Objetivos

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Investigar enfoques para la toma de decisiones éticas.
- Parte 2: Investigar el código de ética
- Desarrolle su propio código personal de conducta ética

Trasfondo / Situación

Cuando se enfrenta a un dilema ético, ¿qué considera al tomar una decisión?

Supongamos que encuentra una nueva unidad flash en el laboratorio de computación, ¿qué haría? Un estudiante de su clase dice que encontró un sitio en Internet que tiene todos los exámenes y cuestionarios de la clase con respuestas, ¿qué haría?

Trabajar en ciberseguridad no siempre implica detener los ciberataques. Como especialista en ciberseguridad, su organización puede confiarle algunos de los datos más confidenciales de los clientes. Se enfrentará a dilemas éticos desafiantes, que pueden no tener una respuesta fácil o clara.

El enfoque de este laboratorio es investigar enfoques o perspectivas para la toma de decisiones éticas. A continuación, investigará códigos de ética y, por último, creará su propio código personal de conducta ética.

Recursos necesarios

- Computadora o dispositivo móvil con acceso a Internet

Instrucciones

Parte 1: Enfoques de investigación para la toma de decisiones ética

Existen varios enfoques o perspectivas sobre la Toma de Decisiones Éticas, incluida la Ética Utilitaria, el Enfoque de Derechos y el Enfoque de Bien Común. Otros modelos de decisión ética incluyen el Enfoque de Equidad o Justicia, así como el Enfoque de la Virtud.

En esta parte, investigará cada modelo o marco de decisión ética y luego formulará el principio subyacente a partir de ese enfoque.

Paso 1: Investigar la ética utilitaria

Defina el principio subyacente del enfoque de la ética utilitaria.

"El principio fundamental del utilitarismo es que una acción es moralmente correcta si produce el mayor bienestar posible para el mayor número de personas."

Paso 2: Investigue el enfoque de derechos en la toma de decisiones éticas.

Definir el principio subyacente del enfoque de derechos en la toma de decisiones éticas.

"Una acción es moralmente correcta si respeta los derechos fundamentales de todas las personas involucradas, independientemente de las consecuencias."

Paso 3: Investigue el enfoque del bien común para la toma de decisiones éticas.

Definir el principio subyacente del enfoque del bien común para la toma de decisiones éticas.

"Una acción es ética si contribuye al bienestar general de la sociedad y promueve el beneficio compartido por todos sus miembros."

Paso 4: Investigue el enfoque de equidad o justicia en la toma de decisiones éticas.

Defina el principio subyacente del enfoque de equidad o justicia en la toma de decisiones éticas.

"Una acción es ética si trata a todas las personas de manera justa e imparcial, garantizando igualdad de oportunidades y corrigiendo desigualdades cuando sea necesario."

Parte 2: Código de Ética de la Investigación

La mayoría de las organizaciones desarrollan su propio código de ética. Desarrollado por la gerencia, este documento se basa en valores y principios para promover el negocio de la empresa con honestidad e integridad.

En esta parte, investigará códigos de ética de la tecnología de la información.

Utilice un navegador de Internet para investigar el código de ética.

Según su investigación, cree una lista de al menos diez elementos. La lista debe ser secuencial de lo más importante a lo menos importante.

Lista de 10 Elementos de un Código de Ética en TI

Honestidad e Integridad – Actuar con transparencia y veracidad en todas las actividades relacionadas con la tecnología.

Respeto a la Privacidad – Proteger la información personal y confidencial de los usuarios y clientes.

Seguridad de la Información – Implementar y mantener medidas de seguridad para evitar accesos no autorizados o ciberataques.

Cumplimiento de la Ley – Cumplir con las regulaciones y leyes de protección de datos, ciberseguridad y derechos digitales.

No causar daño – Evitar desarrollar o implementar tecnologías que puedan causar daño intencional o negligente a individuos o comunidades.

Equidad e Inclusión – Diseñar sistemas accesibles y sin sesgos discriminatorios para garantizar la equidad en el acceso y uso de la tecnología.

Uso Responsable de los Recursos – No utilizar la tecnología para actividades ilícitas o poco éticas, como la piratería o el espionaje.

Respeto a la Propiedad Intelectual – No plagiar ni usar software, hardware o información de manera no autorizada.

Transparencia y Responsabilidad – Explicar claramente cómo funciona la tecnología y asumir responsabilidad por su impacto.

Mejora Continua y Educación – Mantenerse actualizado en temas de ética y seguridad en TI para tomar decisiones informadas.

Parte 3: Desarrolle su propio código personal de conducta ética

Un código de conducta proporciona pautas para comportamientos específicos aceptables e inaceptables.

Busque en Internet códigos de conducta éticos sobre la piratería informática. Desarrolle su propio código de conducta ética personal para los hackers en función de sus hallazgos.

a. Cree un código personal de ética profesional mediante la recopilación de una lista de al menos diez elementos. La lista debe ser secuencial de lo más importante a lo menos importante.
b. Firme el documento como una forma de expresar su compromiso de seguir los principios éticos en su práctica de piratería ética. Conserve este código de ética.

Registre su propio código personal de conducta ética a continuación:

Código Personal de Ética Profesional para Hackers

No causar daño – No utilizar habilidades de hacking para dañar personas, empresas, gobiernos o infraestructuras.

Respeto a la privacidad – No acceder, recopilar ni divulgar información personal sin el consentimiento explícito del propietario.

Uso responsable del conocimiento – Aplicar el conocimiento en ciberseguridad para proteger y mejorar la seguridad digital, no para actividades ilegales.

Legalidad ante todo – Cumplir con las leyes y regulaciones sobre ciberseguridad, privacidad y propiedad intelectual.

Transparencia y ética profesional – Actuar con honestidad y rendir cuentas por las acciones tomadas en el ámbito de la ciberseguridad.

Divulgación responsable de vulnerabilidades – Informar de manera ética a las organizaciones sobre fallos de seguridad en lugar de explotarlos para beneficio propio.

No al cibercrimen – No participar en actividades como el robo de datos, fraudes electrónicos, distribución de malware o ataques de denegación de servicio (DDoS) no autorizados.

Contribuir al bien común – Usar habilidades para mejorar la seguridad en línea y educar a otros en buenas prácticas digitales.

Respeto por la propiedad intelectual – No copiar, modificar ni distribuir software, datos o herramientas sin autorización.

Aprendizaje continuo – Mantenerse actualizado en ciberseguridad y ética para adaptarse a las nuevas amenazas y desafíos tecnológicos.

Preguntas de reflexión

1. ¿Conoce algún incidente de ciberseguridad en el que una empresa fue acusada de actuar de manera poco ética? Si no es así, busque en Internet un ejemplo de esto. Explique

Un ejemplo notable de una empresa acusada de actuar de manera poco ética en un incidente de ciberseguridad es el caso de Ashley Madison en 2015. Ashley Madison era un sitio web que facilitaba encuentros extramatrimoniales, y en julio de 2015, un grupo de hackers llamado "The Impact Team" accedió a su base de datos, obteniendo información sensible de millones de usuarios. Los atacantes exigieron el cierre del sitio; de lo contrario, divulgarían los datos obtenidos. La empresa se negó, y en agosto de 2015, los hackers publicaron más de 60 gigabytes de datos, incluyendo detalles personales de los usuarios.

La controversia ética surgió porque, aunque Ashley Madison ofrecía un servicio de "eliminación completa" de perfiles por una tarifa, la filtración reveló que la empresa no eliminaba realmente la información de los usuarios que pagaban por este servicio. Además, se descubrió que muchas cuentas fueron creadas sin el consentimiento de los propietarios de las direcciones de correo electrónico, y la empresa exigía un pago para eliminarlas. Estas prácticas engañosas y la falta de medidas de seguridad adecuadas llevaron a acusaciones de comportamiento poco ético por parte de la empresa.

Este incidente destaca la importancia de que las empresas manejen los datos de los usuarios con integridad y transparencia, implementando medidas de seguridad robustas y cumpliendo con las promesas hechas a sus clientes.

2. Basándose en su lista de códigos éticos, ¿cuál es el elemento más difícil de seguir en su lista?

Legalidad ante todo – Cumplir con las leyes y regulaciones sobre ciberseguridad, privacidad y propiedad intelectual.

Las respuestas pueden variar. Como hacker ético, puede obtener acceso a sistemas protegidos que contienen datos personales o corporativos. Obtener acceso a los archivos sin leerlos innecesariamente puede ser un desafío para algunos profesionales.