



## DATOS CLAVE

**Nombre del curso:**

Certified Security Sentinel

**Duración:**

2 días

**Idioma:**

Español

**Formato:**

\* Aula con instructor

**Pre-requisitos:**

\* Usar computadora

**Materiales:**

\* Cuaderno de Trabajo

## BENEFICIOS DEL CURSO

El curso Certified Security Sentinel está dirigido a cualquier persona que utiliza una computadora en Internet. Los asistentes podrán entender completamente las amenazas de seguridad que atacan todos los días y también entenderán las medidas asociadas a estos ataques. Los estudiantes aprenden que el eslabón más débil de cualquier programa de seguridad es un empleado mal entrenado. Una vez que el estudiante entienda lo que puede pasar, ellos sabrán lo que debe buscar y con estas tácticas de sentido común, ser capaz de mantener su equipo lo más seguro posible.

La parte de ingeniería social de la clase no se dirige específicamente a las TI o personal de seguridad por sí solos, está diseñado para enseñar a los participantes las habilidades utilizadas por los ingenieros sociales para facilitar la extracción de información de una organización que utiliza métodos técnicos y no técnicos.

Fraude informático, black-hat hacking, los ciber-terroristas; estas frases describen una innovadora generación de criminales que usan la tecnología over-the-wire para atacarnos, nos roban y nos aterrorizan. Sin embargo, la mejor herramienta en su arsenal no es nueva. Sólo se utiliza por los más experimentados, los más peligrosos, los hackers más audaces.

¿Funciona? ¿Pueden las personas aparentemente inteligentes fácilmente ser engañadas? Kevin Mitnick, quien pasó cinco años en prisión por hackeo, dijo en un testimonio ante el Congreso sobre el tema de la Ingeniería Social "tuve tanto éxito con ese ataque que rara vez tuve que recurrir a un ataque técnico."

El programa Certified Security Sentinel es innovador y capacita a los estudiantes sobre cómo se llevan a cabo los ataques, las habilidades necesarias para llevar a cabo un ataque, la forma de capacitar a las personas para identificar un ataque, pero lo más importante: Cómo entrenar a objetivos internos para que la formación sea eficaz y dura.

## MÓDULOS DEL CURSO

**Módulo 1 - Basic Security: How to secure a computer for personal internet use**

What are the Risks?  
Known Risks  
Did You Know?  
What are the Risks?  
Things you NEED to know!  
The "Hacker"  
What is Identity Theft?  
Fighting Identity Theft  
Practice  
Demo  
Don't Panic!

**Módulo 2 - User Awareness**

Overview User  
Attacks User  
Awareness  
Passwords  
Generating Passwords  
Keeping Track Of Passwords  
eWallet  
Encryption Tools  
Other Password Options  
Windows Administrator Account  
Demo  
Windows Processes  
Task Manager

## MÓDULOS DEL CURSO

Processes Tab  
 Searching Processes  
 Web Research  
 Process Information  
 Bad Processes  
 Removing Suspect Processes  
 Start-Up Tuners  
 Downloads  
 The User  
 E-Mail Links  
 Demo

### Módulo 3 - Implementing Countermeasures

Overview  
 Internet Protection Solutions  
 Choosing a Package  
 Free Anti-Virus & Spyware  
 Free Anti-Malware & Anti Spyware  
 Updating  
 Scheduling a Scan?  
 Demo  
 Patch Management  
 Demo  
 Internet Anonymizers  
 How They Work  
 Demo

### Módulo 4 - Essential Security Awareness for Everyone

Why Are You Here?  
 The Employer's Liability  
 Steps to an Effective Security Program  
 Starting at the Top Why  
 This All Matters Areas  
 of Concern What's In  
 This For Me? Course  
 Format

### Módulo 5 - Using the Internet at Work

Module Objectives  
 Why Can't I Just Do What I Want?  
 Internet Acceptable Use Policy  
 The Internet at Work  
 Internet Basics, Threats, Access  
 Your Web Browser  
 ActiveX & Java  
 Media Files  
 E-Mail  
 Chat  
 Web Storage

Web Proxies  
 P2P Spyware  
 Countermeasures  
 Demo

### Módulo 6 - Accessing the Company's Network Through Your Assigned Computer

Module Objectives  
 What's a LAN?  
 Logging In  
 Installing Applications  
 OS Utilities  
 Network Drives  
 Sharing  
 Removable Storage  
 Email Attachments  
 Virus Scanner  
 Management Software  
 Monitoring  
 Demos

### Módulo 7 - Accessing the Corporate Network Remotely

Module Objectives  
 Work from Home  
 Your Home PC  
 From Your House to Work  
 Wireless  
 Hot Spots  
 Web Access for Email  
 Profile Management  
 VPNs  
 Demo

### Módulo 8 - Social Engineering

Introduction  
 What is Social Engineering?  
 Definition of Social Engineering  
 Goals of Social Engineering  
 Types of Social Engineering  
 Attacks by Phone  
 Dumpster Diving  
 On-Line Social Engineering  
 Persuasion  
 Social Engineering Roles  
 Reverse Social Engineering  
 What We Cover  
 Examples of our labs

### Módulo 9 - Understanding and Manipulating our Target

Outline  
 Introduction  
 How are People Motivated?  
 Avoiding Pain  
 Pursuing Pleasure  
 Baselining  
 How to Read a Person  
 Body Movements  
 What About Over the Phone?  
 Re-Framing  
 Putting on the Right "Spin"  
 Marketing  
 Alter Perceptions of Pain or  
 Pleasure  
 Saving-Face  
 Verbal Judo  
 Putting It All Together  
 Practice  
 Summary

### Módulo 10 - Researching Our Target

Outline  
 Introduction  
 Google Hacks  
 Other Research Techniques  
 Dumpster Diving  
 Email Addresses  
 Current SOPs  
 Vendor Agreements  
 Inter-Office Memos  
 Shoulder Surfing  
 Eavesdropping  
 E-mail Telephone  
 Calls Cubicles/Office  
 Areas Restaurants  
 and Bars Job  
 Descriptions  
 Conclusion

### Módulo 11 - Methods of Deception

Outline  
 Introduction  
 Impersonation in Person  
 The Job Interview  
 The Inspector  
 Delivery Person  
 Vendors/Contractors  
 Impersonation on the Phone  
 Help Desk  
 IT Staff  
 Asking for Help  
 Summary