Práctica Pareja 1.3: Material de concienciación

Trabajo realizado por:

Samuel Romero de los Reyes
Ernesto Saquete Rios

Curso de especialización en:
CETI

Índice

1. Introducción

Hoy en día, Internet forma parte esencial de nuestra vida académica, laboral y personal. Usamos la red para estudiar, trabajar, comunicarnos, comprar y entretenernos. Sin embargo, este entorno tan útil también es un espacio donde existen riesgos constantes: desde malware hasta estafas diseñadas para engañar incluso a usuarios experimentados.
Por eso, entender cómo navegar de forma segura no es opcional, sino una necesidad.

El objetivo de esta presentación es proporcionar pautas prácticas y aplicables para estudiantes, profesores y cualquier persona que use Internet a diario. No se trata solo de conocer amenazas, sino de aprender a detectarlas y prevenirlas con hábitos simples y herramientas adecuadas.

2. Principales riesgos en Internet

Cuando hablamos de seguridad en Internet, lo primero es identificar las amenazas más comunes:

2.1. Phishing

El phishing consiste en correos electrónicos, mensajes o páginas web falsificadas que intentan hacerse pasar por empresas reales para robar tus datos: contraseñas, números de tarjeta o información personal. A menudo generan urgencia, como “tu cuenta será cerrada en 24 horas”.

2.2. Malware

Es cualquier software malicioso diseñado para dañar o tomar el control de tu dispositivo. Incluye virus que se replican, troyanos que se ocultan como programas legítimos, y ransomware que cifra tus archivos y pide un rescate. Basta con abrir un archivo infectado o visitar una página comprometida.

2.3. Robo de identidad

Consiste en utilizar tus datos personales sin permiso para realizar compras, abrir cuentas o cometer fraudes. Normalmente ocurre cuando alguien obtiene información como tu DNI, correo, contraseñas o datos bancarios.

2.4. Estafas online

Desde tiendas falsas hasta falsos premios o supuestas inversiones milagro. Estas estafas aprovechan la confianza del usuario para obtener dinero o información. Cada año miles de personas caen en este tipo de fraudes.

2.5. Redes Wi-Fi inseguras

Las conexiones públicas o mal configuradas pueden permitir que un atacante intercepte tu tráfico, capture contraseñas o realice ataques “Man in the Middle” (MITM).

3. Señales de alerta

Una parte fundamental de la seguridad es detectar comportamientos sospechosos. Algunas señales típicas son:

- Enlaces con direcciones extrañas o con nombres que imitan sitios legítimos
- Correos que generan urgencia y piden datos personales, contraseñas o pagos
- Páginas sin HTTPS, lo cual indica que la conexión no está cifrada
- Pop-ups inesperados que dicen que tu dispositivo está infectado o te ofrecen premios
- Ofertas demasiado buenas para ser reales, que normalmente son un gancho para obtener información o dinero

Reconocer estas señales temprano evita la mayoría de incidentes.

4. Buenas prácticas para una navegación segura

4.1. Señales básicas

- Verificar siempre el remitente del correo: no basta con ver el nombre, hay que revisar la dirección real
- No abrir archivos adjuntos sospechosos o de personas que no conoces
- Comprobar la URL antes de introducir tus credenciales, especialmente en páginas de bancos, correo o redes sociales
- Evitar descargar software de páginas no oficiales, ya que es un método muy común para distribuir malware

4.2. Protección del navegador

El navegador es la puerta principal a Internet, por lo que debe estar bien configurado:

- Mantener navegador y extensiones actualizados evita vulnerabilidades
- Usar bloqueadores de anuncios y rastreadores, como uBlock Origin o Privacy Badger, reduce riesgos de páginas maliciosas
- Deshabilitar extensiones que no utilices, porque cada extensión es un posible punto débil
- Aceptar únicamente cookies necesarias y evitar las de seguimiento, que afectan a tu privacidad

5. Contraseñas y autenticación

Este apartado es clave. La mayoría de ataques exitosos ocurren por contraseñas débiles o reutilizadas:

- Usa contraseñas largas, únicas y robustas. Una frase larga es más segura y más fácil de recordar que un conjunto de caracteres aleatorios
- Siempre que sea posible, activa la autenticación en dos pasos (2FA). Incluso si un atacante obtiene tu contraseña, no podrá acceder a tu cuenta
- Para gestionar múltiples contraseñas de forma segura, utiliza un gestor de contraseñas como Bitwarden o Proton Pass. Generan claves fuertes y evitan que tengas que recordarlas todas

6. Redes Wi-Fi seguras

- Evita iniciar sesión en cuentas sensibles cuando estés en Wi-Fi públicas, como cafeterías o aeropuertos
- Si necesitas conectarte desde una red abierta, utiliza una VPN fiable, que cifra tu tráfico y dificulta su interceptación
- En casa, mantén tu router actualizado y cambia la contraseña por defecto
- Utiliza WPA3 (o al menos WPA2) como protocolo de seguridad para tu red doméstica

7. Redes sociales y privacidad

Las redes sociales son un entorno donde compartimos más información de la que imaginamos:

- Configura cuidadosamente la privacidad de tus perfiles para controlar quién puede ver tu información
- Evita publicar datos sensibles como el domicilio, horarios o documentos personales
- Revisa periódicamente los permisos de aplicaciones conectadas a tu cuenta (como juegos o apps de terceros), ya que muchas tienen acceso a datos innecesarios

8. Seguridad en dispositivos

Tu ordenador o móvil es el último eslabón de la cadena, y también el más importante:

- Mantén siempre el sistema operativo actualizado, ya que las actualizaciones corrigen vulnerabilidades
- Utiliza un antivirus o antimalware fiable, especialmente en Windows y Android
- Haz copias de seguridad regularmente para estar protegido frente a fallos del sistema o ataques de ransomware
- No instales aplicaciones desconocidas o con mala reputación, especialmente desde tiendas no oficiales

9. Conclusión

La seguridad en Internet no se basa en una única medida, sino en un conjunto de buenas prácticas, herramientas y hábitos conscientes. Cada decisión cuenta: usar una contraseña segura, evitar un enlace sospechoso, mantener el sistema actualizado, conectarse solo a redes fiables…
No se trata de vivir con miedo, sino de navegar con criterio y responsabilidad.

10. Preguntas

Con esto concluimos la presentación. Estoy disponible para resolver cualquier duda o profundizar en cualquiera de los puntos tratados.

Enlace de la presentación en Canva:

https://www.canva.com/design/DAG5ucOB1Us/fQFBfSXgRnM_BVLo1Z2f5A/view?utm_content=DAG5ucOB1Us&utm_campaign=designshare&utm_medium=link2&utm_source=uniquelinks&utlId=h8f253d5e46