Arthiax · Formaciones

Prevención y protección digital: como protegerse del acoso y las amenazas digitales

Duración: 60 h

Objetivos

Este curso está diseñado para proporcionar a los participantes los conocimientos y herramientas necesarios para protegerse frente al acoso digital y otras amenazas cibernéticas, tanto en el ámbito laboral como personal. A lo largo del curso los usuarios aprenderán a reconocer las diferentes formas de violencia digital, cómo proteger su información y privacidad, y cómo mantener sus dispositivos seguros. El curso incluye desde los conceptos básicos de ciberseguridad, como la gestión de contraseñas seguras y la autenticación en dos pasos, hasta prácticas más avanzadas como la configuración de dispositivos móviles, el uso de redes Wi-Fi públicas de manera segura, y la prevención de suplantación de identidad. Con un enfoque práctico, se abordan las amenazas más comunes en el entorno digital y se proporcionan estrategias y herramientas para una defensa efectiva en el día a día.

TEMARIO

Tema 1: Introducción al acoso y violencia digital

Definición de violencia y acoso digital

1.1.1. Qué es el acoso digital y cómo se manifiesta

1.1.2. Tipos de violencia digital: laboral y personal

1.1.3. Diferencias entre acoso físico y acoso digital

1.1.4. Ejemplos reales de violencia digital

1.2. El impacto del acoso digital en el entorno laboral

1.2.1. Consecuencias psicológicas y emocionales

1.2.2. Cómo el acoso digital afecta el rendimiento laboral

1.2.3. Casos de estudio: acoso digital en el trabajo

1.2.4. Medidas preventivas desde la empresa

1.3. El acoso digital en el ámbito personal

1.3.1. El acoso a través de redes sociales

1.3.2. La invasión de la privacidad personal en el entorno digital

1.3.3. Cómo identificar acoso digital en redes sociales

1.3.4. Estrategias para proteger la privacidad

1.4. Herramientas básicas de defensa digital

1.4.1. Contraseñas seguras y autenticación en dos pasos

1.4.2. Seguridad en redes sociales y correos electrónicos

1.4.3. Protección de la identidad digital

1.4.4. Herramientas para la detección de amenazas digitales

Tema 2: Protección de datos personales en entornos digitales

2.1. Qué es la protección de datos y por qué es importante

2.1.1. Datos personales y su valor en el entorno digital

2.1.2. Riesgos comunes relacionados con la filtración de datos

2.1.3. Cómo proteger los datos personales en internet

2.1.4. La importancia del consentimiento digital

2.2. Herramientas y prácticas de protección de datos

2.2.1. Cifrado de información en dispositivos

2.2.2. Uso de VPN y otras herramientas de privacidad

2.2.3. Buenas prácticas al compartir información personal en línea

2.2.4. Cómo gestionar el acceso a datos en dispositivos compartidos

2.3. Protección de datos en el entorno laboral

2.3.1. Políticas de protección de datos en la empresa

2.3.2. Protección de datos de empleados y clientes

2.3.3. El teletrabajo y la protección de datos

2.3.4. Qué hacer en caso de brecha de seguridad en la empresa

2.4. Amenazas más comunes: phishing, malware y robo de identidad

2.4.1. Qué es el phishing y cómo evitarlo

2.4.2. Identificación de malware y software malicioso

2.4.3. Cómo se produce el robo de identidad en línea

2.4.4. Acciones a tomar tras un robo de identidad

Tema 3: Ciberseguridad básica para protegerse de amenazas digitales

3.1. Introducción a la ciberseguridad para principiantes

3.1.1. Qué es la ciberseguridad y por qué es relevante

3.1.2. Conceptos básicos de ciberseguridad

3.1.3. Principales amenazas digitales y cómo detectarlas

3.1.4. Buenas prácticas de ciberseguridad personal

3.1.5. Obligaciones legales de las empresas en ciberseguridad (Artículo 21 y Directiva NIS2)

3.2. Herramientas de ciberseguridad

3.2.1. Programas antivirus y cómo utilizarlos

3.2.2. Firewalls y protección de red

3.2.3. Actualizaciones de software y su importancia en la seguridad

3.2.4. Uso seguro de conexiones Wi-Fi públicas

3.3. Gestión de la seguridad digital en la empresa

3.3.1. Ciberseguridad en el entorno laboral

3.3.2. Buenas prácticas en el uso de dispositivos corporativos

3.3.3. Cómo gestionar incidentes de seguridad en la empresa

3.3.4. El rol del empleado en la ciberseguridad empresarial

3.4. Recuperación tras un ataque cibernético

3.4.1. Cómo actuar tras un ciberataque

3.4.2. Recuperación de datos comprometidos

3.4.3. Medidas para evitar futuros ataques

Tema 4: Seguridad digital en dispositivos móviles

4.1. Amenazas en dispositivos móviles: riesgos y vulnerabilidades

4.1.1. Tipos de amenazas digitales en móviles

4.1.2. Cómo los dispositivos móviles son objetivo de ataques

4.1.3. Cómo identificar aplicaciones maliciosas

4.1.4. Cómo protegerse ante ataques en móviles

4.2. Configuraciones de seguridad en móviles

4.2.1. Cómo configurar correctamente la seguridad en móviles

4.2.2. La importancia de las actualizaciones en móviles

4.2.3. Cómo gestionar los permisos de aplicaciones

4.2.4. Herramientas de seguridad en móviles: autenticación y bloqueo

4.3. Protección de datos en dispositivos móviles

4.3.1. Cómo proteger la información personal en el móvil

4.3.2. Seguridad en la nube para dispositivos móviles

4.3.3. Qué hacer en caso de robo o pérdida del móvil

4.3.4. Uso seguro de redes Wi-Fi en móviles

4.4. Buenas prácticas en el uso de dispositivos móviles en el trabajo

4.4.1. Seguridad de dispositivos móviles corporativos

4.4.2. Cómo evitar filtraciones de datos desde dispositivos móviles

Tema 5: Seguridad en el uso de redes sociales

5.1. Introducción a la seguridad en redes sociales

5.1.1. Riesgos comunes en redes sociales

5.1.2. Cómo proteger la privacidad en redes sociales

5.1.3. Configuración de seguridad en redes populares

5.1.4. Cómo evitar fraudes y estafas en redes sociales

5.2. Gestión de la identidad digital en redes sociales

5.2.1. Cómo gestionar la reputación digital

5.2.2. Control de la información personal en redes

5.2.3. Qué hacer en caso de suplantación de identidad

5.2.4. Redes sociales y acoso: cómo detectarlo y denunciarlo

5.3. Seguridad laboral y redes sociales

5.3.1. Riesgos laborales en redes sociales

5.3.2. Políticas de uso seguro de redes sociales en el trabajo

5.3.3. Cómo gestionar la seguridad de las cuentas corporativas

5.3.4. Qué hacer en caso de ataque a redes sociales corporativas

5.4. Herramientas de protección en redes sociales

5.4.1. Uso de herramientas de monitorización y alerta

5.4.2. Herramientas de denuncia y reporte en redes sociales

5.4.3. Configuración avanzada de seguridad en redes

5.4.4. Estrategias para evitar el acoso y las amenazas en redes

Tema 6: Herramientas y estrategias para la protección frente a suplantación de identidad

6.1. Qué es la suplantación de identidad digital

6.1.1. Cómo funciona la suplantación de identidad en línea

6.1.2. Ejemplos de suplantación de identidad

6.1.3. El impacto de la suplantación de identidad en la vida personal y laboral

6.1.4. Cómo identificar un intento de suplantación de identidad

6.2. Medidas preventivas contra la suplantación de identidad

6.2.1. Uso de contraseñas seguras y gestión de credenciales

6.2.2. La importancia de la autenticación en dos pasos

6.2.3. Control y protección de la información personal

6.2.4. Cómo actuar ante un intento de suplantación

Tema 7: Buenas prácticas y hábitos de seguridad digital

7.1. Uso de VPN

7.1.1. Qué es una VPN

7.1.2. Ventajas e inconvenientes de usar una VPN

7.1.3. Cómo instalar una VPN

7.2. Gestión de contraseñas y seguridad en internet

7.2.1. Consejos para crear y gestionar contraseñas seguras

7.2.2. Gestores de contraseñas y su uso

7.2.3. Navegación segura: qué hacer y qué evitar

7.2.4. Cómo detectar sitios web no seguros y evitar estafas en línea

7.3. Seguridad en correos electrónicos y mensajería instantánea

7.3.1. Cómo identificar correos maliciosos y phishing

7.3.2. Buenas prácticas en el uso del correo electrónico

7.3.3. Cómo asegurar la comunicación a través de mensajería instantánea

7.3.4. Qué hacer en caso de recibir un correo sospechoso

7.4. Formación continua en seguridad digital

7.4.1. Por qué es importante la formación en seguridad digital

7.4.2. Recursos disponibles para la formación continua

7.4.3. Actualización constante de las amenazas digitales

7.4.4. Cómo implantar un plan de seguridad en la empresa