ESCOLTA DIGITAL

DOSSIER

HACK & SECURE

APARTADO DE CONFIDENCIALIDAD

Los materiales contenidos en este documento representan información propietaria a **HACK&SECURE** y han sido preparados para uso exclusivo del destinatario. El material no debe ser duplicado, usado, por ningún propósito más que de presentar esta propuesta de servicios de **HACK&SECURE.**

La presente documentación tiene de carácter confidencial y no podrá ser objeto de reproducción parcial o total, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. Así mismo tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de sesión de uso sin el permiso previo y escrito de **HACK&SECURE**, cualquier falta de cumplimiento de derechos de uso pueden repercutir en aseveraciones legales y vulneración de la información de carácter confidencial de **HACK&SECURE**.

PRESENTACIÓN

ESCOLTA DIGITAL es un entrenamiento virtual, diseñado por agentes retirados de inteligencia en compañía de hacker éticos y Geeks, conozca en un lenguaje sencillo las tendencias, los ataques más usados por los cracs y sobre todo aprenda como protegerse a usted, a su familia y a su organización.

El entrenamiento de ESCOLTA DIGITAL va dirigido a personal militar activo, retirados, escoltas, guardas de seguridad o a todas aquellas personas que siente que el mundo de la tecnología avanza y se está quedando un paso atrás.

Después de finalizar el entrenamiento estará preparado para afrontar las nuevas amenazas cibernéticas, contara con certificado internacional avalado por el Security College de Estados Unidos y tendrá más oportunidades en su ámbito laboral.

MÉTODO DE ENSEÑANZA

El curso se realiza 100% Virtual, por lo que nuestra plataforma de estudio estará disponible 24 horas los 7 días de la semana.

En el campus virtual el estudiante tendrá a disposición un Foro donde podrá dar sus comentarios adicionales y realizar toda clase de preguntas pertinentes donde los tutores estarán atentos para dar solución lo más pronto posible.

CONTENIDO Y DURACIÓN DEL CURSO

El entrenamiento personal de Escolta digital está desarrollado para una duración de 100 horas aprox. distribuidas en 17 módulos de formación donde el último módulo es una guía práctica para dar inicio a una auditoria ya sea personal o empresarial.

MATERIAL DE ESTUDIO

El temario está constituido por 17 módulos que están distribuidos de tal manera de que el estudiante mientras vaya progresando pueda interpretar los conceptos y el vocabulario utilizado en el mundo de la era digital; Además de la información por módulo se tendrán videos de apoyo que explicaran visualmente los temas tratados.

DIRIGIDO A:

Personal militar activo o retirado, Ex agentes de inteligencia, guardas de seguridad, escoltas o a todas aquellas persona que sienta que se está quedando atrás en una era digital con constante innovación tecnológica.

CONOCIMIENTOS PREVIOS DE LOS ALUMNOS

Con el objetivo de que el programa resulte lo más provechoso posible, es recomendable que los alumnos posean los siguientes conocimientos:

- Mínimos recomendados:
  - Que tengan la facilidad de un computador con acceso Internet
- Óptimos:
  - Invertir diariamente entre 1 y 2 horas de estudio.
  - Llevar a la práctica lo aprendido en cada módulo de forma tal que se vuelva uso y costumbre garantizando la seguridad de la información desde la vida personal.
  - Utilizar el Módulo 0: Ciber alfabeto, que permita comprender la terminología básica a emplear en el curso.

TEMARIO

1. Introducción: Conceptos, términos y definiciones
2. Espionaje, Ciberespionaje, Ciberterrorismo y Hacktivismo
3. Riesgos Digitales
4. Identificación de Técnicas de Ingeniería Social
5. De la real a lo digital
6. Gadgets
7. Drones
8. Anonimato en la Red
9. Aseguramiento de cuentas digitales
10. Aseguramiento de Dispositivos tecnológicos (IOT)
11. Almacenamiento Seguro de Información – Encriptación
12. Borrado seguro de Información
13. Recuperación de Información Borrada
14. Búsqueda efectiva de información en la web a través de fuentes OSINT y control reputacional.
15. Esteganografía (Ocultar documentos e Imágenes)
16. Identificación de Fallos y vulnerabilidades en la seguridad electrónica
17. Identificación y evaluación de riesgos e implementación de medidas de seguridad de la información

DESCRIPCIÓN DE CADA MÓDULO

Módulo 1. Introducción: Conceptos, términos y definiciones

Este es un módulo de introducción con algunos conceptos básicos necesarios para comenzar con el entrenamiento.

Módulo 2. Espionaje, Ciberespionaje, Ciberterrorismo y Hacktivismo

Conozca que es y la evolución del Espionaje, cuales son los países y grupos más conocidos en este tema. Diferencie que es Ciberespionaje, Ciberterrorismo y Hacktivismo. Observe ejemplos reales a nivel mundial de cómo nos vigilan, como es comercializada la información que suministramos en las diferentes fuentes y los ataques más recientes que nos afecta directa o indirectamente. Todo lo descrito en este módulo ayudara al Estudiante de Escolta Digital a entender y a diferenciar que existen personas o grupos interesados a realizar actos delincuenciales lucrativos o no buscando un objetivo particular o colectivo.

Módulo 3. Riesgos Digitales

Durante todo el módulo conocerá acerca de los Riesgos Digitales más utilizados en los diferentes panoramas que puedan generar posibilidad de daño a una persona u organización, como el estudio de los movimientos, comportamientos detectando patrones que se pueden utilizar en contra del estudiante para engañarlos, robarles información, suplantarlos y hasta estafarlos. En este módulo el estudiante identificara cada uno de los diferentes ataques el cual le ayudara a descubrir las perspectivas a los que se ve expuesto y así ser más cuidadoso de no convertirse en víctima.

Módulo 4. Identificación de técnicas de Ingeniería social

Complementando el módulo anterior conozca que es y los diferentes ataques de Ingeniería social que pueden ser Físicos (locales) como Pretexting, Buceo en contenedores, Baiting entre otros y remotos como Phising, suplantación de identidad a través de casos reales. Aprenda a protegerse a nivel personal y organizacional.

Módulo 5. De la vida Real a lo Digital

El estudiante de Escolta digital sabrá que su información digital es de cuidado y que esta debe protegerla, conozca la teoría de los 6 grados de separación, las ventajas y el uso correcto de cada uno de las redes sociales a los que el estudiante se ve expuesto en su día a día. Se expondrán casos reales donde identificara las modalidades de Ciberestafa por medios de las redes sociales y así le dará las herramientas para no convertirse en víctima de este tipo de ataques.

Módulo 6. Gadgets o herramientas de espionaje

Conozca las herramientas usadas en el mundo del Hacking, aunque son herramientas avanzadas el estudiante identificara lo usado en el mundo digital para hacer ataques como man-in-the-middle, robo de información entre otros. Además de que al conocer estas herramientas el participante será más cuidados en las practicas del día a día como usar USB desconocidas y conectarse a redes inalámbricas “Wifi gratis” en los lugares públicos.

Módulo 7 Drones

El Escolta Digital comprenderá la magnitud del uso y funcionamiento de estos innovadores vehículos capaces de realizar distintas tareas y que en la actualidad son claves para captar y manejar información en función de las operaciones para los cuales son utilizados. En este apartado el estudiante aprenderá como Identificar un Dron, los usos comunes, y las diferentes categorías que se manejan en dependencia de su función y peso, además de conocer los tipos de drones, como están relacionados con la Ciberseguridad de forma tal que los configure de manera adecuada, como detectar, identificar y neutralizar estos equipos, las condiciones legales a tomar en cuenta para volar estos dispositivos y finalmente las app más recomendadas para usar drones.

Módulo 8. Anonimato en la Red

El estudiante de Escolta digital no dejara huella en la red si coloca lo visto en este módulo, ya que aprenderá a navegar de forma segura utilizando las opciones avanzada de los navegadores más usados, además conocerá los servicios de cuentas de correos temporales como YooMail, Borrara y hará seguimiento para obtener un listado de todas las plataformas donde su cuenta se encuentra activa con deseat.me. Conocerá y sabrá cifrar información utilizando las mejores herramientas para la protección de la información usando PGP, GPGW4WIN y Kleopatra. Con los dispositivos móviles no se quedara atrás ya que conocerá la forma más segura y privada de comunicarse a partir de las app más usadas en el tema.

Módulo 9 aseguramiento de cuentas

Uno de los tópicos de mayor relevancia en la actualidad por lo que representa nuestra segunda vida o “nuestra identidad digital” es el aseguramiento de cuentas digitales, factor clave en el cual el estudiante de Escolta Digital conocerá las barreras de seguridad necesarias a implementar para blindar sus cuentas en redes sociales, disminuyendo considerablemente las posibilidades de éxitos de un ciberataque, habilitar el doble factor de autenticación, configurar la privacidad de sus cuentas, deshabilitar controles de búsqueda y seguimiento por geocalización, identificar que equipos están conectados a sus cuentas , tiempo y ubicación, detectar intrusos en la red Wifi, y el resguardo de contraseñas a través de software Keepass, entre otros, proveerá una protección avanzada que garantizara que su información permanecerá segura.

Módulo 10. Aseguramiento de Dispositivos tecnológicos (IoT)

La era de las cosas conectadas a Internet es una realidad definitiva, conozca a través de este módulo que significa el Internet de las cosas, las tendencias y el flanco de ataque número uno de los delincuentes para generar nuevas y gigantes Botnets. Actualícese de los ataques que posiblemente tanto el estudiante como las personas que están a su alrededor puedan que sean víctimas pero aún no lo sabe. Los Smart Tv flanco de ataque, conozca como configurarlo y protegerse.

Módulo 11 almacenamiento seguro

En este módulo el estudiante de Escolta Digital será capacitado en Almacenamiento Seguro de la Información, considerando que este es el activo más preciado, su correcto almacenamiento proveerá confianza y garantizara el resguardo de la misma. Conocer e identificar los dispositivos que se utilizan para tal fin, manejar la tendencia actual de almacenamiento en la nube, aprender a encriptar las unidades de almacenamiento, como enviar mensajes encriptados a través de redes sociales, además de conocer herramientas para enviar archivos protegidos con clave, finalmente aprender a cifrar los dispositivos móviles muy utilizados donde usualmente manejamos información muy valiosa, son puntos de relevancia a través de los cuales el participante desarrollara habilidades y buenas prácticas en seguridad de la información

Módulo 12.Borrado seguro de la información

Si usted realmente desea borrar un documento sepa que no es suficiente enviando cualquier tipo de archivo a la papelera de reciclaje de su equipo y luego vaciando la carpeta y mucho menos formateando, es necesario formatear 32 veces el dispositivo para que definitivamente ningún programa de recuperación parcial o total lo recupere, el estudiante conocerá las herramientas más efectivas para realizar los borrados seguros y definitivos. Sepa cómo borrar información de sus cuentas y de sus dispositivos móviles. Conozca cómo destruir un dispositivo de manera efectiva, sabía que existe una USB Killer que daña en definitivo su equipo al conectarla.

Módulo 13. Recuperación de información

Después de conocer como Borrar información, sepa que herramientas le servirían para recuperar si por error o por un daño temporal de los dispositivos se eliminó información importante. Entender la importancia de emplear buenas prácticas a la hora de realizar el respaldo de la información o Backups. Conocer la existencia de laboratorios especializados en recuperación de información de dispositivos que han tenido daños físicos significativos.

Módulo 14 Fuentes Osint y control reputacional

En este apartado el estudiante de Escolta Digital aprenderá como buscar información de forma efectiva a través de las Fuentes Osint, optimizara las búsquedas de su interés utilizando herramientas avanzadas, entendiendo como

es el proceso de búsqueda a través de las distintas fases de las fuentes Osint, de igual forma tendrá acceso a los buscadores especializados explotando al máximo su potencial ya que desarrollara habilidades para tales fines, aprender y manejar software para recolección de metadatos, google hacking, además de identificar la fuente y veracidad de una dirección de correo electrónico a través del dominio, finalmente comprenderá la importancia de censar su presencia en redes sociales, teniendo en cuenta el control reputacional, y la capacidad de implementar correctivos frente a una campaña de desprestigio, así como activar controles que le notifican cuando alguien está hablando de usted o su marca son temas vitales que seguro podrá aprovechar para ser mucho más acertado e integral en una era totalmente digital.

Módulo 15. Esteganografía

Existen desde la antigüedad prácticas para ocultar información importante y muy confidencial, en la segunda guerra mundial esto fue un punto determinante para ganar la guerra. Conozca las diferentes historias del arte de la esteganografía y conozca como en esta nueva era es muy utilizada para enviar información y ocultar virus o malware. Aprenda esta práctica utilizando herramientas como OpenPuff.

Módulo 16. Identificación de Fallos y Vulnerabilidades en la Seguridad Electrónica

Debido que la seguridad electrónica es un complemento de la seguridad física, en este módulo el estudiante de escolta digital podrá identificar vulnerabilidades que ponen en riesgo todo un sistema automatizado casi “perfecto”, aquí conocerá como configurar de forma adecuada los dispositivos electrónicos, cambiando usuarios y contraseñas por defecto, implementar controles para el manejo de estos dispositivos, como DVR, NVR, router Wifi, impresoras, etc, al mismo tiempo aprenderá las prácticas más comunes para inhabilitar estos controles de acceso y monitoreo, con fines éticos para tomar medidas preventivas y correctivas ante posibles ataques de este tipo.

Módulo 17. Identificación evaluación de riesgos e implementación de medidas de Sistemas de información.

Si el estudiante llego a este módulo muchas felicidades, ya obtuvo los conocimientos y las herramientas necesarios para ser un ESOCLTA DIGITAL. En este módulo encontrara el paso a paso de como iniciar una auditoria además de tener disponible formatos de interés como acuerdos de confidencialidad y CHECK LIST para realizar una auditoría de riesgos digitales orientado a la formación si lo que quiere es proteger a una persona o a una organización.

TITULACIÓN

Una vez realizado el curso el estudiante recibirá un certificado valorado por HACK&SECURE SAS y el SECURITY COLLEGE de EEUU. Que lo acredita como ESCOLTA DIGITAL. Para ello, deberá haber completado en su totalidad los módulos y presentado los test de evaluación.