Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Universidad de Oviedo

Escuela de Ingeniería Informática
Universidad de Oviedo

CIBERSEGURIDAD GENERAL

CIBER-SUPERPODERES PARA PROTEGERTE A TI Y A LOS TUYOS

Campus Tecnológico-Deportivo para Jóvenes

Universidad de Oviedo

JOSÉ MANUEL REDONDO LÓPEZ PROYECTO *"F-74 'ASTURIAS'"* V1.2

Acerca del uso de contenido generado por IA

José Manuel
Redondo López

- **En esta presentación se usan algunas imágenes generadas por IA**
  - Salvo error, **cualquier imagen a la que no se le atribuya una fuente** u origen expreso
- **La IA generativa usada para ello es Microsoft Copilot**
  - https://copilot.microsoft.com/
- **Se ha restringido el uso de estas imágenes a la ilustración de los conceptos explicados en algunas de las páginas**
  - Es decir, **como refuerzo visual** a lo explicado en algunas transparencias
  - El procedimiento ha sido describirle a la IA con toda la precisión posible los elementos que quería que apareciesen en la imagen (prompt)
    - Y la selección del mejor resultado obtenido, a juicio del autor de esta presentación
    - **No se ha mencionado ni indicado que se copie el estilo a ningún autor, ni que se plagien obras concretas**
- **El autor declara expresamente su apoyo al trabajo de los artistas, ilustradores y creadores, de extrema importancia en la actualidad**
  - El uso de estas técnicas se ha hecho solo con fines de mejora de las explicaciones, y cuando la alternativa era **no contar con refuerzos visuales** por restricciones de tiempo y presupuesto

¡BIENVENIDO!

José Manuel
Redondo López

- Bienvenido a este curso de **Ciberdefensa Personal** para todos ☺
- Gracias a él podrás conocer y poner en práctica una serie de técnicas que te **protegerán** antes un gran nº de ataques diferentes
  - Esto es cada vez más necesario debido a que...¡esto es una plaga!
- El curso identifica los más comunes y da **contramedidas** contra todos ellos
- La intención es mantener seguros tus equipos, los de tus amigos / familiares...o los que usas en el trabajo
- ¡Convertirte en un "**embajador de la ciberseguridad**" en tu entorno! ☺
- ¡Este es un curso que forma parte de la iniciativa "**Asturian Navy**"!
  - Además, este es el "buque capitán" que **coordina el resto de los materiales**

¿Y TODO EL RESTO DE MATERIAL?

José Manuel
Redondo López

- ***¿Sabías que en Asturias hay un programa de formación integrado por niveles en ciberseguridad?*** **Ahora ya sí ☺**
  - Yo soy la persona que está detrás de esta idea
  - Toco muchos “palos” y cada uno tiene un nombre de barco
- ***¿Cómo “enrolarte” en la armada asturiana?***
  - Ofrezco **muchos contenidos gratuitos**
    - Durante este curso se hará referencia a otros complementarios que te regalo y que forman parte de la misma iniciativa
    - Puedes encontrarlos en: https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki
    - En el futuro quiero subir videos explicando cada curso en mi canal: https://www.youtube.com/@JoseRedondo-dj7xk
  - También **imparto clases en la Universidad de Oviedo**
    - Grado en Ingeniería Informática del Software (GIISOF)
    - Máster Universitario en Ingeniería Web (MIUNGEWEB)
    - Micro credenciales (MU), Diplomas y Máster de Formación Permanente (MFP) en temas de Ciberseguridad (Títulos Propios)

TODOS (gratuitos y no gratuitos) están conectados entre ellos y regidos por los mismos estándares de creación y criterios de calidad

Gratis no implica peor, sino pensado para servicio público

Itinerario de concienciación Itinerario de investigación Itinerario técnico

La "Armada Asturiana" por *José Manuel Redondo López*

Respuesta a indecentes
S-64 "Narval"

No apto para menores
Peligros para los menores en Internet
"A-71 Juan Sebastián Elcano"

Investigar Redes Sociales
Técnicas de investigación para RRSS
F-31 "Descubierta"

Configuración Segura Básica
Asegura tus PCs y dispositivos móviles
R-01 "Dédalo"

Rango 1 (Marinero)

La Mente del Crimen
Mentes criminales y engaño
M-31 "Segura"

Ataques contra Personas
Ciberacoso
P-74 "Atalaya"

Investigación de Webs
Detección de webs problemáticas
S-74 "Tramontana"

Investigación de Personas
Buscar a padre, hijo y espíritu santo
"Santísima Trinidad"

Virtualización Básica
Creación y uso de máquinas virtuales
R-11 "Príncipe de Asturias"

Rango 2 (Marinero de Primera)

Ciberseguridad General
Ciberseguridad general para el día a día
F-74 "Asturias"

Crime-spotting
Ejemplos de fraudes reales para su estudio
"Nautilus"

Para vosotr@s, Programador@s
Técnicas básicas de codificación segura
C-23 "Ferrol"

Vigilancia de Redes
Ataque y defensa en redes modernas
F-83 "Numancia"

Rango 3 (Cabo)

La "Armada Asturiana" por *José Manuel Redondo López*

Introducción a la Ciberdefensa Personal

Técnicas generales contra ciberataques (Niveles A1, A2)

Cursos G-9, PDI, Pr. *DIGICOMPEDU. "BPM P-51 'Asturias'"*

Investigación con Fuentes Abiertas (OSINT)

Técnicas de investigación con fuentes abiertas

OCW (parcialmente). *"A-21 Poseidón"*

Defensa contra el Cibercrimen

Identificación y lucha contra el cibercrimen

Divulgación pública, cursos. *P-45 Audaz"*

Rango 4 (Sargento)

Ciberdefensa Personal Avanzada

Técnicas avanzadas contra ciberataques (Niveles B1, B2)

Cursos G-9, PDI, Pr. *DIGICOMPEDU. "BPM P-51 'Asturias'"*

Seguridad de Redes

Threat hunting

TBA. *L-52 "Castilla"*

Administración Segura de SO

Infrastructure as Code

MUINGEWEB, OCW. *L-62 "Princesa de Asturias"*

Seguridad de Sistemas Informáticos

Capacitación técnica general en ciberseguridad

Grado en Ing. del Software, OCW. *S-81 "Isaac Peral"*

Rango 5 (Suboficial Mayor)

Liderazgo en Ciberdefensa para Equipos

Herramientas y estrategias de protección (Nivel C1)

Proyecto *DIGICOMPEDU. "BPM P-51 'Asturias'"*

Identificación y Análisis de Vulnerabilidades en Web

Seguridad ofensiva: Reconocimiento y Explotación

MUINGEWEB, *TK-210 "красный октябрь" (Octubre Rojo)*

Arquitecturas de Seguridad

Arquitectura de infraestructuras seguras

Guías INCIBE, *F-105 "Cristóbal Colón"*

Desarrollo Seguro de Software

Platform engineering seguro

Guías INCIBE. *F-113 "Menéndez de Avilés"*

Rango 6 (Capitán de Fragata)

Innovación e Investigación en Ciberdefensa

Avances e innovación en ciberdefensa (Nivel C2)

Proyecto *DIGICOMPEDU. "BPM P-51 'Asturias'"*

El lado oscuro de la red

Desinformación y ciberguerra

TBA. *"Flying Dutchman"*

Post-Exploiting e Intrusión en Sistemas

Seguridad ofensiva: Post-Explotación

TBA. *K-329 "Belgorod"*

Protección de Servidores y Aplicaciones Web

CISOs de perfil técnico

MUINGEWEB. *D-73 "Blas de Lezo"*

Rango 7 (Vicealmirante)

La "Armada Asturiana" por *José Manuel Redondo López*

Introducción a la construcción de sistemas seguros y rol del CISO

CISOs de perfil técnico

Microcredenciales. *C-33 "Blas de Lezo"*

(D-73 + coordinación de 12 microcredenciales)

Explotación y Post-Explotación de Sistemas

Seguridad ofensiva: Recorrido completo del MITRE ATT&CK

TBA, *RK-085 "Адмирал Нахимов" (Admiral Nakhimov)*

(TK-210 + K-329)

Rango 8 (Almirante)

Defensa Integral de Sistemas

CISOs de perfil técnico + formación integral en ramas técnicas

TBA. B-*41 "Sigillum Regiae Universitatis Ovetensis" (SRUO)*

(D-73 + F-113 + L-62)

Técnicas, Tácticas y Procedimientos de Explotación y Post-Explotación a Máquinas y Usuarios

Seguridad ofensiva: Recorrido completo del MITRE ATT&CK + OSINT Framework

TBA, B-51 *"Rex Pelagius"*

(RK-085 + A-21)

Rango 9 (Almirante General)

Universidad de Oviedo

Módulos del curso

José Manuel
Redondo López

- 👥 **Aspectos Relativos a las Personas**: Los fallos humanos son la principal causa de problemas de seguridad en la actualidad
  - **Autenticación**: Protección de nuestras cuentas de usuario
  - **Computación "sensata"**: Desarrollo del sentido común
- 🌎 **Uso de Internet**: Simplemente usar Internet conlleva una gran cantidad de peligros que necesitan atención
  - **Usando el navegador de forma segura**: Navegar es una actividad de riesgo si no se hace correctamente
  - **Uso de redes sociales**: El mal uso de las mismas es un peligro, especialmente para la privacidad
- 🗣️ **Uso de Sistemas de Mensajería**
  - **Email**: Tradicional puerta de entrada de malware y otros problemas de seguridad
  - **Aplicaciones de mensajería**: Otra puerta de entrada de malware y problemas, cada vez más presente

Módulos del curso

José Manuel
Redondo López

- ⚙️ **Dispositivos de Computación**: Las máquinas también necesitan atención
  - **Telefonía Móvil**: Nuestros "ordenadores de bolsillo" necesitan protección dada su extensión en la población y capacidad de cómputo
  - **Ordenadores**: Necesitamos proteger nuestra herramienta de trabajo diaria
- 📡 **Redes y Dispositivos "Inteligentes"**
  - **Redes de comunicaciones**: En un mundo interconectado, proteger las máquinas debe ir acompañado de la protección de las comunicaciones entre ellas
  - **Dispositivos "Smart"**: Pequeños ordenadores en forma de dispositivos cotidianos interconectados entre ellos o con Internet, que también requieren atención
- 🏃 **Seguridad "En el Mundo Real"**
  - **Seguridad "Física":** No solo hay que proteger a los equipos "por dentro", sino también "por fuera"
    - Además de la **integridad física de las personas**
  - **Seguridad Financiera:** El objetivo de los ciberdelitos **siempre es económico**, directa o indirectamente
    - Esto requiere la mención de estrategias dirigidas a ello, que debemos prevenir

¿Cómo son los ejercicios prácticos?

José Manuel
Redondo López

- **Los ejercicios de este curso cuentan con los siguientes elementos**
  - **Código y enunciado** resumen de los objetivos
    - El código único es lo que se usa para **enlazar** teoría y práctica
  - **Infraestructura requerida** y (si es aplicable al curso) **puntuación** otorgada
  - **Descripción breve** del ejercicio
  - **Resultados esperados**: qué deberíamos obtener si realizamos el ejercicio correctamente
    - Incluye **posibles preguntas** que deben responderse para garantizar que se han entendido los conceptos
  - **Otra información complementaria**: Para hacerlo
    - Información de estudio y ayuda para complementar los conceptos de teoría asociados

Autenticación

Ejercicio AUTHA1_DETECT.FALSO_AVISO_LOGIN. Identifica falsos avisos que te piden que hagas login en una de tus cuentas pero en una página falsa

Infraestructura requerida	Un navegador cualquiera
Puntuación	

Descripción de la actividad

Consiste en aprender a detectar **si alguna vez has recibido un falso aviso** que te pide que metas tus datos te cuenta en una página que puede ser falsa

Resultados Esperados

Puedes contestar estas preguntas:

- *¿Alguna vez te ha llegado un aviso de este tipo?*
- *¿Cuál ha sido el principal motivo por el que ha sospechado del mismo?*
- *¿Has sido víctima de un timo de esta clase o conoces a alguien que lo fuera, y puedes determinar por qué acabó creyéndose el engaño?*

Otra información necesaria para su realización

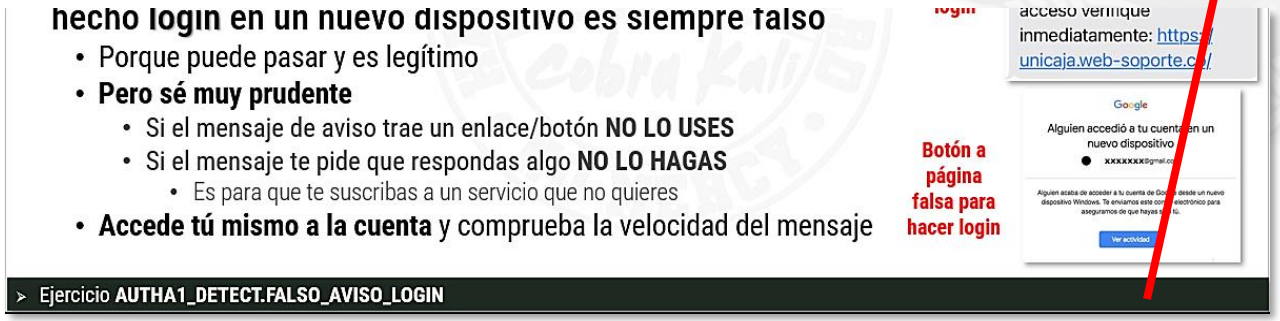
Este tipo de fraude donde recibimos avisos que normalmente requieren que hagamos clic en un enlace o bien que contestemos a un mensaje **son cada vez más frecuentes** y, por tanto, tenemos que ser conscientes de que lo más probable es que **nos va a llegar uno tarde o temprano**, y tendremos que reaccionar adecuadamente para no ser víctimas.

Lo importante es darse cuenta de que ningún mensaje legítimo de una compañía que realmente se preocupe por la seguridad **va a llevar jamás un enlace en el que debas hacer clic**. Los mensajes auténticos te van a pedir que entres en la banca online (o en el servicio correspondiente al mensaje) tú mismo, **navegando manualmente como lo haces de forma habitual,** pero **nunca van a tener un enlace para que hagas clic en él**. De tenerlo, el proveedor del servicio estaría cometiendo una temeridad puesto que el número de mensajes de este tipo con enlaces fraudulentos es altísimo, y por tanto un servicio legítimo nunca debería copiar el aspecto de uno de ellos. Me atrevo a decirte que si te encuentras con algo así algún día, te pienses si seguir con él, porque no es indicio de que se tomen la seguridad muy en serio. Esto es un aviso falso de este tipo, complementando los vistos en teoría:

¿CÓMO SON LOS EJERCICIOS PRÁCTICOS?

José Manuel
Redondo López

- **Todos los ejercicios están vinculados con algún concepto de teoría por su código único**
  - Así puedes hacer el/los ejercicios que refuerzan ese concepto de teoría directamente
  - ¡Teoría y prácticas siempre están enlazadas!
  - No todas las transparencias de teoría requieren ejercicios para su comprensión



Autenticación

Ejercicio AUTHA1_DETECT.FALSO_AVISO_LOGIN. Identifica falsos avisos que te piden que hagas login en una de tus cuentas pero en una página falsa

Infraestructura requerida	Un navegador cualquiera
Puntuación	

Descripción de la actividad

Consiste en aprender a detectar **si alguna vez has recibido un falso aviso** que te pide que metas tus datos te cuenta en una página que puede ser falsa

Resultados Esperados

Puedes contestar estas preguntas:

- *¿Alguna vez te ha llegado un aviso de este tipo?*
- *¿Cuál ha sido el principal motivo por el que ha sospechado del mismo?*
- *¿Has sido víctima de un timo de esta clase o conoces a alguien que lo fuera, y puedes determinar por qué acabó creyéndose el engaño?*

Otra información necesaria para su realización

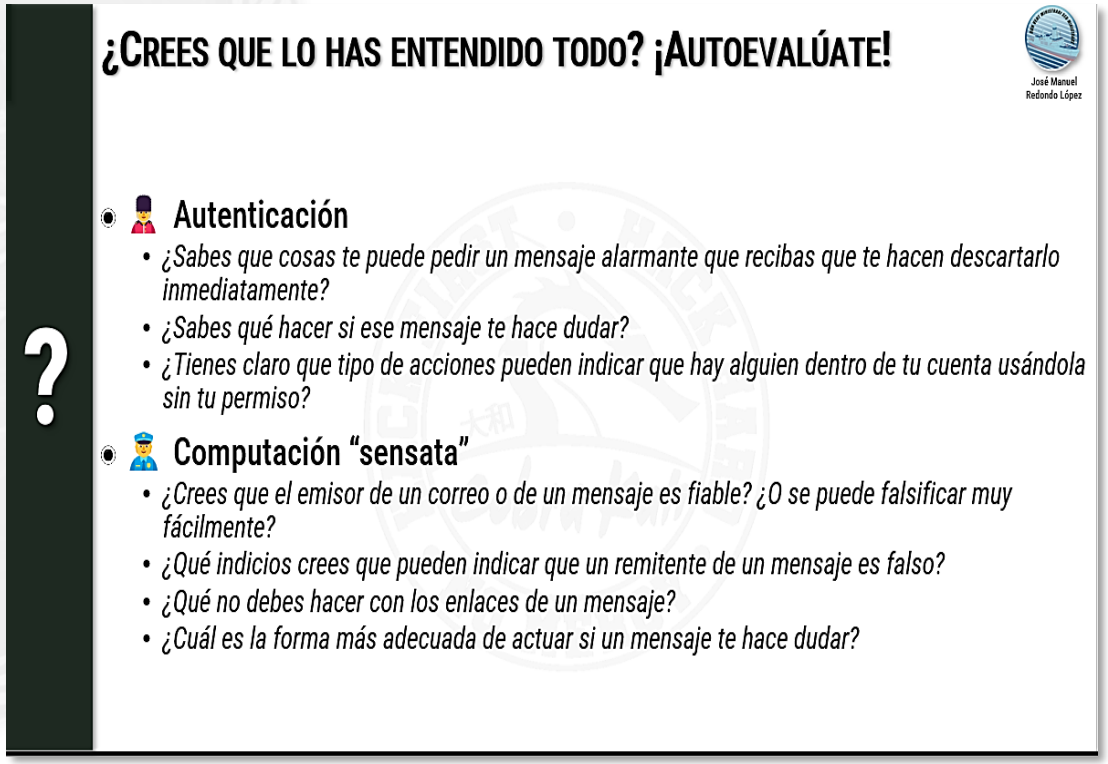
Este tipo de fraude donde recibimos avisos que normalmente requieren que hagamos clic en un enlace o bien que contestemos a un mensaje **son cada vez más frecuentes** y, por tanto, tenemos que ser conscientes de que lo más probable es que **nos va a llegar uno tarde o temprano**, y tendremos que reaccionar adecuadamente para no ser víctimas.

Lo importante es darse cuenta de que ningún mensaje legítimo de una compañía que realmente se preocupe por la seguridad **va a llevar jamás un enlace en el que debas hacer clic**. Los mensajes auténticos te van a pedir que entres en la banca online (o en el servicio correspondiente al mensaje) tú mismo, **navegando manualmente como lo haces de forma habitual,** pero **nunca van a tener un enlace para que hagas clic en él**. De tenerlo, el proveedor del servicio estaría cometiendo una temeridad puesto que el número de mensajes de este tipo con enlaces fraudulentos es altísimo, y por tanto un servicio legítimo nunca debería copiar el aspecto de uno de ellos. Me atrevo a decirte que si te encuentras con algo así algún día, te pienses si seguir con él, porque no es indicio de que se tomen la seguridad muy en serio. Esto es un aviso falso de este tipo, complementando los vistos en teoría:

ELEMENTOS COMUNES DE TEORÍA

José Manuel
Redondo López

- **Cada uno de los seis módulos de los 5 bloques de la teoría de este curso tiene algo para ayudarte a seguirlo**
  - **Es una transparencia de "autoevaluación"**
  - Con un conjunto de preguntas que puedes hacerte para saber si has entendido correctamente los contenidos de dicho módulo
  - Es la forma de no avanzar (si no quieres) hasta estar seguro de que has entendido cada parte
  - Hace el curso muy modular y **facilita el aprendizaje** autónomo al ritmo de cada uno



¿QUIERES APRENDER A TENER CIBER-SUPERPODERES?

PRESENTACIÓN