联网流动，开展计算机安全行动是至关重要的。这所大学的专家通过一个最新的和高质量的方案使学生更接近通信的计算机安全领域。它是一个完整的准备，旨在培训学生在其专业领域取得成功。

如果你正在寻找高质量的培训，以帮助你在拥有最多专业机会的领域之一实现专业化，这是你最好的选择"

电信领域的进步不断发生，因为这是发展最快的领域之一。因此，有必要拥有能够适应这些变化的IT专家，并对该领域出现的新工具和技术拥有第一手的知识。

在这一领域中，计算机安全必须是公司必须最关注的方面之一，因为他们的所有信息都在网络上，因此，如果用户不受控制地进入网络执行非法任务，就会给组织带来严重问题，无论是经济上还是声誉上。

大学的通信计算机安全专家涉及这一领域所涉及的全部问题。它的研究与其他专注于特定区块的课程相比具有明显的优势，这使得学生无法了解与包括在电信多学科领域的其他领域的相互关系。此外，该教育课程的教学团队对该培训的每个科目都进行了精心挑选，以便为学生提供最完整的学习机会，并始终与时事挂钩。

该课程的目标是那些有兴趣获得更高水平的通信计算机安全知识的人。主要目的是使学生能够在现实世界中，在一个再现他们未来可能遇到的条件的工作环境中，以严格和现实的方式应用在本大学专家中获得的知识。

此外，由于这是一个100%在线的大学专家，学生不受固定时间表的限制，也不需要移动到另一个物理位置，而是可以在一天中的任何时间访问内容，平衡他们的工作或个人生活与学术生活。

这个**通信信息安全专科文凭**包含了市场上最完整和最新的课程。主要特点是：

- 由计算机安全专家提出的实际案例的发展
- 该书的内容图文并茂、示意性强、实用性强，为那些视专业实践至关重要的学科提供了科学和实用的信息
- 可以进行自我评估过程的实践，以推进学习
- 其特别强调计算机通信安全方面的创新方法
- 理论课、向专家提问、关于有争议问题的讨论区和个人反思性论文
- 可以从任何有互联网连接的固定或便携式设备上获取内容

> 不要错过与我们一起参加这个通信信息安全专科文凭的机会。这是推进你的职业生涯的完美机会"

这所大学的专家是你在选择进修课程以更新你的通信计算机安全知识方面的最佳投资"

这个培训有最好的教材，这将使你做背景研究，促进你的学习。

这个100%在线的大学专家将使你的学习与你的专业工作相结合。你选择训练的地点和时间。

教学人员包括来自电信IT领域的专业人士，他们把自己的工作经验带到了这个培训中，还有来自领先公司和著名大学的公认专家。

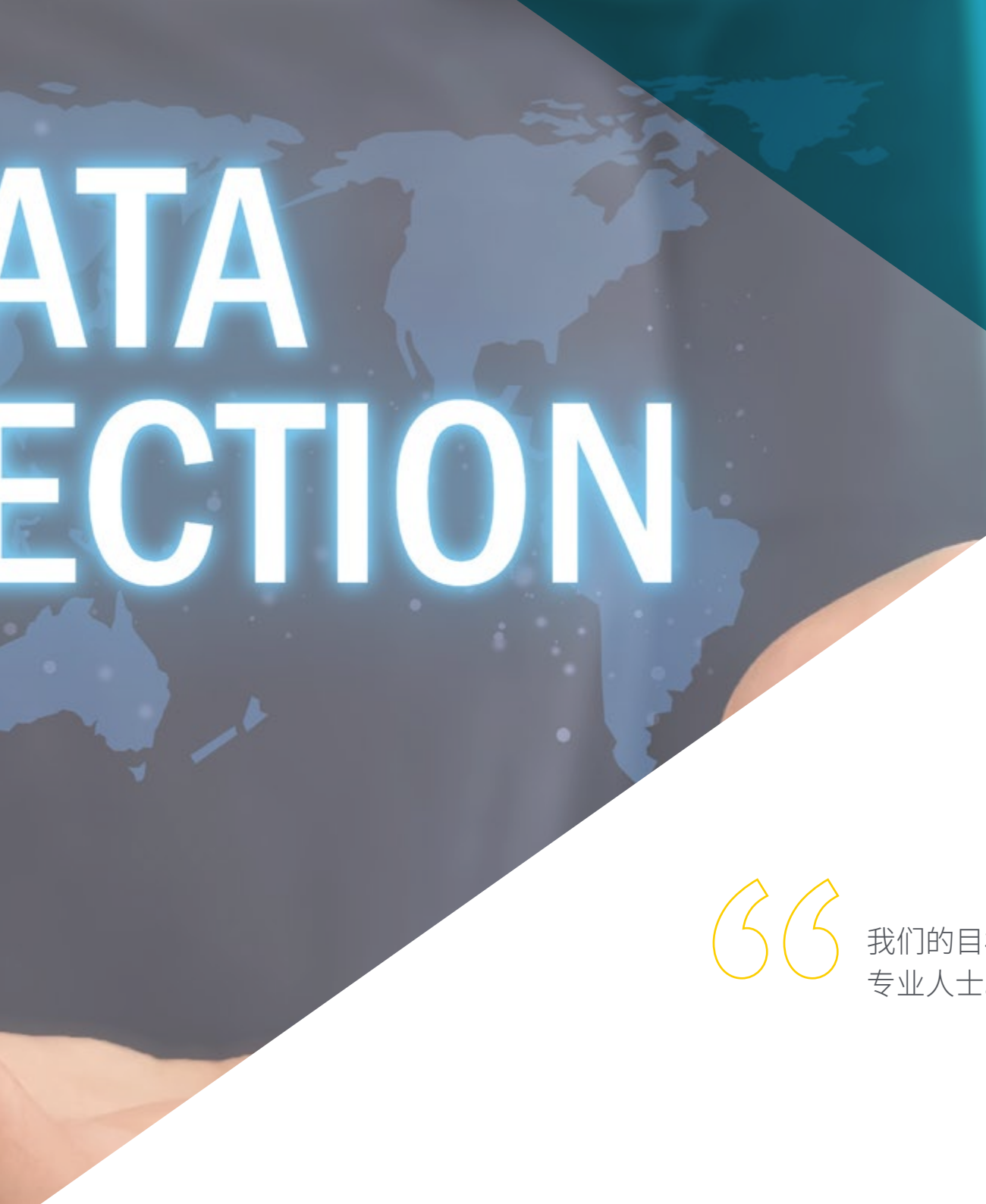
它的多媒体内容是用最新的教育技术开发的，将允许专业人员进行情景式学习，即一个模拟的环境，提供一个身临其境的培训，为真实情况进行培训。

该课程的设计重点是基于问题的学习，通过这种方式，专业人员必须尝试解决整个学年出现的不同专业实践情况。为此，该专业人员将得到由公认的、经验丰富的通信计算机安全专家开发的最先进的互动视频系统的协助。

02

目标

通信信息安全专科文凭的目的是促进该领域专业人员的表现，使他们能够获得和学习该领域的主要发展。

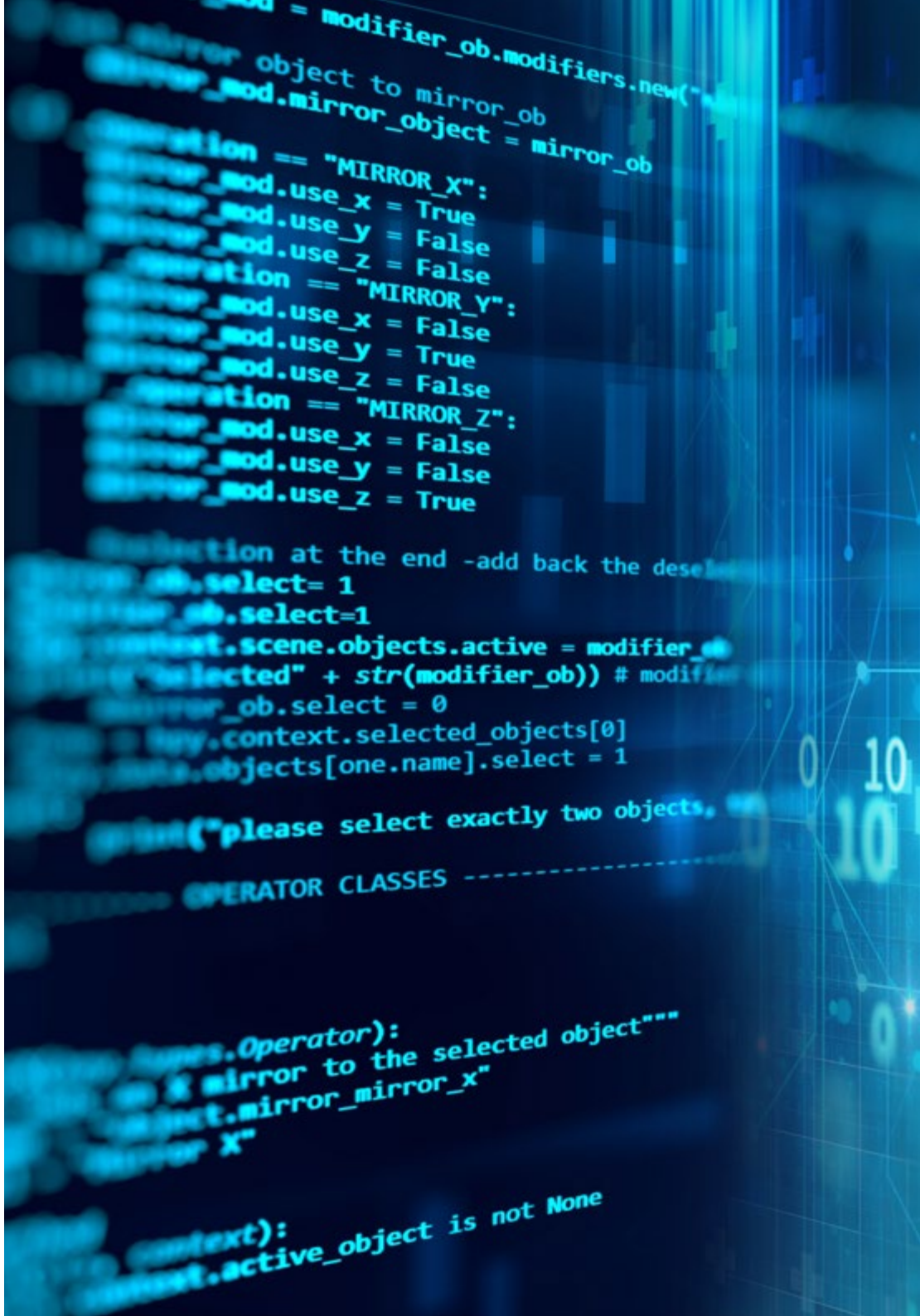


我们的目标是使你成为你所在行业的最佳专业人士。为此，我们有最好的方法和内容"

总体目标

- 培训学生，使他们能够在通信计算机安全领域以完全安全和高质量的方式开展工作

> 在世界领先的西班牙语
> 私立网上大学进行培训"



具体目标

模块1.通信系统和网络的安全

- 了解并知道如何在电信网络、系统和服务中应用编程的基本原理
- 掌握国际标准化组织的协议和网络的规则和规定
- 理解对称和非对称密码学、数字签名、哈希函数和通信架构各层次的安全化的概念
- 理解基于访问控制的各种安全机制和协议：认证和周边防御
- 了解电信网络和系统安全的技术和人为威胁的运作
- 根据其保护的资产，适当地对网络和系统的不同安全服务进行分类
- 将网络和服务管理系统应用于电信网络和服务的配置、运行、监控和定价
- 知道如何通过应用隧道、防火墙、加密和认证协议以及内容保护机制来管理电信网络和服务的安全
- 能够理解和应用主要的安全编程技术

模块2.安全架构

- 理解IT安全的基本原则
- 掌握IT安全标准和认证程序
- 分析安全技术所基于的组织和密码学基础
- 识别ICT所涉及的不同元素的主要威胁和漏洞，以及其原因
- 对网络安全工具及其具体功能有深入了解
- 知道如何从不同角度应用构成ICT安全架构的技术

模块3.信息系统审计

- 掌握系统审计的主要概念、标准和方法
- 了解审计的组织要素和法律框架
- 获得设计新的内部IT控制体系的参考指南
- 理解并识别技术发展带来的风险
- 检测不同的信息系统如何满足或不满足预期的安全要求
- 能够进行网络安全的持续改进过程

03

结构和内容

内容的结构是由到电信工程领域最优秀的专业人士设计的，他们在专业领域有丰富的经验和公认的声望最新的教育技术可以为高等教育带来的好处。

我们拥有市场上最完整和最新的科学方案。我们努力追求卓越，并希望你们也能实现这一目标"

模块1.通信系统和网络的安全

1.1. 经典安全、密码学和密码分析的全球视角
- 1.1.1. 计算机安全:历史视角
- 1.1.2. 但是安全到底是什么意思?
- 1.1.3. 加密货币的历史
- 1.1.4. 替换密码
- 1.1.5. 案例研究:密码机

1.2. 对称密码学
- 1.2.1. 简介和基本术语
- 1.2.2. 对称加密
- 1.2.3. 操作模式
- 1.2.4. DES
- 1.2.5. 新的 AES 标准
- 1.2.6. 流密码
- 1.2.7. 密码分析

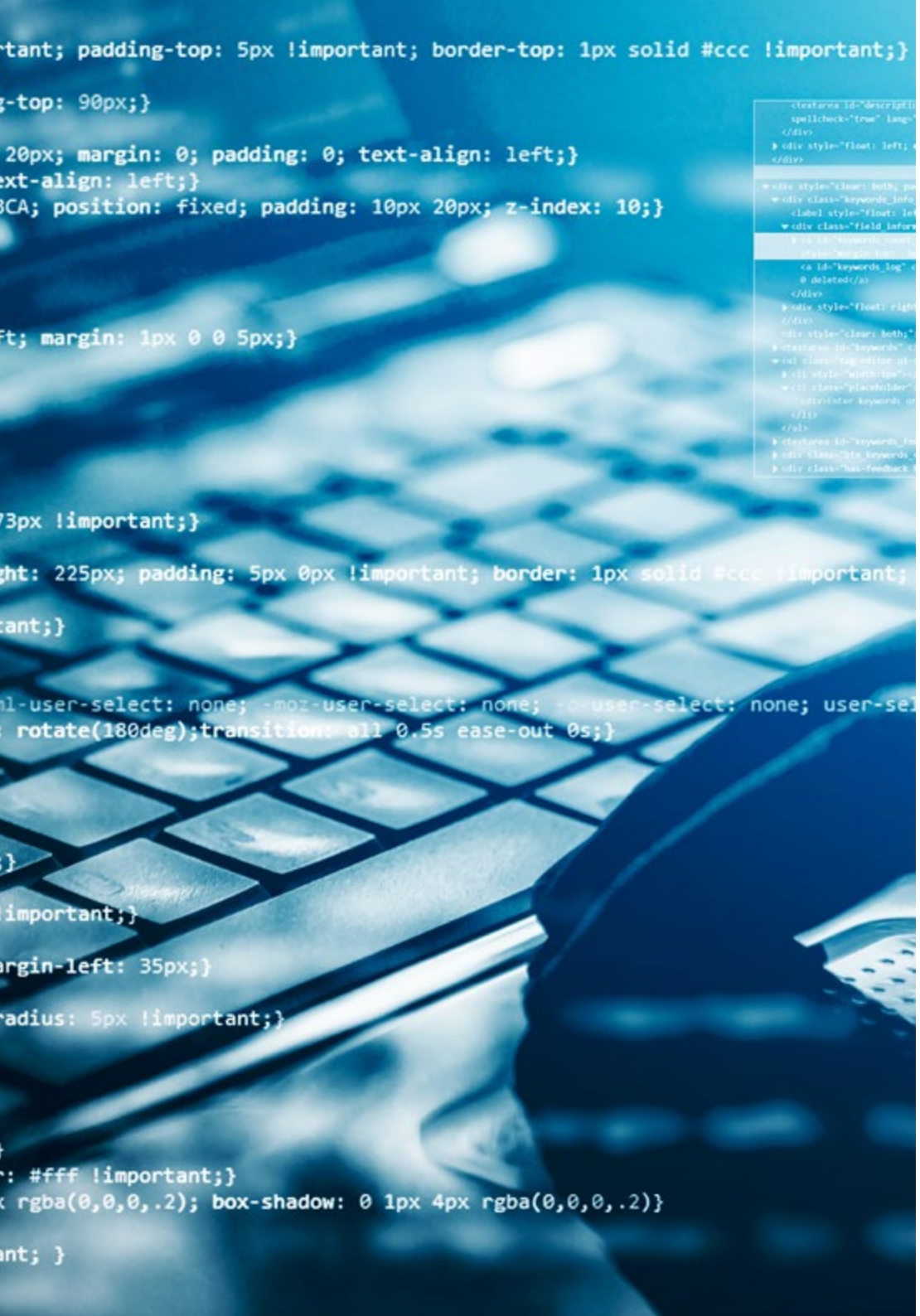
1.3. 非对称密码学
- 1.3.1. 公钥密码学的起源
- 1.3.2. 基本概念和操作
- 1.3.3. RSA 算法
- 1.3.4. 数字证书
- 1.3.5. 密钥存储和管理

1.4. 网络攻击
- 1.4.1. 网络威胁和攻击
- 1.4.2. 枚举
- 1.4.3. 流量拦截:sniffers
- 1.4.4. 拒绝服务攻击
- 1.4.5. ARP中毒攻击

1.5. 安全架构
- 1.5.1. 传统安全架构
- 1.5.2. 安全套接层:SSL
- 1.5.3. SSH 协议
- 1.5.4. 虚拟专用网络 (VPNs)
- 1.5.5. 外部存储单元的保护机制
- 1.5.6. 硬件保护机制

1.6. 系统保护技术和安全代码开发
- 1.6.1. 操作安全
- 1.6.2. 资源和控制
- 1.6.3. 监测
- 1.6.4. 入侵检测系统
- 1.6.5. 主机 IDS
- 1.6.6. 网络 IDS
- 1.6.7. 基于签名的 IDS
- 1.6.8. 诱饵系统
- 1.6.9. 代码开发的基本安全原则
- 1.6.10. 故障管理
- 1.6.11. 公敌一号:缓冲区溢出
- 1.6.12. 加密货币

1.7. 僵尸网络和垃圾邮件
- 1.7.1. 问题的根源
- 1.7.2. 垃圾邮件的过程
- 1.7.3. 传送垃圾邮件
- 1.7.4. 邮件列表的细化
- 1.7.5. 保护技术
- 1.7.6. 第三方提供的反垃圾邮件服务
- 1.7.7. 案例研究
- 1.7.8. 外来垃圾邮件



1.8. 审计和网络攻击
- 1.8.1. 信息收集
- 1.8.2. 攻击技术
- 1.8.3. 工具

1.9. 恶意软件和恶意代码
- 1.9.1. 什么是恶意软件?
- 1.9.2. 恶意软件的类型
- 1.9.3. 病毒
- 1.9.4. 隐病毒
- 1.9.5. 蠕虫
- 1.9.6. 广告软件
- 1.9.7. 间谍软件
- 1.9.8. 恶作剧
- 1.9.9. 网络钓鱼
- 1.9.10. 木马
- 1.9.11. 恶意软件的经济学
- 1.9.12. 可能的解决方案

1.10. 取证分析
- 1.10.1. 证据收集
- 1.10.2. 证据分析
- 1.10.3. 反法医技术
- 1.10.4. 实际案例研究

模块2.安全架构

2.1. 计算机安全的基本原则
- 2.1.1. 什么是计算机安全的含义
- 2.1.2. 计算机安全的目标
- 2.1.3. 计算机安全服务
- 2.1.4. 缺乏安全的后果
- 2.1.5. 安全防御 "原则
- 2.1.6. 安全政策、计划和程序
  - 2.1.6.1. 用户账户管理
  - 2.1.6.2. 用户识别和认证
  - 2.1.6.3. 授权和逻辑访问控制
  - 2.1.6.4. 服务器监控
  - 2.1.6.5. 数据保护
  - 2.1.6.6. 远程连接的安全性
- 2.1.7. 人为因素的重要性

2.2. IT安全的标准化和认证
- 2.2.1. 安全标准
  - 2.2.1.1. 标准的目的
  - 2.2.1.2. 负责机构
- 2.2.2. 美国的标准
  - 2.2.2.1. TCSEC
  - 2.2.2.2. 联邦标准
  - 2.2.2.3. FISCAM
  - 2.2.2.4. NIST SP 800
- 2.2.3. 欧洲标准
  - 2.2.3.1. ITSEC
  - 2.2.3.2. ITSEM
  - 2.2.3.3. 欧洲网络和信息安全局（ENISA）
- 2.2.4. 国际标准
- 2.2.5. 认证过程

2.3. 对IT安全的威胁：漏洞和恶意软件
- 2.3.1. 简介
- 2.3.2. 系统的易损性
  - 2.3.2.1. 网络安全事件
  - 2.3.2.2. 计算机系统漏洞的原因
  - 2.3.2.3. 漏洞的类型
  - 2.3.2.4. 软件制造商的责任
  - 2.3.2.5. 漏洞评估工具
- 2.3.3. 计算机 安全威胁
  - 2.3.3.1. 网络入侵者的分类
  - 2.3.3.2. 攻击者的动机
  - 2.3.3.3. 攻击的阶段
  - 2.3.3.4. 攻击的类型
- 2.3.4. 计算机病毒
  - 2.3.4.1. 一般特征
  - 2.3.4.2. 病毒的类型
  - 2.3.4.3. 病毒的损害
  - 2.3.4.4. 如何防治病毒

2.4. 网络恐怖主义和事件应对
- 2.4.1. 简介
- 2.4.2. 网络恐怖主义和网络战争的威胁
- 2.4.3. 企业失败和被攻击的后果
- 2.4.4. 计算机网络中的间谍活动

2.5. 用户识别和生物识别系统
- 2.5.1. 用户认证、授权和注册介绍
- 2.5.2. AAA安全模型
- 2.5.3. 访问控制
- 2.5.4. 用户识别
- 2.5.5. 密码验证
- 2.5.6. 用数字证书进行认证
- 2.5.7. 远程用户识别

2.5.8. 单点登录
2.5.9. 密码管理器
2.5.10. 生物识别系统
2.5.10.1. 一般特征
2.5.10.2. 生物识别系统
2.5.10.3. 系统的实施
2.6. 密码学和密码协议的基础知识
2.6.1. 密码学简介
2.6.1.1. 密码学、密码分析和密码学
2.6.1.2. 加密系统的运作
2.6.1.3. 加密系统的历史
2.6.2. 密码分析
2.6.3. 加密系统的分类
2.6.4. 对称和非对称密码系统
2.6.5. 用密码系统进行认证
2.6.6. 电子签名
2.6.6.1. 什么是电子签名?
2.6.6.2. 电子签名的特点
2.6.6.3. 认证机构
2.6.6.4. 数字证书
2.6.6.5. 基于可信的第三方系统
2.6.6.6. 使用电子签名
2.6.6.7. 电子身份证
2.6.6.8. 电子发票
2.7. 网络安全工具
2.7.1. 互联网连接中的安全问题
2.7.2. 外部网络安全
2.7.3. 代理服务器的作用
2.7.4. 防火墙的作用
2.7.5. 远程连接的认证服务器
2.7.6. 活动日志的分析
2.7.7. 入侵检测系统
2.7.8. 诱饵
2.8. 虚拟专用网络和无线网络的安全
2.8.1. 虚拟专用网络的安全
2.8.1.1 VPN的作用
2.8.1.2 VPN的协议
2.8.2. 无线网络中的传统安全
2.8.3. 对无线网络可能的攻击
2.8.4. WEP 协议
2.8.5. 无线网络安全的标准
2.8.6. 加强安全的建议
2.9. 使用互联网服务的安全问题
2.9.1. 安全浏览网页
2.9.1.1. www服务
2.9.1.2. www上的安全问题
2.9.1.3. 安全建议
2.9.1.4. 保护互联网上的隐私
2.9.2. 电子邮件安全
2.9.2.1. 电子邮件的特点
2.9.2.2. 电子邮件的安全问题
2.9.2.3. 电子邮件安全建议
2.9.2.4. 高级电子邮件服务
2.9.2.5. 雇员对电子邮件的使用
2.9.3. 垃圾邮件
2.9.4. 网络钓鱼
2.10. 内容控制
2.10.1. 互联网上的内容传播
2.10.2. 打击非法内容的法律措施
2.10.3. 对内容进行过滤、编目和封锁
2.10.4. 对形象和声誉的损害

模块3.信息系统审计

3.1. 信息系统审计良好做法的标准
- 3.1.1. 简介
- 3.1.2. 审计和COBIT
- 3.1.3. 对ICT管理系统的审计
- 3.1.4. 认证

3.2. 系统审计的概念和方法
- 3.2.1. 简介
- 3.2.2. 系统评估的方法:定量和定性
- 3.2.3. IT审计方法
- 3.2.4. 审计计划

3.3. 审计合同
- 3.3.1. 审计工作的法律性质
- 3.3.2. 审计业务的各方
- 3.3.3. 审计业务的主题
- 3.3.4. 审计报告

3.4. 审计的组织要素
- 3.4.1. 简介
- 3.4.2. 审计部门的任务
- 3.4.3. 审计规划
- 3.4.4. IS审计方法

3.5. 审计的法律框架
- 3.5.1. 个人数据的保护
- 3.5.2. 软件的法律保护
- 3.5.3. 技术犯罪
- 3.5.4. 签约、签名和电子身份证

3.6. 外包审计和参考框架
- 3.6.1. 简介
- 3.6.2. 外包基础知识
- 3.6.3. 审计IT外包的情况
- 3.6.4. 参考框架CMMI, ISO27001, ITIL

3.7. 安全审计
- 3.7.1. 简介
- 3.7.2. 物理和逻辑安全
- 3.7.3. 环境的安全
- 3.7.4. 物理安全审计的计划和执行

3.8. 网络和互联网审计
- 3.8.1. 简介
- 3.8.2. 网络漏洞
- 3.8.3. 互联网上的原则和权利
- 3.8.4. 数据控制和处理

3.9. 计算机应用和系统的审计
- 3.9.1. 简介
- 3.9.2. 参考模型
- 3.9.3. 对申请质量的评估
- 3.9.4. 对开发和维护领域的组织和管理的审计

3.10. 对个人数据的审计
- 3.10.1. 简介
- 3.10.2. 数据保护法律和法规
- 3.10.3. 审计的发展
- 3.10.4. 侵权和制裁

> 这种培训将使你能够以一种舒适的方式推进你的职业生涯"

04

方法

这个培训计划提供了一种不同的学习方式。我们的方法是通过循环的学习模式发展起来的:**再学习**。

这个教学系统被世界上一些最著名的医学院所采用,并被**新英格兰医学杂志**等权威出版物认为是最有效的教学系统之一。

发现再学习，这个系统放弃了传统的线性学习，带你体验循环教学系统：这种学习方式已经证明了其巨大的有效性，尤其是在需要记忆的科目中”

案例研究，了解所有内容的背景

我们的方案提供了一种革命性的技能和知识发展方法。我们的目标是在一个不断变化,竞争激烈和高要求的环境中加强能力建设。

> 和TECH,你可以体验到一种正在动摇世界各地传统大学基础的学习方式”

你将进入一个以重复为基础的学习系统，在整个教学大纲中采用自然和渐进式教学。

学生将通过合作活动和真实案例，学习如何解决真实商业环境中的复杂情况。

一种创新并不同的学习方法

该技术课程是一个密集的教学计划，从零开始，提出了该领域在国内和国际上最苛刻的挑战和决定。由于这种方法，个人和职业成长得到了促进，向成功迈出了决定性的一步。案例法是构成这一内容的技术基础，确保遵循当前经济，社会和职业现实。

> 我们的课程使你准备好在不确定的环境中面对新的挑战，并取得事业上的成功”

在世界顶级计算机科学学校存在的时间里，案例法一直是最广泛使用的学习系统。1912年开发的案例法是为了让法律学生不仅在理论内容的基础上学习法律，案例法向他们展示真实的复杂情况，让他们就如何解决这些问题作出明智的决定和价值判断。1924年，它被确立为哈佛大学的一种标准教学方法。

在特定情况下，专业人士应该怎么做？这就是我们在案例法中面对的问题，这是一种以行动为导向的学习方法。在整个课程中，学生将面对多个真实的案例。他们必须整合所有的知识，研究，论证和捍卫他们的想法和决定。

再学习方法

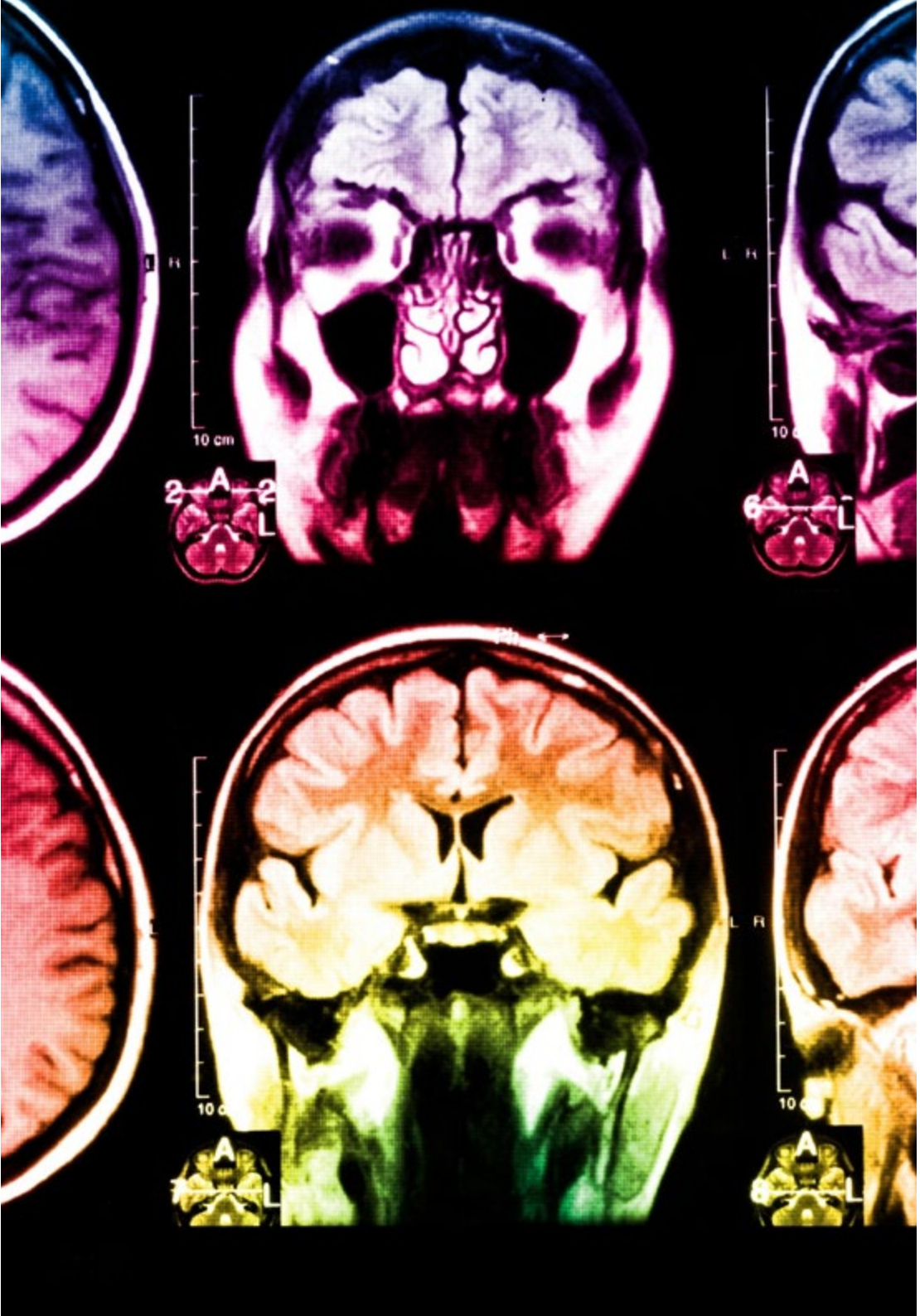
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

我们用最好的100%在线教学方法加强案例研究：再学习。

> 在2019年，我们取得了世界上所有西班牙语在线大学中最好的学习成绩。

在TECH，你将用一种旨在培训未来管理人员的尖端方法进行学习。这种处于世界教育学前沿的方法被称为再学习。

我校是唯一获准使用这一成功方法的西班牙语大学。2019年，我们成功地提高了学生的整体满意度（教学质量,材料质量,课程结构,目标……），与西班牙语最佳在线大学的指标相匹配。



在我们的方案中，学习不是一个线性的过程，而是以螺旋式的方式发生（学习，解除学习，忘记和重新学习）。因此，我们将这些元素中的每一个都结合起来。这种方法已经培养了超过65万名大学毕业生，在生物化学，遗传学，外科，国际法，管理技能，体育科学，哲学，法律，工程，新闻，历史，金融市场和工具等不同领域取得了前所未有的成功。所有这些都是在一个高要求的环境中进行的，大学学生的社会经济状况很好，平均年龄为43.5岁。

再学习将使你的学习事半功倍，表现更出色，使你更多地参与到训练中，培养批判精神，捍卫论点和对比意见：直接等同于成功。

从神经科学领域的最新科学证据来看，我们不仅知道如何组织信息，想法，图像y记忆，而且知道我们学到东西的地方和背景，这是我们记住它并将其储存在海马体的根本原因，并能将其保留在长期记忆中。

通过这种方式，在所谓的神经认知背景依赖的电子学习中，我们课程的不同元素与学员发展其专业实践的背景相联系。

该方案提供了最好的教育材料，为专业人士做了充分准备：

学习材料

所有的教学内容都是由教授该课程的专家专门为该课程创作的，因此，教学的发展是具体的。

然后，这些内容被应用于视听格式，创造了TECH在线工作方法。所有这些，都是用最新的技术，提供最高质量的材料，供学生使用。

大师课程

有科学证据表明第三方专家观察的有用性。

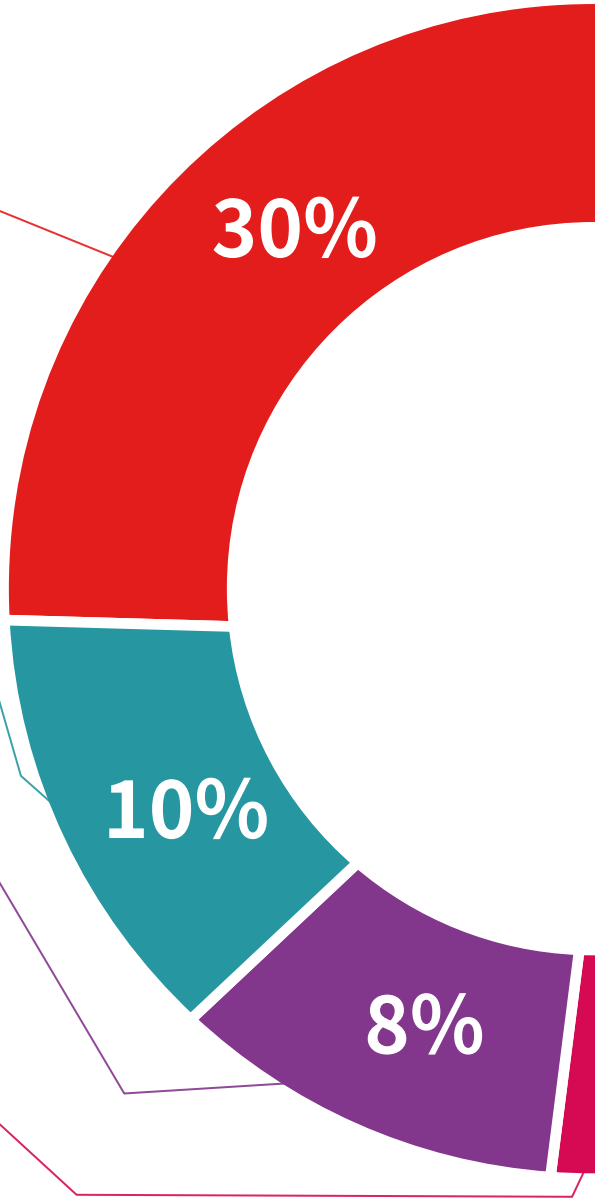
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

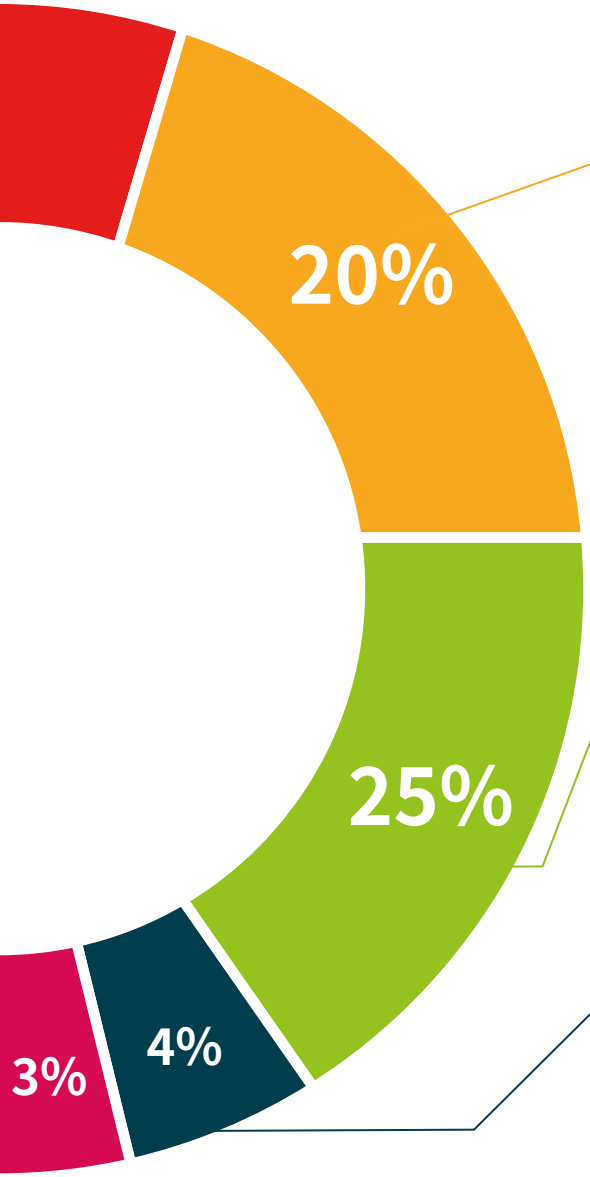
技能和能力的实践

你将开展活动以发展每个学科领域的具体能力和技能。在我们所处的全球化框架内，我们提供实践和氛围帮你取得成为专家所需的技能和能力。

延伸阅读

最近的文章，共识文件和国际准则等。在TECH的虚拟图书馆里，学生可以获得他们完成培训所需的一切。





案例研究

他们将完成专门为这个学位选择的最佳案例研究。由国际上最好的专家介绍,分析和辅导案例。

互动式总结

TECH团队以有吸引力和动态的方式将内容呈现在多媒体丸中，其中包括音频,视频,图像,图表和概念图，以强化知识。

这个用于展示多媒体内容的独特教育系统被微软授予“欧洲成功案例”称号。

测试和循环测试

在整个课程中，通过评估和自我评估活动和练习，定期评估和重新评估学习者的知识：通过这种方式，学习者可以看到他/她是如何实现其目标的。

05

学位

通信信息安全专科文凭课程除了保证最严格和最新的培训外，还可以获得由TECH科技大学颁发的专科文凭学位证书。

成功完成该课程并获得大学学位，无需旅行或通过繁琐的程序"

这个**通信信息安全专科文凭**包含了市场上最完整和最新的课程。

评估通过后，学生将通过邮寄收到**TECH科技大学**颁发的相应的**专科文凭**学位。

TECH科技大学颁发的证书将表达在专科文凭获得的资格，并将满足工作交流，竞争性考试和专业职业评估委员会的普遍要求。

学位：**通信信息安全专科文凭**

官方学时：**450小时**


tech 科学技术大学

授予

文凭

_____先生/女士，身份证号码_____
顺利通过并获得认证的课程是

专科文凭

通信信息安全

这是一个由本大学授予的学位，相当于450个小时，
开始日期是 dd/mm/aaaa,结束日期是dd/mm/aaaa。

截至2018年6月28日，TECH是一所被公共教育部认可的私立高等教育机构。

2020年六月17日

Tere Guevara Navarro女士
校长

Unique TECH Code: AFWORD23S techtitute.com/certificates

*海牙认证。如果学生要求他或她的纸质学位进行海牙认证，TECH EDUCATION将作出必要的安排，并收取额外的费用。

tech 科学技术大学

专科文凭
通信信息安全

- 模式:在线
- 时间:6个月
- 学历:TECH科技大学
- 时间:16小时/周
- 时间表:按你方便的
- 考试:在线

专科文凭
通信信息安全

tech 科学技术大学