MÓDULOS DEL CURSO

Servicio de capacitación y concientización en ciberseguridad de Fortinet

Módulos de capacitación básica

Los módulos de capacitación son módulos interactivos de aproximadamente ocho minutos que están diseñados para enseñarles a los estudiantes a través de presentaciones y ejercicios interactivos multimedia. Los cursos incluyen exámenes y evaluaciones.

	Tiempo del curso (en minutos)	Servicio estándar	Servicio premium
Concientización sobre la seguridad de la información	9:40	✔	✔
Actores maliciosos	11:20	✔	✔
Ingeniería social	8:00	✔	✔
Ataques de suplantación de identidad	9:40	✔	✔
Seguridad de correo electrónico	12:20	✔	✔
Malware y ransomware	9:10	✔	✔
Protección de contraseña	12:20	✔	✔
Autenticación de múltiples factores	11:00		✔
Seguridad de datos	12:10		✔
Privacidad de datos	10:30		✔
Control de acceso	12:20		✔
Seguridad móvil	13:00		✔
Amenaza interna	9:30		✔
Política de escritorio limpio	8:20		✔
Teletrabajo	10:10		✔
Seguridad de conferencias web	7:10		✔
Compromiso del correo electrónico empresarial	8:30		✔
Propiedad intelectual	9:00		✔
Consejos para un viaje seguro	13:20		✔
Redes sociales	10:20		✔
Gerentes: Marcos de seguridad de la información	16:50		✔
Gerentes: Concientización sobre la seguridad de la información	13:10		✔
Gerentes: Implementación y administración del servicio de capacitación y concientización en ciberseguridad de Fortinet	12:50		✔

Micromódulos de capacitación

Los micromódulos son un resumen de los módulos base, normalmente de menos de dos minutos cada uno, que se utilizan como seguimiento de los módulos base para reforzar un tema específico.

	Servicio estándar	Servicio premium
Ingeniería social	✔	✔
Ataques de suplantación de identidad	✔	✔
Seguridad de correo electrónico	✔	✔
Malware y ransomware	✔	✔
Protección de contraseña	✔	✔
Seguridad de datos		✔
Privacidad de datos		✔
Compromiso del correo electrónico empresarial		✔
Amenaza interna		✔
Política de escritorio limpio		✔

Módulos de nano capacitación

Los nanomódulos, que suelen durar menos de un minuto, pueden utilizarse para reforzar un tema o como ayudas/accesorios para promover la concientización en ciberseguridad en toda la organización.

	Servicio estándar	Servicio premium
Espionaje sobre el hombro	✔	✔
Tailgating	✔	✔
¿Ve algo?, ¿escucha algo?, diga algo	✔	✔
Seguir las políticas de la empresa	✔	✔
Evite conectarse a redes Wi-Fi desconocidas	✔	✔
Buena higiene de las contraseñas	✔	✔
Piense antes de hacer clic	✔	✔
Consejos de conferencias web		✔
Consejos para viajar		✔
Haga una copia de seguridad de sus datos		✔
Eliminación de datos		✔
Desactive el Wi-Fi automático		✔
Cifre información confidencial		✔
Active los bloqueos de pantalla		✔
Actualice su software		✔
Proteja sus dispositivos		✔
Bluetooth no detectable		✔
Utilice autenticación de múltiples factores		✔

Módulos base por agrupación de temas

SERVICIO ESTÁNDAR

SERVICIO PREMIUM

	Concientización sobre InfoSec	Privacidad de datos	Seguridad en Internet	Protección de contraseña	Seguridad física
Concientización sobre la seguridad de la información	✔				
Actores maliciosos	✔		✔		
Ingeniería social	✔		✔		✔
Ataques de suplantación de identidad	✔	✔	✔	✔	
Seguridad de correo electrónico	✔	✔	✔		
Malware y ransomware	✔		✔		
Protección de contraseña	✔	✔		✔	
Autenticación de múltiples factores	✔	✔		✔	
Seguridad de datos	✔	✔	✔	✔	✔
Privacidad de fechas	✔	✔			
Control de acceso	✔	✔			✔
Seguridad móvil	✔		✔	✔	
Amenaza interna	✔	✔	✔	✔	✔
Política de escritorio limpio	✔	✔			✔
Teletrabajo	✔	✔	✔		
Seguridad de conferencias web	✔		✔		
Redes sociales	✔	✔	✔	✔	
Compromiso del correo electrónico empresarial	✔	✔	✔	✔	
Propiedad intelectual	✔	✔			
Consejos para un viaje seguro	✔		✔		✔
Gerentes: Marco de seguridad de la información	✔	✔	✔		
Gerentes: Concientización sobre la seguridad de la información	✔	✔			
Los gerentes: Implementación del Servicio	✔				

Micromódulos por agrupación de temas

SERVICIO ESTÁNDAR

SERVICIO PREMIUM

	Concientización sobre InfoSec	Privacidad de datos	Seguridad en Internet	Protección de contraseña	Seguridad física
Ingeniería social	✔		✔		✔
Ataques de suplantación de identidad	✔	✔	✔	✔	
Seguridad de correo electrónico	✔	✔	✔		
Malware y ransomware	✔		✔		
Protección de contraseña	✔	✔		✔	
Seguridad de datos	✔	✔	✔	✔	✔
Privacidad de datos	✔	✔			
Compromiso del correo electrónico empresarial	✔	✔		✔	
Amenaza interna	✔	✔	✔	✔	✔
Política de escritorio limpio	✔	✔	✔		✔

Descripciones del curso

Nombre del módulo	Descripción
Control de acceso	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir el control de acceso y las estrategias de confianza cero ▪ Describir la autenticación, la autorización y el registro ▪ Enumerar los principales tipos de control de acceso ▪ Describir la importancia del control de acceso ▪ Enumerar las acciones a efectuar
Actores maliciosos	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Identificar los tipos de actores maliciosos ▪ Conocer los motivos de los actores maliciosos ▪ Enumerar las acciones para evitar ataques de ciberseguridad ▪ Conocer a las personas que son actores maliciosos
Compromiso del correo electrónico empresarial	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir las estrategias comunes que utilizan los actores maliciosos para comprometer la seguridad del correo electrónico de su empresa ▪ Identificar las diferentes etapas de un ataque BEC ▪ Enumerar las acciones que puede efectuar para protegerse de un ataque BEC
Política de escritorio limpio	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describa los riesgos ▪ Defina el principio de escritorio limpio ▪ Enumere ejemplos de la adherencia al principio de escritorio limpio ▪ Enumere las acciones que debe efectuar para proteger la información en su espacio de trabajo
Privacidad de datos	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir la privacidad de datos ▪ Describir la importancia de la privacidad de datos ▪ Describir la función de la organización ▪ Enumerar tipos de datos y regulaciones ▪ Enumerar las acciones que puede realizar
Seguridad de datos	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir la seguridad de datos ▪ Describir el ciclo de vida de los datos ▪ Enumerar los tipos de datos y los riesgos ▪ Enumerar los riesgos de los datos no seguros ▪ Enumerar las acciones que puede realizar
Seguridad de correo electrónico	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Identificar las tácticas que se utilizan para comprometer la seguridad del correo electrónico ▪ Conocer por qué el correo electrónico es un objetivo ▪ Reconocer las señales de un ataque por correo electrónico ▪ Enumerar las acciones para evitar que la seguridad del correo electrónico se comprometa
Amenaza interna	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describa los tipos de amenaza interna ▪ Conozca cómo puede ocurrir una amenaza interna ▪ Enumere las acciones para evitar convertirse o ayudar en una amenaza interna
Propiedad intelectual	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Definir la propiedad intellectual ▪ Identificar cómo puede ocurrir el robo de propiedad intellectual ▪ Enumerar las acciones que puede efectuar para mitigar el robo de propiedad intelectual
Concientización sobre la seguridad de la información	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir la concientización de la seguridad de la información ▪ Describir conceptos y términos clave

Nombre del módulo	Descripción
Malware y ransomware	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir el malware ▪ Describir los tipos de malware ▪ Describir cómo evitar el malware ▪ Enumerar los signos de un ataque de malware ▪ Enumerar las acciones que puede realizar
Seguridad móvil	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describa cómo se utilizan los dispositivos móviles en el lugar de trabajo ▪ Conozca los riesgos de seguridad que involucra el uso de dispositivos móviles ▪ Enumere las acciones para mitigar los riesgos asociados con el uso de dispositivos móviles
Autenticación de múltiples factores	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir el propósito de la MFA ▪ Enumerar los tipos de MFA ▪ Describir cómo la MFA aumenta la seguridad ▪ Enumerar las acciones que puede efectuar para proteger su información
Protección de contraseña	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir los riesgos ▪ Enumerar las características de las contraseñas no seguras ▪ Enumerar las características de las contraseñas seguras y únicas ▪ Enumerar las acciones para proteger su contraseña
Ataques de suplantación de identidad	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir el phishing y otras formas comunes de ciberataque ▪ Describir los riesgos asociados con ataques de phishing ▪ Describir cómo identificar y evitar ataques de phishing ▪ Enumerar las medidas que pueden adoptar los empleados para evitar convertirse en la víctima de un ataque de phishing
Consejos para un viaje seguro	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Identificar cómo se puede poner en riesgo la ciberseguridad durante un viaje ▪ Describir las tácticas que puede utilizar un actor malicioso ▪ Aplicar acciones para mantenerse seguro mientras viaja
Ingeniería social	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Definir la ingeniería social ▪ Conocer los riesgos ▪ Enumerar los vectores de ataque típicos ▪ Enumerar las acciones que puede realizar
Es sociales	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir los riesgos asociados con las redes sociales ▪ Conocer algunas de las vulnerabilidades comunes asociadas con las redes sociales ▪ Enumerar las acciones que puede efectuar para proteger sus cuentas de redes sociales
Seguridad de conferencias web	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describa los riesgos asociados con las conferencias web ▪ Enumere las acciones que puede efectuar para mitigar los riesgos asociados con las conferencias web
Teletrabajo	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describa los riesgos asociados con el teletrabajo ▪ Describa las estrategias comunes que utilizan las organizaciones para proteger los entornos de teletrabajo ▪ Enumere las acciones que los empleados pueden efectuar para mantener su información segura durante el teletrabajo
Gerentes: Marcos de seguridad de la información	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir la evolución de las ciberamenazas ▪ Describir la evolución de la superficie de ataque. ▪ Describir estudios de casos de la vida real de ciberataques de alto perfil ▪ Enumere las acciones que puede efectuar para crear una fuerza laboral ciberconsciente

Nombre del módulo	Descripción
Gerentes: Concientización sobre la seguridad de la información	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir los marcos de trabajo de ciberseguridad ▪ Describir los 10 principios de la ciberresiliencia del Foro Económico Mundial (WEF) ▪ Describir el marco de trabajo de la ciberseguridad (CSF) del NIST ▪ Describir dónde encaja la capacitación en el núcleo del CSF del NIST ▪ Describir brevemente el servicio de capacitación sobre la concientización de la seguridad de Fortinet
Gerentes: Implementación y administración del servicio de capacitación y concientización en ciberseguridad de Fortinet	Al final de esta breve lección, sus alumnus podrán hacer lo siguiente: ▪ Describir cómo planificar la implementación del servicio de concientización y capacitación sobre seguridad de Fortinet ▪ Describir cómo implementar el servicio ▪ Describir cómo efectuar una posimplementación y evaluación continua del servicio

Recursos de comunicación

Los recursos de comunicación están disponibles tanto en el servicio estándar como en el premium.

	Posters	Hojas de sugerencias	Protectores de pantalla	Pancartas
Servicio de capacitación y concientización en ciberseguridad				✔
Esté atento: No Tailgating	✔		✔	
Bloquee antes de irse	✔		✔	
¿Ve algo?, ¿escucha algo?, diga algo	✔		✔	
No haga clic tan rápido	✔		✔	
El Wi-Fi gratis tiene un precio	✔		✔	
Sea único: Sus credenciales de acceso son clave para los cibercriminales	✔		✔	
Amenazas internas		✔		
Seguridad móvil		✔		

Sobre el nuevo servicio de capacitación y concientización en ciberseguridad de Fortinet

El servicio de capacitación y concientización en ciberseguridad de Fortinet es una oferta de software como servicio (SaaS) que puede integrarse con FortiPhish para proporcionar una solución clave completa. La capacitación entregada en múltiples formatos, incluyendo video, texto, audio, imágenes y animación, satisface los diferentes estilos de aprendizaje para asegurar que la capacitación sea entendida y aplicada. Las extensiones más pequeñas y fáciles de consumir, como el microaprendizaje y el nanoaprendizaje, junto con los recursos de comunicación, permiten a las organizaciones aumentar su capacitación para ayudar a reforzar las lecciones clave.

Más información sobre el servicio.

FORTINET

www.fortinet.com

julio 29, 2022

1378653-0-0-ES