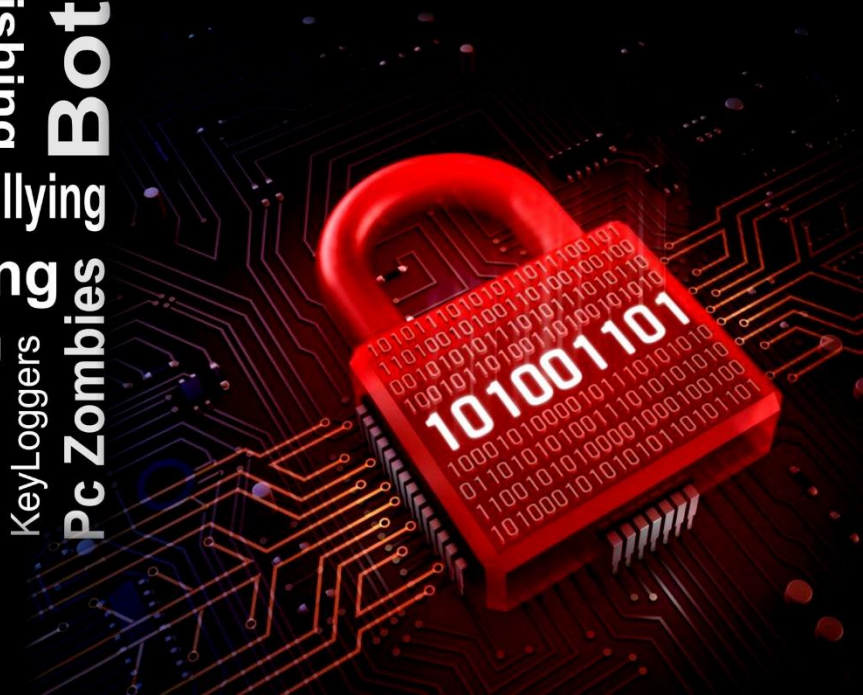
SECURACTIVA

JORNADAS CIBERSEGURIDAD

malware
virus
spam
BotNet
Firewalls
Phishing
Bitcoin
ciberdelincuente
Deep Web
Grooming
Snifers
Ciberbullying
Tecnoadicciones
Sexting
Pc Zombies
Social Media
Pentesting
hacking
Pharming
KeyLoggers
WIFI
Https
Security



Junta de Castilla y León

Curso de formación:

“Peligros y situaciones no deseadas en Internet”

Securactiva

Presentación del promotor

Desde hace varios años en Securactiva Noreste, como empresa proveedora de servicios TIC, venimos detectando que en la era digital en la que nos movemos existe una gran necesidad de conocimiento sobre el uso y protección de la información personal y profesional.

Por ello nos hemos volcado fomentando el acercamiento y concienciación de la Ciberseguridad y Seguridad de la información a colectivos, empresas, agrupaciones y público objetivo con el fin de distribuir dicho conocimiento mediante publicaciones, portales, encuentros presenciales y eventos en materia de Ciberseguridad.

Securactiva

Bulevar Juan Carlos I, 6
24404 Ponferrada (León)

Tlf: 987 40 86 49

E-mail: info@securactiva.com
Web: www.securactiva.com

AGENDA DEL CURSO

- Día 1
  - Introducción a la seguridad en Internet
    - Por qué es importante y especialmente con los menores
  - La seguridad del medio de conexión
    - De qué forma nos conectamos y en qué lugar. ¿Somos nosotros los dueños de la red?
    - Riesgos de las conexiones WiFi
  - Seguridad en el sistema operativo
    - Gestión de cuentas de usuario: Que el tutor sea el administrador y no el menor
  - Seguridad al descargar contenidos desde Internet
  - Configuración del navegador para mejorar la seguridad
  - Medidas de prevención frente a virus y programas no deseados

AGENDA DEL CURSO

- Día 2
  - Verificación de contenidos: Cómo distinguir información falsa en la red
  - Suplantación de identidad
  - Robo de información personal:
    - Cuentas bancarias
    - Cuentas de correo
    - Redes sociales
  - Gestión de la privacidad al navegar por Internet
    - Cookies y elementos de recopilación de hábitos
    - Herramientas anti rastreo: Ghostery
    - Configuración de la privacidad en las redes sociales

AGENDA DEL CURSO

- Día 3
  - Importancia de los contenidos que publicamos en Internet
    - Publicaciones en redes sociales
    - Concienciación a los menores
  - Protección de los menores frente a contenido inadecuado
  - Acoso a los menores, tipos de chantajes y amenazas que reciben
    - Cyberbullying
    - Grooming
    - Sexting
  - Aspectos legales
    - Líneas de denuncia ante robo de datos
    - Tratamiento de datos personales

DÍA 1

ÍNDICE DÍA 1

- Día 1
  - Introducción a la seguridad en Internet
    - Por qué es importante y especialmente con los menores
  - La seguridad del medio de conexión
    - De qué forma nos conectamos y en qué lugar. ¿Somos nosotros los dueños de la red?
    - Riesgos de las conexiones WiFi
  - Seguridad en el sistema operativo
    - Gestión de cuentas de usuario: Que el tutor sea el administrador y no el menor
  - Seguridad al descargar contenidos desde Internet
  - Configuración del navegador para mejorar la seguridad
  - Medidas de prevención frente a virus y programas no deseados

Introducción a la seguridad en Internet I

- **Definiciones de Seguridad Informática**

  1. Área de la informática que se enfoca en la protección de las infraestructuras computacionales y, especialmente, de la información contenida o circulante.
  2. Disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

- **¿Qué entendemos por seguridad en Internet?**

  Adoptar la actitud y las medidas necesarias para conocer los riesgos y prevenir las amenazas que pueden surgir durante el uso de Internet desde cualquier dispositivo.

Introducción a la seguridad en Internet II

- **¿Por qué es importante navegar seguros?**
  - Vivimos en un mundo con una interacción constante con Internet y con multitud de aparatos conectados a la red.
  - Debemos ser capaces de utilizarlos de manera que minimicemos el riesgo de sufrir cualquier daño o resultado no deseado, tomando para ello las medidas de protección adecuadas.
  - Tenemos que saber proteger nuestra vida digital: Información personal, cuentas de correo, cuentas de redes sociales, compras electrónicas, etc.
- **Protección de los menores**
  - Los padres, tutores y educadores tenemos la responsabilidad de proteger y concienciar especialmente a los menores de hacer un uso adecuado de Internet.
  - Los menores son menos conscientes de los riesgos que existen en Internet y son más vulnerables, y a menudo son víctimas de situaciones que les perjudican seriamente.

Seguridad del medio de conexión I

- **Aspectos a tener en cuenta**
  - ¿Dónde nos conectamos? ¿Somos nosotros los dueños de la red?
    - Lugares privados: En nuestra casa, en el trabajo.
    - Lugares públicos: En una cafetería, en un aeropuerto, en la estación de tren, en el instituto, en una biblioteca, en la universidad, etc.
  - ¿Cómo nos conectamos? Por cable, por red WiFi, por conexión de datos 3G/4G.
  - ¿Desde qué dispositivo nos conectamos? Ordenador, móvil, tablet, TV, …
- **Recomendaciones al usar una red pública, sea por cable o WiFi**
  - Si no nos garantizan nuestra privacidad al navegar o no estamos seguros, seremos precavidos.
  - No entraremos en cuentas personales de correo, ni del banco, ni en nuestras cuentas de redes sociales, ni en otros lugares donde tengamos que entrar con usuario y contraseña y tengamos información valiosa.

Seguridad del medio de conexión II

- **Advertencias y recomendaciones sobre las redes WiFi**

  Las redes WiFi nos permiten conectarnos a Internet sin cables y sin consumir datos de conexiones 3G/4G, lo cual tiene ventajas evidentes. Sin embargo estas redes pueden implicar un riesgo mayor que otro tipo de conexiones.

  - En las redes WiFi públicas, puede conectarse cualquier persona, ya que la contraseña es pública.
  - Es sencillo “espiar” y ver el contenido que están consultando los demás usuarios.
  - Si no configuramos correctamente la red WiFi de nuestra casa, otras personas pueden conectarse a ella y capturar lo que estemos viendo nosotros.
  - Aunque la red tenga contraseña, puede no ser garantía suficiente si el cifrado es débil.
  - Debemos configurar nuestra red con un cifrado “**WPA2**”, evitando siempre el cifrado antiguo “WEP” ya que tiene fallos y es fácil romperlo.
  - Debemos cambiar la contraseña que viene de fábrica con el router WiFi: Existen muchas listas y programas en Internet que proporcionan las contraseñas de fábrica.

Seguridad en el acceso al sistema operativo I

- **El usuario administrador**
  - Es importante separar el usuario administrador del sistema (que tiene privilegios para realizar cualquier tarea) del resto de usuarios.
  - En equipos que van a ser usados por menores es muy conveniente que el tutor sea el administrador y no el menor. De este modo el tutor tiene la responsabilidad de decidir qué programas instalar en el sistema y cuáles no.
- **El usuario estándar**
  - Se trata de un usuario al que se le permite hacer un uso personal del equipo pero que no tiene permisos para realizar cambios que afecten a todo el sistema, como instalar o eliminar programas, o modificar archivos que son necesarios para que el sistema funcione.
  - Para el usuario estándar, es más difícil infectarse con virus ya que no tiene permisos para instalar nuevo software.
  - En los entornos laborales es una práctica de seguridad muy común que los usuarios no tengan permisos de administrador, y que haya un departamento encargado de las tareas de administración.

Seguridad en el acceso al sistema operativo II

- **Ejercicio práctico**

  Gestión de cuentas de usuario en Windows: Creación de una cuenta de usuario estándar.

Los navegadores de Internet I

Un navegador es un software o programa informático que permite explorar Internet, visualizando el contenido de las páginas web que visitamos. Hoy día los navegadores son programas muy complejos que ofrecen multitud de capacidades al navegar por Internet. Por ejemplo: visualizar vídeo a pantalla completa, leer documentos PDF dentro del navegador, descargar todo tipo de archivos, explorar el código fuente de las páginas web, etc.

Además, los navegadores han evolucionado para permitir instalar extensiones y complementos (en inglés *plugins*) que aumentan las funciones originales. Hay miles de complementos gratuitos disponibles para los diferentes navegadores, ofreciendo al usuario la posibilidad de personalizar a su gusto su explorador de Internet.

- **Recomendaciones**
  - Mantener siempre actualizado el navegador, ya que en cada nueva versión se corrigen fallos de seguridad y se añaden mejoras.
  - Utilizar un navegador alternativo a Internet Explorer.

Los navegadores de Internet II

- **Ejercicio práctico**
  - Conocer e instalar navegadores alternativos a Internet Explorer.
  - Añadir plugins para mejorar la seguridad y la navegación:
    - Bloqueadores de publicidad: Adblock Plus o Adblock Edge.
    - Verificadores de seguridad de direcciones web: McAfee Site Advisor.

Amenazas software: algunas definiciones de la *fauna* existente I

- **Programas maliciosos**
  - **Malware**: Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza para expandirse herramientas de comunicación populares, como el email, la mensajería instantánea, y medios de almacenamiento extraíbles, como memorias USB. La mayoría del malware peligroso actual busca robar información personal valiosa.
  - **Virus**: Programa informático diseñado para alterar la forma normal en que funciona una computadora, sin permiso ni conocimiento del usuario. Los virus son capaces de reproducirse, bien copiándose en otros dispositivos o equipos, o bien auto-enviándose por email para expandirse.
  - **Troyano o caballo de Troya**: Tipo de código malicioso que parece ser algo que no es. Una distinción importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de Troya tienen códigos maliciosos que cuando se activan causan perdida o robo de datos. Por lo general, también tienen un componente de puerta trasera, que permite al atacante descargar amenazas adicionales en el equipo infectado.
  - **Spyware**: Software que realiza un seguimiento de la navegación del usuario del equipo y envía información de identificación personal o información confidencial a otras personas sin que el usuario se entere.
  - **Adware**: Software generalmente no deseado, que facilita el envío y aparición de contenido publicitario al equipo en el que se encuentra instalado.

Amenazas software: algunas definiciones de la *fauna* existente II

- ***"Discípulos"* producidos por infecciones**
  - **Bot**: computadora individual infectada con malware, la cual forma parte de una red de bots (*botnet*). El término bot proviene de robot, y hace referencia a que el ordenador es manejado a su antojo por otra persona. A un bot también se le suele llamar *ordenador zombie*.
  - **Botnet**: Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos se utilizan para actividades malintencionadas, como el envío de *spam* y ataques distribuidos de denegación de servicio (ataques a servidores web). Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet. Las botnets son conocidas también como *redes de zombies*.

Seguridad al descargar software desde Internet I

- **Recomendaciones**
  - Descargar los programas desde su página web oficial siempre que sea posible.
  - Existen multitud de páginas que “engañan” a los usuarios de diversas formas:
    - Ofreciendo programas diferentes a los que el usuario busca
    - Cobrando por programas gratuitos
    - Incluyendo software de publicidad intrusiva dentro del programa original
  - Si desconocemos la web oficial de un programa podemos buscar en sitios conocidos como la *Wikipedia*.
- **Medidas de prevención frente a virus y programas no deseados**
  - Antivirus (actualizarlo con mucha frecuencia).
  - Anti-spyware y anti-adware (actualizarlo con frecuencia).
  - Página web de VirusTotal.com.

Seguridad al descargar software desde Internet II

- **Ejercicio práctico I**
  - Comprobar lo fácil que resulta descargar un programa malicioso que no queremos.
  - Subir la muestra sospechosa descargada a la web de *VirusTotal* para analizarla con múltiples antivirus.
- **Ejercicio práctico II**
  - Descargar e instalar un antivirus.
  - Descargar e instalar un anti-spyware.
- **Ejercicio práctico III**
  - Conocer las ventajas de las máquinas virtuales frente a los programas maliciosos y la prevención contra desastres.
  - Instalar una máquina virtual y familiarizarse con su manejo.

Programas de interés

- **Antivirus de pago**
  - Panda Antivirus
  - McAfee Antivirus
  - Kaspersky Antivirus
  - Norton Antivirus
  - ESET Nod32.
- **Antivirus gratuitos**
  - AVG
  - Avast
- **Antivirus gratuitos**
  - Malwarebytes Antimalware

Preguntas tras el día 1

- **¿PREGUNTAS?**

- **¡Nos vemos en el próximo día!**

DÍA 2

ÍNDICE DÍA 2

- Día 2
  - Suplantación de identidad
  - Robo de información personal:
    - Cuentas bancarias
    - Cuentas de correo
    - Redes sociales
  - Gestión de la privacidad al navegar por Internet
    - Cookies y elementos de recopilación de hábitos
    - Herramientas anti rastreo: Ghostery

Verificación de contenidos

- **¿Qué es verdad y qué no en la información que existe en Internet?**

  No resulta fácil hoy en día distinguir la información falsa, incorrecta, o sesgada de la información real. Nos ocurre al consultar diferentes periódicos o ver noticias en televisión.

  En Internet la tarea de diferenciar la información correcta de la que no lo es resulta aún más compleja por la cantidad de contenidos que existen.

- **Ejemplos prácticos de información dudosa**
  - Periódico “El Mundo Today”
  - Wikipedia

- **Recomendaciones**
  - Sentido común, ser conscientes de que existen páginas donde lo que se publica son opiniones (blogs, redes sociales, etc), y de que hay otras muchas que engañan deliberadamente.
  - Contrastar siempre la información, buscándola en más páginas.
  - Si se trata de contenido técnico o científico, acudir a páginas especializadas, enciclopedias, revistas y artículos científicos (como Google Scholar).

Suplantación de identidad – Definición y tipos I

- **¿Qué es?**

  La suplantación de identidad consiste en apropiarse de las credenciales que otra persona utiliza para acceder a un servicio en la red, como:

  - Cuenta de correo electrónico
  - Cuentas de redes sociales
  - Cuentas bancarias
  - Cuentas de webs de compras
  - Cuentas de blogs personales
  - Cuentas de juegos online, de foros temáticos, etc.

- **¿Para qué se utiliza?**

  La suplantación de identidad se usa para:

  - Fines lucrativos: Realizar transacciones bancarias, cobros y compras a cargo de otros
  - Cometer delitos en nombre de otro
  - Robar información confidencial y espiar a individuos y empresas
  - Enviar campañas de *spam* masivo de publicidad

Suplantación de identidad – Definición y tipos II

- **Técnicas de suplantación de identidad**
  - Phishing
  - Pharming
  - Spim
  - SMiShing

Suplantación de identidad – Phishing I

El término **”phishing”** es una contracción de las palabras en inglés "fishing" (pesca) y "phreaking“ (que se refiere a piratear líneas telefónicas).

Es una técnica fraudulenta que usan los ciberdelincuentes para conseguir información de los usuarios de Internet, generalmente sobre cuentas bancarias o de correo.

Se basa en métodos de “ingeniería social", lo que significa que no aprovecha una vulnerabilidad en los ordenadores sino un "fallo humano" al engañar a los usuarios de Internet con un correo electrónico que aparentemente proviene de una empresa fiable, comúnmente de una página web bancaria o empresarial.

- **Ejemplos de phishing**
  - De cuentas de correo:
    - http://www.spamloco.net/2008/11/phishing-de-gmail-con-tarjeta-falsa.html
  - Bancario:
    - http://www.osi.es/es/actualidad/avisos/2015/10/detectado-phishing-que-suplanta-al-banco-sabadell
    - https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen

Suplantación de identidad – Phishing II

- **Recomendaciones para evitar el phishing**
  - Comprobar que la página del servicio comienza con HTTP**S**.
  - Comprobar la identidad de la página haciendo clic en el candado.
  - Tener precaución al seguir enlaces en correos o descargar ficheros adjuntos, aunque sean de contactos conocidos.
  - No acceder al servicio de banca online desde ordenadores públicos, no confiables o que estén conectados a redes WiFi públicas.
  - **Ningún banco envía por correo electrónico solicitudes de datos personales** de sus clientes. Si recibimos un correo en este sentido, no facilitar ningún dato y contactar directamente con el banco.

Suplantación de identidad – Pharming I

El término **”pharming”** deriva de la palabra “farm” (granja) en inglés. Es un ciberataque que consiste en redireccionar el tráfico web de una página legítima hacia otra página falsa. Esto se realiza de manera automática y sin que el usuario tenga que pulsar ningún enlace falso.

Técnicamente, consiste en cambiar la dirección numérica (dirección IP única) asociada al nombre de una página web. Por ejemplo, la web de facebook.com tiene asociada la dirección IP: 31.13.76.102. La dirección numérica y la dirección *con nombre* son equivalentes.

El pharming puede afectar a:

- Muchos ordenadores a la vez (hacer *granjas*) si un servidor de nombres de páginas de Internet (sus siglas son DNS) se ve afectado por un ataque.
- Un ordenador personal infectado por un virus que cambie los nombres de las páginas en dicho ordenador:
  - A través del fichero HOSTS. En Windows se encuentra en la carpeta:
    C:\Windows\System32\drivers\etc
  - Configurando servidores proxy en el navegador del usuario.

Suplantación de identidad – Pharming II

- **Ejemplo práctico de pharming**
  - Modificación el fichero de HOSTS para cambiar la página de Google por la de Facebook

- **Recomendaciones contra el pharming**
  - Tener un antivirus actualizado
  - Siempre que se nos pida introducir un usuario y contraseña en una página web, debemos comprobar que la página web utiliza HTTPS.
  - Fijarnos si la página que se carga al acceder a una dirección web tiene una apariencia diferente a la que estamos acostumbrados.
  - Si la página de nuestro banco cambia de apariencia, debemos contactar con su servicio de atención al cliente para confirmar estos cambios antes de introducir nuestros datos de acceso.
  - No introducir datos personales o bancarios en páginas web cuyo certificado digital no sea reconocido de forma automática por nuestro navegador.

Suplantación de identidad – Spim II

- **Consejos frente al spim**
  - Si un contacto conocido nos envía un mensaje o un enlace que no encaja en la conversación que estamos manteniendo, debemos preguntarle antes de hacer clic.
  - Si no estamos seguros de quién es el remitente que nos envía el mensaje, no debemos hacer clic en ningún enlace o adjunto que nos envíe.

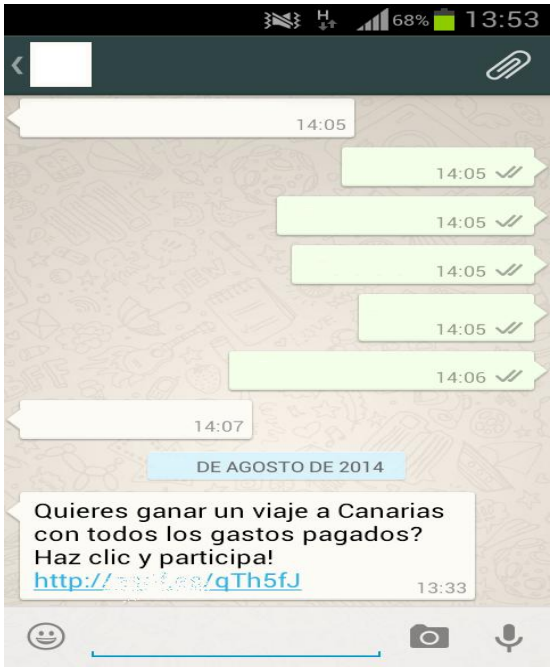
Suplantación de identidad – Spim I

Se trata de un fraude que consiste en enviar *spam* a los usuarios a través de aplicaciones de mensajería instantánea, como Skype, WhatsApp y similares.

Los mensajes de spim aparecen en forma de ventanas emergentes o de texto añadido en las conversaciones. Los enlaces incluidos en estos mensajes suelen llevar a páginas fraudulentas.

Se detecta peor que el spam de email, ya que los enlaces maliciosos pueden llegarnos en mitad de una conversación con alguien conocido.

- **Ejemplo de spim**



Suplantación de identidad – SMiShing I

El **“SMiShing”** es una estafa derivada del *phishing*.

Mediante el envío de mensajes SMS, se solicitan datos al usuario o se le pide que llame a un número o que entre a una página web.

Esta estafa, como las anteriores, puede tener diferentes objetivos:

- **Suscribir al usuario a un servicio SMS premium**. Ejemplo:
  - *“FELICIDADES, ha sido seleccionado de entre millones de usuarios con un coche. Para obtener su premio envía al [número] la palabra COCHE.”*
- **Que el usuario llame a un número de tarificación especial**:
  - *“Marta está desesperada buscándote, dice que habló contigo estos días y pide tu teléfono. Dime si puedo dárselo. Contesta.”*
- **Robar datos bancarios**:
  - *“Estimado cliente, su tarjeta visa ha sido bloqueada por su seguridad. Para desbloquear su tarjeta visite urgente esta [web] y complete los pasos. Tiene 24h.”*
- **Que el usuario acceda a una web fraudulenta para infectar su ordenador o estafarle con algún producto/servicio inexistente**:
  - *“Esta es la web que te dije: [web] . Está todo a mitad de precio: Calvin Klein, Dolce Gabanna, Hugo Boss, Loewe, Chanel, etc.”*

Suplantación de identidad – SMiShing II

- **Consejos para protegerse del SMiShing**
  - Desconfiar de los SMS que hablan de trabajos, premios (sin haber jugado) o paquetes recibidos (sin haberlos pedido).
  - No acceder a ninguna página web que llegue a través de SMS, más aún si desconocemos el número del remitente.
  - No dar datos bancarios ni similares a través de SMS ni telefónicamente.

Gestión de la privacidad al navegar por Internet I

- **El negocio de la recopilación de los hábitos de navegación**

  La gran mayoría de páginas web, sólo por el hecho de visitarlas, recopilan estadísticas sobre los contenidos que buscamos en ellas, de los anuncios en los que hacemos clic, del tiempo que pasamos visitándolas, etc.

  Estos datos, aparentemente anónimos (ya que no requieren dar datos personales), utilizan la dirección IP de nuestra conexión a internet para identificar la línea desde donde nos conectamos y también identificadores del ordenador y del navegador que usamos.

  El seguimiento de los hábitos y los gustos de los usuarios, permite a las empresas ofrecer publicidad dirigida, de una forma más certera y eficiente de acuerdo al tipo de usuario.

Gestión de la privacidad al navegar por Internet II

- **Las cookies**

  Las cookies son pequeños archivos de texto que se almacenan en el ordenador mientras navegamos por las páginas web. Pueden guardarse de forma temporal o permanente.

  Las cookies son usadas para diferentes objetivos, algunos con más *ética* que otros:

  - Mantener una sesión activa cuando nos identificamos en un servicio web (por ejemplo al entrar en el correo electrónico).
  - Guardar las preferencias cuando cambiamos el aspecto de las páginas web que lo permiten, para adecuarla a nuestros gustos.
  - Recopilar información sobre el texto que buscamos.
  - Recoger estadísticas de tiempo de visita de una página.
  - Llevar control sobre qué anuncios hacemos clic.

Gestión de la privacidad al navegar por Internet III

- **¿Se puede evitar el rastreo de nuestros hábitos?**

  En una navegación cotidiana, no es posible al 100% evitar que una página web recoja cierta información sobre nosotros, como la dirección IP desde la que nos conectamos, o el tipo de navegador y de sistema operativo.

  Sin embargo, sí es posible bloquear el seguimiento de gustos o preferencias publicitarias que realizan muchas webs. Existen utilidades que bloquean cookies y otros elementos que las empresas insertan en sus páginas para recopilar hábitos.

- **Ejercicio práctico**

  - Instalar el complemento *Ghostery* en el navegador para bloquear el rastreo de hábitos de navegación.
  - Administrar la configuración de anuncios de las cuentas de Google.

Preguntas tras el día 2

- **¿PREGUNTAS?**

- **¡Nos vemos en el próximo día!**

DÍA 3

ÍNDICE DÍA 3

- Día 3
  - Importancia de los contenidos que publicamos en Internet
    - Publicaciones en redes sociales
    - Concienciación a los menores
  - Protección de los menores frente a contenido inadecuado
  - Ciberacoso a los menores: tipos de chantajes y amenazas que reciben
    - Cyberbullying
    - Grooming
    - Sexting
  - Aspectos legales
    - Líneas de denuncia ante robo de datos personales o ciberacoso

Importancia de los contenidos que publicamos en Internet

Cuando publicamos cualquier material en Internet, como texto, fotos, vídeos, audios, etc., debemos tener muy claro que ese material va a estar al alcance de más personas, y no sabemos qué fines le van a dar.

Además en muchos casos no tendremos el control total sobre lo que hemos publicado, y no será posible retirarlo por completo aunque queramos.

Los menores son muy propensos a ser atacados a través de información que ellos mismos han publicado o compartido con otros.

Es importante tener claros dos aspectos:

- **Pensar antes de publicar**:
  - Si algo puede ser utilizado en nuestra contra o pudiera traernos problemas en el futuro, mejor no publicarlo.
- **Si un servicio de Internet es gratuito, es posible que el producto seas tú**:
  - La mayoría de servicios gratuitos tienen objetivos comerciales.

Acoso a menores a través de Internet

Hoy día el *ciberacoso* o acoso a menores en Internet se da con frecuencia, y hay que advertirles y educarles para prevenir y evitar estas situaciones, que provocan gran sufrimiento.

Tipos de acoso principales que se producen:

- **Ciberbullying u hostigamiento entre menores**:
  - Es el uso de información electrónica y medios de comunicación digitales para ejercer el acoso sicológico entre menores. No intervienen personas adultas. En ciberbullying se incluyen actuaciones de chantaje, vejaciones e insultos de niños a otros niños.
- **Grooming:**
  - El grooming (en español “acicalar”) consiste en conductas y acciones de un adulto para ganarse la amistad de un menor de edad, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él. En algunos casos, se puede buscar la introducción del menor al mundo de la prostitución infantil o la producción de material pornográfico.
- **Sexting :**
  - Se refiere al envío de contenidos eróticos o pornográficos por medio de Internet o teléfonos móviles. Es una actividad que puede exponer a los menores de edad al grooming y al ciberbullying, como medio de presión y ridiculización contra la persona protagonista.

Medidas ante el ciberacoso

- No responder a mensajes ofensivos. Guardar las conversaciones como pruebas para demostrar lo que ocurre.
- Avisar de inmediato a un adulto.
- Denunciar empleando los servicios de Internet de la guardia Civil y la Policía:
  - www.policia.es/colabora.php
  - www.gdt.guardiacivil.es

Preguntas tras el día 3

- **¿PREGUNTAS?**

¡Hasta la próxima!