Digital e inteligencia artificial

Concienciación en ciberseguridad

Una media jornada para que cada empleado reconozca los ataques más comunes y sepa qué hacer: correo de phishing, falsa llamada de un directivo, solicitud fraudulenta de cambio de datos bancarios, memoria USB manipulada, ransomware. Los ejemplos proceden de situaciones de empresa, los buenos reflejos siguen siendo sencillos y la sesión termina con el procedimiento de notificación de su empresa.

Duración : 0,5 día

Objetivos

1. Reconocer un correo, un mensaje o una llamada fraudulentos
2. Aplicar las reglas básicas: contraseñas robustas, gestor de contraseñas, doble autenticación
3. Explicar cómo entra un ransomware en la empresa y qué limita los daños
4. Proteger la información de la empresa en desplazamientos, en teletrabajo y en las redes sociales
5. Notificar sin demora un incidente o una duda, según el procedimiento interno

Programa

Media jornada

• Por qué los atacantes apuntan a los empleados: phishing, suplantación de identidad, fraude del CEO, falso cambio de cuenta bancaria

• Ejercicio: detectar los indicios en una serie de correos verdaderos y falsos

• Contraseñas, doble autenticación, actualizaciones, memorias USB y dispositivos personales

• Asistentes de IA y fugas de información: lo que nunca hay que copiar en una herramienta en línea

• Reflejos ante una duda o un incidente, procedimiento de notificación de la empresa, cuestionario final

Metodología

• Ejemplos reconstruidos de correos y mensajes fraudulentos

• Cuestionario interactivo a lo largo de la sesión

• Juego de rol: la llamada apremiante de un falso proveedor que pide modificar sus datos bancarios

• Posibilidad de impartirla en francés o en darija para los equipos de campo

• Ficha de reflejos de una página entregada a cada participante

Evaluación y documentos

Cuestionario final de conocimientos y evaluación en caliente a J+1. Certificado numerado, verificable en línea, para cada participante; informe de formación entregado a la empresa, con las preguntas que más dificultades plantearon.

Materiales bilingües para cada participante; cada formación presencial incluye su gemelo digital en OmniLearn.

Conviene saber

Formato corto, que puede programarse para varios grupos sucesivos, incluidos los equipos por turnos. Para las reglas sobre datos personales, véase «Datos personales: Ley 09-08 y CNDP».

Información práctica

Duración	0,5 día
Público	Todos los empleados que utilizan un ordenador, un correo o un teléfono profesional
Requisitos previos	Ningún requisito previo
Número de participantes	Grupos de 6 a 12 participantes, en la empresa
Formato	En la empresa, presencial en sus instalaciones
Idioma	Francés, darija o inglés; materiales bilingües
Financiación	Contratos especiales de formación de la OFPPT (TFP), GIAC, Maroc PME: preparamos los expedientes con usted, sin coste adicional.
Personalización del programa	Programa adaptado a sus procedimientos, sus equipos y su público

Preguntas frecuentes

¿Hacen falta conocimientos de informática?
No. La sesión se dirige a todo empleado que utilice correo, un ordenador o un teléfono profesional. No se emplea ningún término técnico sin explicarlo con un ejemplo.

¿Sustituye la formación a las protecciones técnicas?
No, las complementa. Antivirus, filtrado y copias de seguridad reducen los riesgos, pero una gran parte de los ataques pasa por un empleado que hace clic, responde o reenvía. La sesión actúa sobre ese eslabón.

¿En qué se diferencia de la formación ISO/IEC 27001:2022?
ISO/IEC 27001:2022 se dirige a quienes construyen o auditan un sistema de gestión de la seguridad de la información. Esta media jornada se dirige a todos los empleados y trata de los buenos reflejos cotidianos.