CURSO DE SEGURIDAD INFORMÁTICA PARA USUSARIOS

HORAS: 12 Horas, modalidad presencial

OBJETIVOS

- Utilizar la seguridad informática como herramienta para mitigar riesgos de fuga de información sensible, robo de identidad o actividades ilícitas.

- Conocer la legislación vigente y la responsabilidad que conlleva para el usuario y la empresa el robo de información sensible.

- Conocer los riesgos que implica el uso de ordenadores personales (tanto portátiles como sobremesa) y servidores cara a Internet.

- Familiarizarse con los posibles tipos de ataques, técnicas maliciosas que los intrusos informáticos pueden utilizar para introducirse en ordenadores.

- Aprender desde un HackLab las técnicas utilizadas por los Crakers cuando planean e intentan un ataque a páginas Web, servidores de correo, bases de datos y sistemas de redes de ordenadores, así como las contramedidas necesarias para abortar dichos ataques.

- Adquirir los conocimientos para la toma de decisiones cuando se trata de salvaguardar la información sensible y datos confidenciales de personas, la institución o empresa a la que pertenecen. Aprenderán sobre seguridad y penetración a redes inalámbricas Wifi.

- Realizar de forma correcta copias de seguridad, así como conocer y saber usar las distintas herramientas de seguridad de que disponen los usuarios, tales como antivirus, vacunas, antimalware, pruebas de seguridad, etc
- Saber configurar la privacidad y seguridad en las principales redes sociales.

CONTENIDO DEL CURSO

MODULO 1: PRL (Prevención de riesgos tecnológicos):

- Introducción al hacking ético.
- Fases de un ataque
- Hacker VS Cracker
- Estafas y ataques: Ingeniería social, Phishing, robo de contraseñas (por fuerza bruta y diccionario), keylogger, enlaces maliciosos, metadatos, redes envenenadas, xploit, etc.
- Malware: Virus, troyanos, spam, gusanos, etc.
- Contramedidas.

- Contraseñas seguras.
- Principales consejos de seguridad.
- Responsabilidad legal de los usuarios y empresas en el robo de información.
- Uso de herramientas de seguridad para usuarios y prueba Eicar.
- Políticas de seguridad lógica.
- Botnet y ordenadores zombis.
- Demostraciones prácticas de distintos ataques en laboratorio Hacker.

MODULO 2: Seguridad y privacidad en redes sociales:

- Introducción a la Ciberseguridad.
- Revisión de las cláusulas de privacidad y seguridad de los contratos aceptados por los usuarios con las redes sociales.
- Configuración de las opciones de seguridad y privacidad en redes sociales.
- Responsabilidades legales de los usuarios de RRSS.
- Me protejo en Facebook.
- Me protejo en Twitter.
- Me protejo en Línkedin.
- Plan de crisis.
- Tipos de atraque específicos de las redes sociales.
- Contramedias.
- Demostraciones prácticas de distintos ataques en laboratorio Hacker.

MODULO 3: Seguridad web, en dispositivos móviles y en la navegación por Internet:

- Introducción a la seguridad web y en dispositivos móviles.
- Noticias.
- Hacia dónde vamos.
- Principales riesgos de las nuevas tecnologías.
- Capturas y control remoto de webcam.
- Robo de cookies y de las contraseñas del navegador.
- Google hacking.
- Ataques web por inyección de código SQL.
- Shodan: el buscador de los crackers.
- Seguridad móvil.
- Enlaces y códigos QR maliciosos.
- Uso de herramientas profesionales de auditoría y seguridad web.
- Captura de tráfico.
- Robo de identidades.
- Wifis y redes envenenadas.
- Consejos para una navegación segura.
- Uso de Proxy y Red tor.
- Protocolo Https.
- Contramedias. o Demostraciones prácticas de distintos ataques en laboratorio Hacker

DOCENTES:

1 Docente especialista, 1 Hacker ético (técnico en seguridad)

PRECIO DEL CURSO:

Trabajadores por cuenta ajena que bonifiquen: 144,00 €

Autónomos:

Desempleados: