Hábilon elearning

CONTENIDO

HÁBITOS SEGUROS FRENTE AL FRAUDE DIGITAL

CÓDIGO	AUTOR	DURACIÓN ESTIMADA	NIVEL DE FORMACIÓN
01B09C03	Yolanda Corral	15 h	Medio

Dirigido a

Profesionales de cualquier área que utilicen correo electrónico, mensajería, herramientas colaborativas o canales digitales y necesiten prevenir engaños, suplantaciones y fraudes en el trabajo.

Descripción

Con este contenido de curso profesional el alumnado aprenderá a reconocer y prevenir fraudes digitales en el entorno laboral. Se priorizarán las técnicas de ingeniería social, el phishing y otras formas de suplantación, los engaños facilitados por IA y el uso seguro del correo y de las herramientas colaborativas. El alumnado concretará estos aprendizajes en un plan personal de hábitos preventivos.

COMPETENCIAS

1. Reconocer y asumir la responsabilidad individual en la seguridad digital empresarial, aplicando hábitos seguros en el puesto de trabajo para proteger sus activos de información.
2. Reconocer las dinámicas de manipulación utilizadas en las técnicas de ingeniería social y aplicar criterios de verificación antes de realizar acciones que puedan comprometer la seguridad de la organización.
3. Identificar fraudes y amenazas digitales dirigidos a la organización, aplicando criterios de verificación antes de realizar acciones que puedan comprometer la información, los recursos o la actividad empresarial.
4. Identificar señales de engaño y suplantación facilitadas por la inteligencia artificial, aplicando pautas de verificación reforzada ante comunicaciones o solicitudes de riesgo para evitar engaños altamente sofisticados.
5. Utilizar el correo electrónico y las herramientas colaborativas aplicando hábitos de seguridad preventiva para reducir riesgos en comunicaciones, el intercambio de archivos y el trabajo compartido.
6. Elaborar un plan personal de mejora en seguridad digital para aplicar hábitos preventivos sostenibles en el puesto de trabajo.

CRITERIOS DE EVALUACIÓN (Objetivos)

1. Identificar riesgos digitales habituales en la actividad profesional, relacionándolos con los principios de confidencialidad, integridad y disponibilidad de la información. Diferenciar hábitos seguros e inseguros en el puesto de trabajo, identificando aquellos que puedan aumentar o reducir la exposición a riesgos de seguridad. Comprender el modelo de responsabilidad compartida y el papel del empleado en la protección de la organización.
2. Reconocer los principales mecanismos de manipulación psicológica utilizados en los intentos de ingeniería social, como la urgencia, la autoridad, el miedo, la ilusión o la confianza. Identificar situaciones de riesgo en las que se induce a la acción rápida, al incumplimiento de procedimientos internos o a la revelación de información corporativa. Aplicar el pensamiento crítico y pautas de verificación ante peticiones inusuales, imprevistas o sospechosas, respetando los procedimientos de seguridad de la organización.
3. Reconocer señales características de phishing, smishing, vishing, qrishing y otros fraudes digitales habituales en el entorno profesional. Diferenciar comunicaciones legítimas de intentos de engaño, aplicando criterios de contraste sobre remitentes, dominios, enlaces, archivos adjuntos, solicitudes y otros elementos de la comunicación. Aplicar pautas de verificación mediante canales seguros antes de responder, descargar archivos, ejecutar software o autorizar operaciones financieras o bancarias.
4. Reconocer usos de la inteligencia artificial generativa que pueden facilitar la suplantación y la elaboración de contenidos engañosos, como la clonación de voz, los deepfakes y la generación de textos persuasivos. Identificar señales de riesgo en comunicaciones, contenidos o solicitudes aparentemente legítimos, especialmente cuando implican suplantación de personas, cambios de instrucciones o acciones sensibles que puedan derivar en daños para la organización. Aplicar pautas de verificación reforzada ante solicitudes críticas o situaciones en las que pueda existir suplantación mediante contenidos generados o manipulados con IA.
5. Aplicar pautas seguras en el envío de correos electrónicos, verificando destinatarios, adjuntos y enlaces y utilizando la copia oculta (CCO) cuando sea necesario para proteger las direcciones de los destinatarios. Reconocer riesgos habituales en entornos colaborativos al compartir, editar o dar acceso a documentos, especialmente cuando intervienen usuarios externos a la organización. Configurar, revisar y revocar permisos de acceso al compartir carpetas o archivos con usuarios internos o externos, aplicando criterios de necesidad y mínimo acceso."
6. Analizar las vulnerabilidades, riesgos y hábitos digitales presentes en las tareas, herramientas y rutinas del puesto de trabajo, identificando las principales áreas de mejora. Elaborar un plan de mejora en seguridad digital, priorizando acciones y hábitos preventivos realistas y aplicables al puesto de trabajo, y diferenciando entre medidas inmediatas y actuaciones que requieren coordinación interna.

CONTENIDOS

Unidad 1. Cultura de seguridad digital en la empresa y responsabilidad en la empresa

1. Seguridad de la información en la actividad empresarial
   1.1. Triada CID: Confidencialidad, integridad y disponibilidad de la información
2. El papel del empleado en la seguridad digital
   2.1. Hábitos seguros e inseguros en el puesto de trabajo
3. Responsabilidad compartida en la organización

Unidad 2. Ingeniería social y psicología del engaño
1. Principios de la ingeniería social.
    1.1. Psicología del engaño: urgencia, autoridad, miedo, escasez y simulación de confianza
2. Técnicas de manipulación y persuasión en el entorno profesional
3. Verificación antes de actuar
    3.1. Criterio de verificación y pensamiento crítico
    3.2. Comprobación de la legitimidad de las peticiones

Unidad 3. Riesgos y amenazas: phishing, ransomware y fraudes empresariales
1. Fraudes digitales habituales en la empresa
    1.1. Phishing mediante correo electrónico corporativo
    1.2. Smishing y mensajería instantánea
    1.3. Qrishing mediante códigos QR
    1.4. Vishing y llamadas de suplantación
2. Suplantación y fraude en las relaciones empresariales
    2.1. Estafas BEC: fraude del CEO, suplantación de directivos y proveedores
    2.2. Solicitudes fraudulentas: pagos, cambios de cuenta y peticiones de información
3. Ransomware y secuestro de información
    3.1. Vías de entrada y consecuencias del ransomware
    3.2. Extorsión y exposición de información robada
4. Verificación antes de actuar

Unidad 4. Evolución de los engaños y amenazas en la era de la IA
1. Evolución de los engaños con inteligencia artificial generativa (IA)
    1.1. Suplantación de identidad: deepfakes de voz y vídeo en el entorno empresarial
    1.2. Perfiles falsos e identidades sintéticas en entornos profesionales
2. Perfeccionamiento de los ataques mediante IA
3. Verificación reforzada ante solicitudes de riesgo

Unidad 5. Uso seguro del correo y herramientas colaborativas
1. Uso seguro del correo corporativo
    1.1. Adjuntos, enlaces y verificación de remitentes
    1.2. Uso de CCO y prevención de exposición de información
2. Herramientas colaborativas e intercambio en la nube
    2.1. Permisos de acceso, edición e invitación a participantes externos

Unidad 6. Plan de mejora de la seguridad digital en el puesto de trabajo
1. Autodiagnóstico de hábitos y conductas digitales en el puesto de trabajo
2. Priorización de mejoras de seguridad
    2.1. Acciones inmediatas de bajo esfuerzo
    2.2. Cambios que requieren coordinación interna
3. Rutinas de higiene digital en el puesto de trabajo
4. Plan personal de seguridad digital
    4.1. Compromisos de mejora y hábitos preventivos sostenible