ACCIÓN FORMATIVA: CLAVE: 03 (07)-EXT/2024 "COMERCIO ELECTRÓNICO Y CIBERSEGURIDAD"

Cronograma lista de tareas y prácticas para el Curso de Comercio Electrónico y Ciberseguridad

2. Cronograma

Tema I. Introducción a la ciberseguridad

Tema II. Protección de datos personales y privacidad

Este tema abarca el análisis de la información que recogen los navegadores y cómo proteger los datos personales de los usuarios.

- Tarea 1: **Análisis de la información recopilada por navegadores (Webkay – Cover Your Tracks).** Aquí se analiza qué información recopilan las webs sobre los usuarios al navegar con Google Chrome en modo normal y en modo incógnito**,** utilizando herramientas como Webkay y Cover Your Tracks. El objetivo es comparar si ambos modos permiten a las páginas obtener detalles como sistema operativo, ubicación o características del dispositivo, y evaluar si el modo incógnito realmente mejora la privacidad del usuario frente a estos rastreos.
  - Recursos web:
    - Webkay
    - Cover Your Tracks
- Tarea 2: **Análisis las cookies que tiene una página web**. Se estudian las cookies que un sitio web almacena en el navegador del usuario, identificando su propósito y cómo afectan la privacidad, utilizando herramientas como CookieYes.
  - Recursos web:
    - CookieYes
- Tarea 3: **Análisis de la IP pública.** Consiste en verificar si la dirección IP pública es visible al navegar con Google Chrome tanto en modo estándar como en modo incógnito, usando herramientas como "Cuál es mi IP". Se analiza si el modo incógnito afecta la exposición de la IP.
  - Recursos web:
    - Cuál es mi IP
- Tarea 4: **Vamos a engañar a los navegadores y las webs (Extensión de navegador User-Agent Switcher and Manager).** Se utilizará una extensión de navegador para modificar el "User-Agent" del navegador, simulando diferentes dispositivos o navegadores. El objetivo es observar cómo responden las páginas web a estos cambios y cómo se puede reducir la exposición de la huella digital del usuario, limitando la cantidad de información que los sitios pueden recopilar sobre el navegador y dispositivo utilizado, mejorando así la privacidad del usuario. – **Video grabado**
  - Recursos web:
    - Webkay

- **Tarea 5: Ocultar nuestra IP pública a los navegadores y las webs (ProtonVPN** - Proton). Se enseña cómo utilizar una VPN para ocultar la IP pública, evitando que los sitios web y servicios en línea puedan rastrear la ubicación real del usuario, protegiendo su identidad y mejorando significativamente la privacidad. - **Video grabado**
    - Recursos web:
        - Cuál es mi IP
- **Tarea 6: Login con cuenta google en aplicación de tercero**. Los alumnos explorarán los riesgos asociados con el uso de la opción de iniciar sesión con una cuenta de Google en aplicaciones de terceros, como la recolección excesiva de datos personales por parte de las aplicaciones, que obtienen acceso a la cuenta de Google o redes sociales. - **Video grabado**
    - Recursos web:
        - pngtree

PRÁTICAS DÍA 1.

- **Práctica 1: Crear contraseñas seguras y protección datos personales con Protón Pass.** Se verá cómo utilizar un gestor de contraseñas. para generar y gestionar contraseñas seguras, aprendiendo la importancia de crear contraseñas robustas para proteger la información personal. Además, explorarán cómo crear alias de correo electrónico**,** lo que les permite proteger su dirección de correo principal al usar un alias en diferentes servicios, mejorando la privacidad. También se destacarán los beneficios de utilizar un gestor de contraseñas, como manera de almacenar credenciales de manera segura, evitar el uso de contraseñas repetidas y facilitar el acceso a cuentas sin comprometer la seguridad.- **Video grabado**
    - Recursos web:
        - Proton
        - PC Componentes
        - MediaMarkt
        - Generador DNI
- **Práctica 2: Cifrado de documentación con Cryptomator**. Los alumnos aprenderán a cifrar documentos y carpetas utilizando Cryptomator, comenzando por los archivos presentes en el escritorio del ordenador para asegurar que solo personas autorizadas puedan acceder a ellos. Luego, se enseñará cómo subir estos archivos cifrados a servicios de almacenamiento en la nube, garantizando su protección incluso fuera del dispositivo local. Además, los alumnos aprenderán a descargar los archivos cifrados desde la nube y a desencriptarlos nuevamente en el escritorio. También se cubrirá cómo cifrar unidades USB con Cryptomator, ofreciendo una capa adicional de seguridad para datos portátiles y transferibles. - **Video grabado**
    - Recursos web:
        - Cryptomator
- **Practica 3: Correo electrónico Gmail cifrado.** Los alumnos aprenderán a utilizar el modo confidencial de Gmail para enviar correos electrónicos de forma más segura. Este modo permite establecer fechas de caducidad para los mensajes, evitando que el destinatario los reenvíe, copie o descargue, y añade una capa adicional de protección mediante la opción de exigir un código de acceso enviado por SMS para abrir el correo. Esto garantiza que las comunicaciones sean más privadas y seguras, limitando el acceso no autorizado. - **Video grabado**
    - Recursos web:
        - Gmail

- **Practica 4: USB perdido** – Se va a simular el escenario de un USB perdido, utilizando **Canary Tokens**, una herramienta que permite insertar un token trampa en archivos de Word y Excel. Estos archivos actúan como señuelos y, cuando alguien los abre, se activa el token, enviando una alerta que incluye información como la **IP pública de la red** donde se abrió. Esta práctica muestra los peligros de insertar un USB desconocido en un ordenador, ilustrando cómo los atacantes pueden aprovechar este método para comprometer la seguridad de un sistema y rastrear información sensible.
    - Recursos web:
        - Canary Tokens

Tema III: Identificación y mitigación de amenazas comunes

- **Tarea 1: Identifica vulnerabilidades (V) y amenazas (A).** Se entregará a los alumnos un documento en el que se describen diferentes situaciones relacionadas con la ciberseguridad. Cada situación representará un ejemplo de vulnerabilidad (V) o amenaza (A)**,** y los estudiantes deberán analizar cada caso y decidir si se trata de una vulnerabilidad en el sistema o una amenaza externa. Esta actividad fomenta el entendimiento práctico de cómo identificar y diferenciar entre los riesgos inherentes a los sistemas y los ataques potenciales. – **Tarea formato papel**
- **Tarea 2: Identificar casos de Typosquatting.** Los alumnos analizarán diferentes dominios de sitios web para identificar posibles casos de typosquatting**,** una técnica en la que los atacantes registran dominios similares a los legítimos, pero con ligeras variaciones tipográficas, evaluando cómo estas variaciones pueden ser utilizadas para engañar a los usuarios, y cómo este tipo de ataques representa un riesgo para la seguridad en línea.
    - Recursos web:
        - apple.com / appple.com
        - google.com / gooogle.com
        - bancosantander.es / banco-santander.es
        - juntaex.es / juntaeex.es
        - saludextremadura.ses.es / salud-extremadura.es

- **Tarea 3: Técnica de homoglifos** (**juntaex – saludextremadura**). Los alumnos explorarán la técnica de homoglifos**,** que consiste en usar caracteres visualmente similares pero diferentes en el código, para crear dominios fraudulentos que parezcan legítimos.
    - Recursos web:
        - irongeek – homogluph-attack-generator

Tema IV: Uso seguro de dispositivos y redes

- **Tarea 1: Búsqueda de dispositivos IoT conectados a internet.** los estudiantes utilizarán **Shodan**, un motor de búsqueda especializado en dispositivos conectados a internet, para localizar dispositivos IoT (Internet de las Cosas) accesibles. A través de comandos específicos, se identificarán dispositivos como impresoras, cámaras, servidores médicos, y bases de datos expuestas en España - **Video grabado**
    - Recursos web:
        - Shodan
        - Insecam

Tema V: Introducción a la seguridad en el comercio electrónico (E-Commerce)

- **Tarea 1: Diseño de un ataque de Spear Phishing**. Los alumnos se enfrentarán a un caso simulado en el que deberán diseñar un ataque de Spear Phishing dirigido a un objetivo específico. Utilizando información proporcionada en el caso, debatirán y colaborarán para personalizar un ataque de Spear Phishing que resulte convincente. El ejercicio permitirá a los alumnos comprender cómo los atacantes diseñan estos ataques y la importancia de identificar señales de alerta para prevenir este tipo de ataques.
- **Simulacro en directo** – **Ataque de vishing – La falsa llamada del SES**. Se explicará cómo realizar un ataque de vishing (phishing por voz) utilizando servicios de spoofing telefónico. Durante la demostración, se simulará como se realizaría un ataque de vishing a partir de una falsa llamada del Servicio Extremeño de Salud (SES) en la que se suplantará la identidad de la institución para obtener información sensible de la víctima.
    - Recursos web:
        - SpoofCard
- **Vídeo de ataque de fuerza bruta sobre una máquina vulnerable.** Los estudiantes verán un vídeo demostrativo sobre cómo se realiza un ataque de fuerza bruta contra una máquina vulnerable. En el vídeo, se mostrará cómo un atacante prueba sistemáticamente combinaciones de contraseñas hasta encontrar la correcta, explotando la debilidad de una contraseña poco robusta o de fácil adivinación.
    - Recursos:
        - YouTube - Ataque de fuerza bruta

Tema VI: Protección de datos en el comercio electrónico

- **Tarea 1: Derecho al olvido - Desindexación de datos en Google**. Los alumnos aprenderán a ejercer el derecho al olvido mediante el proceso de desindexación de datos personales en Google. Utilizando el Formulario de derecho al olvido de Google, explorarán cómo solicitar la eliminación de información personal de los resultados de búsqueda, los pasos necesarios para proteger su privacidad en línea, eliminando datos que puedan afectar su reputación o seguridad personal de los motores de búsqueda.
    - Recursos web:
        - Formulario de derecho al olvido de Google
- **Tarea Alternativa**: Lista Robinson. Los alumnos aprenderán a utilizar la Lista Robinson**,** un servicio diseñado para que las personas puedan evitar recibir publicidad no deseada de empresas con las que no han tenido contacto previo. Durante la actividad, los alumnos explorarán cómo inscribirse en la lista para bloquear llamadas telefónicas, correos electrónicos, SMS y correos postales publicitarios, entendiendo así cómo funciona este mecanismo para proteger su privacidad y controlar el uso de sus datos personales con fines comerciales.
    - Recursos web:
        - Lista Robinson

PRÁTICAS DÍA 2.

- **Práctica 1: Phishing a las tiendas de correo electrónico Amazon y Ebay**. Los alumnos visualizarán un video grabado en el que se utilizan herramientas de hacking ético para realizar ataques simulados de **phishing**, suplantando páginas de comercio electrónico. El video mostrará cómo los atacantes crean versiones falsas de estas páginas web, diseñadas para engañar a los usuarios y obtener sus credenciales. A través de esta simulación, los alumnos comprenderán cómo se llevan a cabo estos ataques, cómo funcionan las técnicas de suplantación de sitios web y la importancia de estar alerta ante correos electrónicos sospechosos y enlaces fraudulentos. - **Video grabado**
- **Práctica 2: Caso Práctico sobre protección de datos. Encuesta de hábitos de compra**. Los alumnos realizarán un caso práctico sobre protección de datos, enfocado en el análisis de riesgos de una encuesta de hábitos de compra proporcionada por INCOEX. A través de una tarea en formato papel, los alumnos revisarán las diferentes fases del análisis de riesgos, que incluyen la identificación de los datos sensibles recogidos en la encuesta, la evaluación de las posibles amenazas, las vulnerabilidades presentes y las medidas de mitigación necesarias para proteger la información. Esta práctica les permitirá comprender cómo se evalúan y gestionan los riesgos en el tratamiento de datos personales - **Tarea formato papel**

Tema VII: Pagos seguros en el comercio electrónico

- **Tarea 1: Análisis de la información legal de una tienda online.** Los alumnos se centrarán en analizar el apartado del aviso legal de la tienda online. Revisarán el contenido de este apartado para identificar información relevante sobre la titularidad del sitio, derechos de propiedad intelectual, limitaciones de responsabilidad y cumplimiento de las normativas legales. Esta tarea tiene como objetivo enseñar a los alumnos a evaluar si el aviso legal de un sitio web cumple con los requisitos necesarios para garantizar la transparencia y la protección de los usuarios.
    - Recursos web:
        - La Suite Perfumería
- **Tarea 2: Análisis de la información sobre cookies en una tienda online.** Los alumnos realizarán un análisis de la política de cookies de una tienda online. Revisarán cómo se presenta la información sobre las cookies utilizadas, su propósito (técnicas, analíticas, publicitarias, etc.), y si se proporciona al usuario la opción de gestionar o rechazar el uso de estas cookies. El objetivo de esta tarea es que los alumnos comprendan la importancia de que las tiendas online cumplan con las normativas de privacidad y protección de datos, asegurando la transparencia en el uso de cookies y garantizando el control del usuario sobre su privacidad.
    - Recursos web:
        - Futunatura
- **Tarea 3: Análisis de los datos de registro del dominio (pc componentes).** Los alumnos realizarán un análisis de los datos de registro del dominio de una tienda online a través de diversas herramientas. Examinarán la información del dominio, como el nombre del registrante, la organización propietaria, fechas de creación y expiración del dominio, y los servidores DNS asociados. Esta tarea tiene como objetivo enseñar a los alumnos cómo verificar la legitimidad de un sitio web y su dominio, analizando los datos de registro para detectar posibles fraudes o actividades sospechosas.
    - Recursos web:

        - ICANN WHOIS
        - Registros WHOIS
        - Who.is
- **Tarea 4: Análisis de la información de registro SSL** (La Suite Perfumería - phrack). Los alumnos realizarán un análisis del certificado SSL de una tienda online, utilizando diversas herramientas. Evaluarán la validez del certificado, su nivel de cifrado, la entidad emisora, y si cumple con los estándares de seguridad actuales. Esta tarea tiene como objetivo enseñar a los alumnos a verificar la seguridad de las conexiones HTTPS, asegurándose de que los datos transmitidos entre el usuario y el sitio web estén cifrados y protegidos frente a interceptaciones. Además, aprenderán a identificar posibles debilidades en la implementación del SSL que puedan comprometer la seguridad.
    - Recursos web:
        - SSL Labs
- **Vídeo sobre identificación de fraudes en tiendas online.** Los alumnos visualizarán un vídeo educativo sobre la identificación de fraudes en tiendas online. El vídeo explicará cómo detectar señales de advertencia en sitios de comercio electrónico fraudulentos, como la falta de información legal, precios extremadamente bajos, o políticas de devolución sospechosas. A través de ejemplos prácticos, los estudiantes aprenderán a evaluar la legitimidad de una tienda online, aplicando técnicas de análisis de dominio, certificados SSL, y políticas de cookies para evitar caer en estafas o fraudes en sus compras por internet.
    - Recursos:
        - YouTube - Cómo detectar fraudes en tiendas online

Tema VIII: Implementación de seguridad en tiendas online

Aunque este tema es clave para la seguridad en el comercio electrónico, se presenta principalmente como contenido teórico, explicando las mejores prácticas para implementar medidas de seguridad en tiendas online.

3. Instalación Previa de Extensiones de Navegador

Antes de iniciar la actividad formativa, los técnicos informáticos deben instalar las siguientes extensiones de navegador en los equipos de los participantes. Estas herramientas serán esenciales durante las sesiones prácticas del curso, especialmente en temas relacionados con la protección de la privacidad y la seguridad en el uso de navegadores web:

Extensiones Chrome (Brave): https://chromewebstore.google.com/?hl=es
Addons Firefox: https://addons.mozilla.org/en-US/firefox/

- **ProtonPass:** Gestión segura de contraseñas, para fomentar el uso de credenciales robustas.
- **Privacy Badger:** Bloqueo de rastreadores de terceros para evitar el seguimiento de usuarios.
- **I don’t care about cookies:** Facilita la navegación al eliminar ventanas emergentes relacionadas con cookies.
- **Cookie AutoDelete:** Elimina automáticamente las cookies una vez que se cierra una pestaña, mejorando la privacidad.

- **User-Agent Switcher and Manager:** Permite cambiar el "user-agent" que envía el navegador, útil para pruebas de seguridad.
- **Wappalyzer:** Identifica las tecnologías utilizadas por los sitios web, como CMS, plataformas de e-commerce y otros servicios.

4. Recursos Web Genéricos

Además de las herramientas anteriores, durante el desarrollo del curso se utilizarán los siguientes recursos web, que serán de utilidad tanto en la fase teórica como en las prácticas:

- **IPDeny:** Lista de bloqueos de IP, para controlar el acceso a través de listas negras de direcciones IP.
- **Quad9:** Servicios de DNS seguros, que ayudan a proteger contra amenazas en línea bloqueando dominios maliciosos.
- **Fakeinet:** Detección de tiendas online fraudulentas, utilizado para identificar posibles fraudes en tiendas de comercio electrónico.
- **Protección de datos - LOPD:** Protección de datos y normativas, para acceder a listas de tiendas fraudulentas y normativa legal de protección de datos.
- **Lista Robinson:** El Servicio de Lista Robinson te permite, de forma fácil y gratuita, evitar publicidad de empresas a las que no hayas dado tu consentimiento para que te envíen publicidad. Funciona para publicidad por teléfono, correo postal, correo electrónico y SMS/MMS.
- **Notmyplate**: Evitar que las aplicaciones de estacionamiento expongan su ubicación