CIBERSEGURIDAD

REALIZADO POR :

- ***Marian López***
- ***Alba González***

Marian	**Alba**

ÍNDICE:

- Hackers y crackers.
- Pharming.
- Phising.
- Conceptos de seguridad activa y seguridad pasiva
- Spam.
- Cookies. Eliminación de cookies del navegador.
- Hoaxes.
- Certificado digital.
- P2P.
- Ataques denegación DNS (DDos).
- Virus informáticos
- Deep Web.
- Síntomas para detectar que nuestro ordenador ha sido atacado.
- Software para proteger el ordenador.
- Uso seguro de la Webcam.
- Protección de la WiFi.
- Medidas de prevención frente a posibles ataques.
- Seguridad en los DISPOSITIVOS MÓVILES.
- Gusanos
- Software malintencionado o malware (malicious software).

HACKERS Y CRACKERS :

Los hackers son aquellos expertos informáticos que utilizan sus conocimientos técnicos para superar un problema, normalmente asociado a la seguridad.
Los crackers son aquellas personas que utilizan técnicas de hacking con fines criminales o maliciosos.

PHARMING :

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (*Domain Name System*) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio a otra máquina distinta.

PHISING:

Phishing, conocido como suplantación de identidad, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta . El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

CONCEPTOS DE SEGURIDAD ACTIVA Y SEGURIDAD PASIVA:

La seguridad activa en informática es la que se usa diariamente para prevenir cualquier tipo de ataque en un sistema.
Existen muchas acciones para lograrlo y, dependiendo de cada situación, se deben adoptar unas u otras.
La seguridad pasiva en informática es la que entra en acción para minimizar los daños causados por un usuario o un accidente en los sistemas. Igual que con la seguridad pasiva, existen varias prácticas para cada situación.

SPAM:

Los términos correo basura, correo no solicitado y mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido, habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.

COOKIES. ELIMINACIÓN DE COOKIES EN EL NAVEGADOR :

Cookie o galleta informática es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador. Eliminación de cookies en el navegador:

➔ En Mozilla FIrefox:

1. Abre Firefox y clica en la parte superior derecha en el menú hamburguesa (tres líneas horizontales). Al desplegarse, clica sobre el símbolo de la rueda dentada "Opciones".

2. Selecciona en la lista de la izquierda "Privacidad y seguridad" ("Privacy and Security") y dirígete a la pestaña desplegable de la sección "Historial" ("History"). Puedes llegar también hasta aquí si se abre una nueva ventana con la dirección "*about:preferences#privacy".*

3. Deja tal cual la opción "Recordar el historial" ("Remember history") del menú desplegable y clica en "limpiar historial reciente" ("clear your recent history").
4. Se abrirá una nueva ventana, en la que hay que marcar la opción "Cookies" y después "Borrar ahora". De esta forma se eliminan todas las cookies almacenadas en el espacio de tiempo seleccionado.
5. Si lo que quieres es borrar solo determinadas cookies, entonces vuelve a la ventana del paso 2 y selecciona la opción "eliminar cookies de forma individual" ("remove individual cookies"). A través de la función de búsqueda podrás buscar las cookies y borrarlas.

➔ En Chrome :

1. Abre Chrome, clica en la parte superior derecha en el símbolo de tres puntos. Se desplegará una lista en la que hay que seleccionar "Configuración".

2. Se accede a una nueva interfaz. En la parte superior izquierda se despliega otro menú simbolizado con las tres líneas horizontales. En él se selecciona

"Configuración avanzada" y aquí "Privacidad y seguridad" ("Privacy and security").

3. De la lista de opciones que aparece hay que seleccionar "Configuración de contenido" ("Content settings") y tras ello "Cookies". A continuación, hay que acceder a la sección "Todas las cookies y todos los datos de sitios" ("All cookies and site data"). También se puede llegar hasta este punto al introducir en una nueva ventana la dirección "*chrome://settings/content/cookies".*
4. Al clicar sobre "Eliminar todo" ("Remove all") se eliminan todas las cookies de una vez, aunque si lo que se pretende es deshabilitar solo algunas, entonces hay que seleccionarlas manualmente en la lista.

➔ En Internet Explorer :

1. Abre Internet Explorer y clica en la rueda dentada que aparece en la parte superior derecha. En el menú desplegable selecciona "Seguridad".

2. A continuación selecciona la opción "Eliminar historial de exploración" ("Delete Browsing History") y marca en el menú que está abierto "Cookies y datos de los sitios web" ("Cookies and website data"). En versiones anteriores este punto se denomina "Cookies". Para confirmar, clica sobre "Eliminar" ("Delete").

HOAXES :

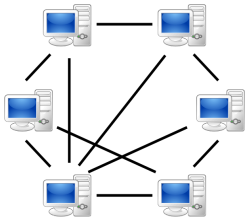
Un bulo es una falsedad articulada de manera deliberada para que sea percibida como verdad.
El término se popularizó principalmente en castellano al referirse a engaños masivos por medios electrónicos, especialmente Internet.

CERTIFICADO DIGITAL :

Un certificado digital es un fichero informático firmado electrónicamente por un prestador de servicios de certificación, considerado por otras entidades como una autoridad para este tipo de contenido, que vincula unos datos de verificación de firma a un firmante, de forma que únicamente puede firmar este firmante, y confirma su identidad.

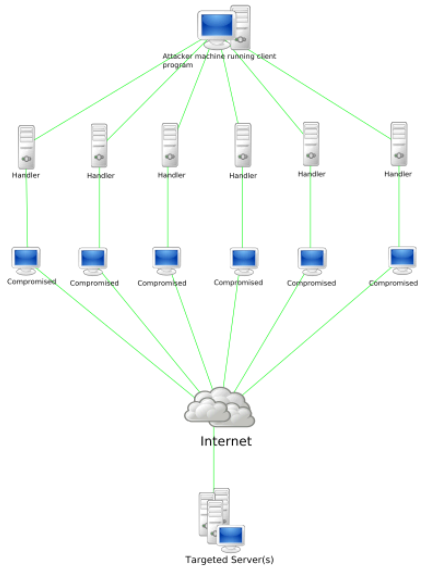
P2P :

Una red *peer-to-peer* (*P2P*, por sus siglas en inglés) es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nudos que se comportan como iguales entre sí.



ATAQUES DENEGACIÓN DNS (DDos) :

Un ataque de denegación de servicio, también llamado ataque DoS (por sus siglas en inglés, Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.



VIRUS INFORMATICOS:

Los virus informáticos son programas para interferir expresamente en el funcionamiento de un ordenador que tiene la capacidad de causar daño. ALGUNOS TIPOS DE VIRUS

1- Virus básico

Es la modalidad de virus más sencilla y antigua, creado con el objetivo de entorpecer el funcionamiento de los sistemas operativos de los procesadores, ralentizando su funcionamiento. También puede borrar información de archivos o equipos.

2- Troyanos

Su fortaleza se reside en que logran un nivel de camuflaje que puede pasar desapercibido para algunas versiones de antivirus.Es un malware que se aloja en diversas aplicaciones y archivos del sistema operativo.

3- Spyware

Es una clase de virus más especializado, ya que es un programa espía. Su objetivo es robar absolutamente toda la información de tu ordenador y hacérsela llegar a su dueño.

DEEP WEB

La mayor parte de los usuarios que ingresan en la internet profunda saben exactamente lo que están buscando y donde buscarlo, ya que las páginas que hay ahí carecen de vínculos. Este sitio es muy peligroso ya que se encuentra todo tipo de gente y tienes que tener mucho cuidado, lo preferible es no entrar.

SISTEMAS PARA DETECTAR QUE NUESTRO ORDENADOR HA SIDO ATACADO

Mi ordenador me habla: aparecen todo tipo de pop-ups en el escritorio.

El PC va tremendamente lento

No arrancan las aplicaciones

Mi ordenador me habla en un idioma raro...

SOFTWARE PARA PROTEGER EL ORDENADOR

Avast Software

Avira

AVG Free Antivirus

Bitdefender

USO SEGURO DE LA WEBCAM

La webcam puede ser activada sin que te des cuenta, por eso es necesario tomar algunas medidas.

1- No chatear con personas desconocidas

2- No transmitir imágenes

3- Cuando no se esté utilizando, desconectarla

4- Utilizar cámaras con luz piloto para ver si está grabando o no

5- Pasar siempre el antivirus para que no puedan acceder

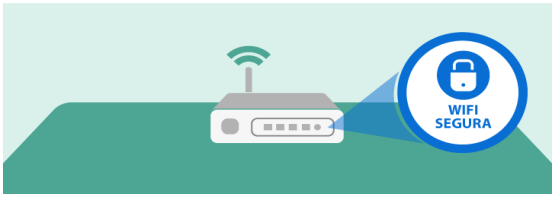
PROTECCIÓN DE LA WiFi

El router debe incorporar al menos el protocolo WPA entre sus medidas de seguridad. Para mayor protección también es mejor:

1- Cambiar la contraseña por defecto

2- Cambiar el nombre de la WiFi o SSID

3- Apagarlo si nos ausentamos varios días



MEDIDAS DE PREVENCION FRENTE A POSIBLES ATAQUES

1- Proteger los equipos

2- Contraseñas fuertes

3- Utilizar protocolos de seguridad

4- No descargar contenido pirata

SEGURIDAD EN LOS DISPOSITIVOS MOVILES

1- Pin

2- Patrón

3- Huella

4- Antivirus o Cortafuegos

5- Contraseña de gmail, etc ... difícil

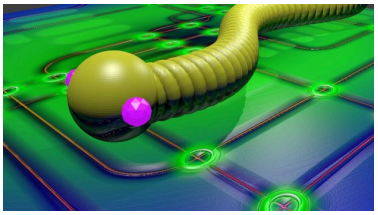
6- No apuntar tus contraseñas o datos personales en ninguna aplicación

7- Tener cuidado que aplicaciones descargas, metes tu tarjeta o pones datos

8- No darle al botón de cookies o anuncios que te salten(con el botón de aceptar)

GUSANOS

Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. Estos se propagan de ordenador en ordenador, pero a diferencia de un virus, tiene la capacidad de propagarse sin ayuda de la persona. Lo más peligro es su capacidad para replicarse en el sistema informático, por lo que una computadora podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador a gran escala.



SOFTWARE MALINTENCIONADO O MALWARE

Es un tipo de software que tiene como objetivo infiltrarse o dañar un ordenador o todo otro sistema de información.

BIBLIOGRAFÍA

- Imagen portada
- Código QR
- Licencia
- Hackers
- Imagen hackers
- Crackers
- Pharming
- Imagen pharming
- Imagen phising
- Phising
- Imagen seguridad activa y pasiva
- Seguridad activa y pasiva
- Spam
- Eliminación cookies del navegador
- Imagen cookies
- Cookies
- Imagen hoaxes
- Hoaxes
- Certificado digital
- Imagen certificado digital
- P2P
- Imagen P2P
- Ataques denegación DNS (DDos)
- Imagen ataques denegación DNS (DDos)
- Virus informáticos
- Deep Web
- Síntomas para detectar que nuestro ordenador ha sido atacado
- Software para proteger el ordenador

➢ Uso seguro de la Webcam
➢ Protección WiFi
➢ Medidas de prevención frente a posibles ataques
➢ Seguridad en los dispositivos móviles
➢ Gusanos
➢ Software malintencionado o malware