ÁREA DE TECNOLOGÍA E INFORMÁTICA
TALLER

PROFESOR: JAVIER GÓMEZ R.

TEMA	TECNOLOGÍA Y SOCIEDAD
SUBTEMAS	Principales riesgos o peligros en Internet
OBJETIVO	Reforzar el nivel de conciencia de los estudiantes respecto al adecuado uso de los recursos de la Internet.
PROCESOS IMPLICADOS	• Observación, atención, búsqueda, análisis, síntesis, organización, comprensión y presentación adecuada de información. • Administración de tiempo

Nombre(s): samuela andres gomez gutierrez	Curso:1103	Fecha:05/03/2019

RECURSOS:

1. WEB: http://roble.pntic.mec.es/jprp0006/tecnologia/4eso_informatica/peligros_internet/0peligros_internet.htm
2. VIDEO: https://www.youtube.com/watch?v=sKPRxGXKEUE
3. WEB DEL PROFESOR: http://profejavier-g.blogspot.com/

1. USANDO EL RECURSO Nº 1, COMPLETE LA SIGUIENTE TABLA SÍNTESIS:

PELIGROS EN LA INTERNET			
MALWARE (¿Qué es?): El ***hardware*** es la parte física de un ordenador o sistema informático, está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables y circuitos de luz, placas, utensilios, cadenas y cualquier otro material, en estado físico, que sea necesario para hacer que el equipo funcione			
	DEFINICIÓN	QUÉ DAÑO REALIZA	OPINIÓN: ¿QUÉ PODRÍAS HACER PARA EVITARLO?
1. VIRUS	"Los virus son programas de ordenador como el Word o el Photoshop, pero en vez de estar diseñados para hacer algo útil han sido concebidos para dañar los sistemas informáticos en mayor o menor medida."	"se especializa en copiarse en un tipo determinado de archivos" "infectar las partes del disco duro que intervienen en el arranque del ordenador"	Siempre estar precavido en tanto a anuncios donde toca poner datos personales, siempre utilizar el software original
2. TROYANOS	"Se denomina troyano a un programa malicioso capaz de alojarse en computadoras y permitir	Este se especializa en el control de todo el ordenador, haciendo lo que se le ocurra con el sistema operativo	No instalar programas que no sean oficiales, ya que los troyanos se encuentran en aplicaciones de puquinas no oficiales

	el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.”		
3. GUSANOS	“Son programas "Malware" que suelen acompañar a un correo electrónico como archivo adjunto (aunque no siempre).”	Estos se especializan en copiar información y borrarlo o dañar totalmente el ordenador	Tener mucho cuidado en conectarme en sistemas en el cual desconfié(siempre se debe confirmar si es seguro)
4. SPYWARE	es un software que una vez introducido en el ordenador realiza un seguimiento de la información personal del usuario y la pasa a terceras entidades, generalmente con fines publicitarios.	Los daños no solo son a nivel hardware sino que también personalmente ya que esta transfiere información personal a personas que quieran hacer algún mal	“Ajuste las preferencias del browser para limitar el uso ventanas pop-up y cookies No de click en links dentro de ventanas de pop-up Elija "no" cuando sean hechas preguntas inesperadas Sea cuidadoso del software que "Gratis" que descarga No siga los links de email que dicen ofrecer software anti-spyware”
5. PHISHING	“Es una técnica que se basa en intentar engañar al usuario (ingeniería social), normalmente mediante un correo electrónico, diciéndole que pulse en un determinado enlace, para validar sus claves por tal motivo o tal otro.”	Los daños que ocasiona este virus no es en el hardware lo que hace es robar información si el usuario se deja engañar de los enunciados	Lo que se puede hacer es siempre confirmar cualquier anuncio que le llega a cuentas de correos y demás, ya que los maleantes utilizan este método para poder robarles a las personas
6. PHARMING	“es más peligroso que el phishing, ya que es más difícil de descubrir. Se basa en redirigirnos a la página falsa del banco diseñada por lo	Los daños que ocasiona este virus no es en el hardware lo que hace es robar información si el usuario se deja	Siempre debemos mirar primero lo que es una dirección IP, un dominio y un servidor DNS: para estar seguros de que la pagina sea autentica

	ladrones de forma automática, es decir, sin que nosotros necesitemos pulsar ningún enlace”	engañar de los enunciados	
7. SPAM	Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas)	“perjudican de alguna o varias maneras al receptor “	Para que no nos pase esto lo que siempre debemos hacer es asegurarnos de donde nos mandaron el mensaje y así corroborar que este no sea para algún maleante

2. USANDO LOS RECURSOS Nº 1 y 2, REALICE EN GOCONQR UN MAPA MENTAL QUE SINTEICE EL CONTENIDO DEL VIDEO Y DE LA TABLA.

Esté atento a las explicaciones del profesor sobre cómo se hace un mapa mental en GoConqr.

Condiciones para el mapa:

- El mapa debe incluir imágenes
- La estructura debe tener
    - Tema principal en el centro: “Riesgos o peligros en la Internet”
    - Cuatro (4) temas secundarios:
        1. “Relacionados con el Malware”
        2. “Relacionados con el uso de la INFORMACIÓN”
        3. “Relacionados con la COMUNICACIÓN INTERPERSONAL”

        y

4. “Relacionados con la REPERCUSIÓN ECONÓMICA”

** *Cada uno de los temas secundarios debe tener sus correspondientes ramas temáticas según lo observado en los recursos proporcionados*

Terminado el mapa mental, realice el proceso para copiar la URL o dirección de internet del recurso y péguela en el siguiente cuadro:

URL O DIRECCIÓN WEB DEL RECURSO	https://www.goconqr.com/es-ES/p/17135309-peligros-de-la-internet-mind_maps