**Prevención y seguridad en el internet y telecomunicaciones**

1 hora máxima de sesión.

***Pensar en cómo dividir la sesión para que no sea aburrida y sea muy didáctica.***

Durante la presentación usaremos PollEverywhere, para saber la opinión del grupo.

**Instalaciones:**

**Software Legal:** Por lo general el software comprado está libre de problemas.

**Actualizar sistemas:** Ningún sistema es perfecto, muchos sistemas van mejorando y quitando errores con actualizaciones, los crackers al encontrar una debilidad en los sistemas pueden tener acceso a diferentes tipos de información o hasta tomar el control completo de sus dispositivos, por lo que es bueno mantener la última actualización para evitar esto.

**Instalar Antivirus:** No se necesita pagar un antivirus muy caro, existen varias opciones gratuitas que nos pueden ayudar, es importante estar revisando constantemente nuestros equipos y sobre todo los nuevos que bajamos de internet ya que estos podrían tener un virus oculto y afectarnos.

**Instalar un Firewall o Cortafuegos:** Nuestros equipos todo el tiempo se están conectando a diferentes servidores o redes, por lo que es bueno tener una protección en esto ya que es una manera en la que los crackers pueden ingresar a nuestra computadora.

**Software Anti-Spyware:** Normalmente los crackers desarrollan aplicaciones para robar información, por lo que podrían robarse desde archivos, mirar nuestra cámara o saber todo lo que hemos tecleado y de aquí sacar nuestros datos personales.

**Navegación Segura:** Identificar los sellos o certificados que garanticen la seguridad de la página. Sobre todo a la hora de hacer compras por internet, al ingresar datos personales o confidenciales, tener cuidado con los anuncios (Usar software contra estos adblocker)

* En el navegador debe de empezar con https:// y tener un candado cerrado.
* Tener cuidado con los estafadores en la compra en línea, ¿cómo comprar en línea?.

**Contraseñas Seguras:** Utilizar contraseñas compuestas por 8 caracteres mínimo y combinar letras, números y símbolos. Es conveniente cambiar la contraseña con frecuencia. Sobre todo las de cuentas que llegamos a abrir en equipos ajenos o redes públicas.

**Protección de Correo:**

* No abrir mensajes de correos desconocidos o spam, proteger su cuenta con algún software Anti-Spam.
* Desconfiar de e-mails de bancos, subastas o sitios de venta, sobre todo si piden contraseñas, información confidencial, etc.

**Ciber Bullying y Phishing:** Cuentas falsas de facebook, un buen método de detección es pedirle que use su cámara web o buscar sus fotos en google ***(A los padres les interesa la seguridad de sus hijos, investigar más temas interesantes).***

**Cosas que no tienes que hacer con un celular:** Estafas por Teléfono,Robo de Información, Bancos Falsos y casos como WhatsApp Gold.

**Usar Motores de Búsqueda:** Cualquier cosa esta en google, por lo que si en algún momento necesitas ayuda en algo o dudas de algo, puedes googlear tu problema.

**Actividades:**

* Hacer una página web bancaria falsa o de facebook y pedirle a los participantes que ingresen, después enseñarles cómo se pueden robar datos.
* Hacer una cuenta falsa de facebook y enseñarles cómo la pueden identificar y qué es lo que deben hacer.
* ***Pensar en más actividades.***

**Bibliografía:**

<https://www.osi.es/es/actualizaciones-de-seguridad>

**Entregables:**

* Una guía/revista de supervivencia al internet (Con una versión digital).

**Estilo de la Presentación:**

* Mantener un Estilo Moderno y Tecnológico, el diseño tiene que ir junto con la presentación.