RedXXI educa y tu digital

Junta de Castilla y León

AndroidLost

Es una aplicación muy útil por si pierdes el teléfono móvil. Con esta aplicación podrás hacer todo lo que quieras a través de tu ordenador, desde encontrar tu Android en caso de que lo pierdas o bloquear todo lo que contiene el teléfono para que nadie lo pueda usar.

Cómo empezar...

Descarga la aplicación al teléfono

1

Registra tu teléfono

2

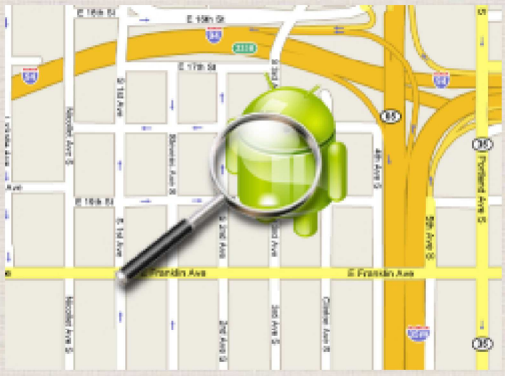
3

Vuelve a iniciar sesión en la página web

¡... y empieza a controlar remotamente tu teléfono!

¿Qué puede hacer AndroidLost...?

- Hacer sonar una alarma
- Toma una foto y la envia a tu email si se introduce un PIN erróneo
- Enviar su ubicación
- Enviar el estado del teléfono al servidor (bateria, imei,...)
- Activar y desactivr la wifi y el GPS
- Bloquear y desbloquear el teléfono
- Borrar tarjeta SD
- Tomar una foto con la cámara frontal y enviarla a tu email
- Enviar un email con la ubicación cuando tiene bateria baja



Fuente: upsdroid.blogspot.com.es

...y mucho más...

Maestros colaboradores Red XXI - Ávila

Plan de Seguridad y Confianza Digital
Dirección General de Innovación y Equidad Educativa
Consejería de Educación

VIRUS Y FRAUDES

Actualiza tu software, el sistema operativo, el navegador de Internet y el antivirus en todos tus dispositivos. Instala solo aplicaciones de fuentes de confianza y revisa los privilegios.

TECNOADICCIONES

Limita el tiempo de uso del ordenador y dispositivos móviles. Planifica con antelación lo que vas a hacer o para qué te vas a conectar. No dejes a los amigos y actividades físicas de lado para estar conectado a internet.

#SegConCyL

Junta de Castilla y León

CFIE Ciudad Rodrigo

Plan de Seguridad y Confianza Digital en el ámbito educativo

Junta de Castilla y León

CFIE Ciudad Rodrigo

PRIVACIDAD

Cuidado al activar la geolocalización, atentan contra tu privacidad. Protege tus datos personales para que no sean utilizados de forma fraudulenta. Piensa antes de publicar fotografías o comentarios en internet. Una vez que lo hemos subido a la red perdemos el control sobre ello.

CIBERBULLYING

No lo produzcas, no hagas daño. Si sabes que se está produciendo bullying ayuda a la víctima, de lo contrario eres cómplice.

SEXTING

NO lo produzcas, no envíes a NADIE fotos comprometedoras. No sabes qué uso se va a hacer de las fotografías o en qué manos puede caer tu dispositivo móvil.

IDENTIDAD DIGITAL

Es nuestro "yo digital". Cuidar nuestra imagen o reputación en Internet es cuidar nuestra imagen en nuestra vida real, ya que Internet no es más que una extensión misma de la realidad.

GROOMING

No aceptes contactos en tus redes sociales ni en mensajería si no los conoces en persona. Tu importancia no se mide por el número de "amigos" en las redes sociales.

SUPLANTACIÓN DE IDENTIDAD

Evítala limitando la difusión voluntaria de datos personales y privados en redes sociales, juegos online, mensajería. Configura correctamente la privacidad. Mantén tu equipo seguro.

NETIQUETA

Trata a los demás como quieres ser tratado.

¿Cómo puedes evitar que los ordenadores de un centro acabe en una botnet?

Se recomendienda mantener actualizado el sistema operativo y todos los programas instalados en él, proteger el ordenador con alguna herramienta de seguridad como antivirus y tener unos buenos hábitos de uso. ¡Ah! Y aplicando el sentido común: no instalar nada que no se haya elegido, no pulsando enlaces de e-mails cuyo remitente se desconoce, desconfiando de los chollos que te anuncian por Internet, etc.

¿Qué ocurre si algún ordenador se queda encendido en el centro?

Que podría ser infectado con un virus que lo convierta en un terminal zombie, infectando a su vez el resto de los ordenadores del centro y conviertiendo la red escolar en parte de una Botnet. Dando a los hackers herramientas para poder llevar a cabo sus tareas delictivas e ilegales.

Servicio AntiBotnet

Desde la OSI se pone a tu disposición el Servicio Antibotnet, un mecanismo que permite conocer si existen amenazas o incidentes de ciberseguridad relacionados con redes de ordenadores comprometidos o botnets asociados a tu conexión a Internet. Para ello se chequea la dirección IP pública que tengas asignada en cada momento contra nuestra base de datos.

La finalidad del servicio es proporcionar información y herramientas que puedan ayudarte en la desinfección de los dispositivos afectados, contribuyendo así a un Internet más confiable y seguro para todos.

OSI Oficina de Seguridad del Internauta

Junta de Castilla y León
Consejería de Educación

BOTNET O RED ZOMBIE EN LA ESCUELA

Botnet o red zombie de ordenadores.

¿Últimamente has notado que tu ordenador va más lento de lo normal, el ventilador hace mucho ruido aún cuando no lo estás utilizando y algunas aplicaciones han dejado de funcionar correctamente?

Capturar contraseñas y datos personales.

Recopilan las contraseñas de los servicios de banca, redes sociales, correo web (Gmail, Outlook, etc.) que utilizan los usuarios del ordenador infectado para después venderlas en la “deep web”, el mercado negro

Mi ordenador es un Zombie

Estos síntomas podrían ser debidos a que tu ordenador se ha convertido en un pc “zombi”. ¿Eso qué significa? Que hay alguien, aparte de ti, que está controlando tu ordenador sin que seas consciente de ello.

Pero, ¿cómo tu ordenador se ha convertido en un zombi? Se ha infectado con un tipo de virus capaz de controlar tu ordenador de forma remota. Esto quiere decir que alguien, sin estar físicamente delante de tu ordenador, y con los conocimientos técnicos suficientes, puede manejarlo a su antojo. Pero eso no es todo, si tu ordenador es un zombi, estará formando parte de una red zombi de ordenadores, conocida con el término anglosajón botnet.

¿Qué es una botnet?

No es más que un gran número de ordenadores zombi, infectados con el mismo tipo de virus, que están controlados por una misma persona u organización criminal.

¿Por qué quieren que tu ordenador pertenezca a una botnet?

Principalmente para llevar a cabo actividades que les generen unos beneficios económicos de manera ilegal.

¿Qué consiguen los hackers infectando una red?

Capturar contraseñas y datos personales.
Enviar spam y propagar virus.
Hacer que una página web deje de estar disponible.
Manipular encuestas y abusar de los servicios de pago por publicidad.
Llevar a cabo desde los ordenadores otro tipo de fraudes.
Acceder a páginas web cuyo contenido es denunciable o ilegal: pedofilia, prostitución, drogas, etc. Almacenar y compartir ficheros con copyright, suplantar tu identidad para publicar anuncios falsos, etc. ¡Cualquier otra cosa que se te ocurra!

CÓMO CONSTRUIR CONTRASEÑAS SEGURAS

Imágenes YouTube
https://www.youtube.com/watch?v=iV9CmN-g_go

Aquí veras una Forma de crear CONTRASEÑAS SEGURAS Pero fáciles de Recordar.

Piensa en una frase fácil de memorizar...

Utiliza la primera letra de cada palabra.
Mi mamá cocina mejor que tu mamá.
mmcmqtm

Añade una letra mayúscula a la frase.
mmcMqtm

También añade un numero.
2mmcMqtm

Finalmente añade algún carácter en cualquier lugar.
2mmc&Mqtm

¡NUNCA utilices la misma contraseña de tu correo electrónico para cuentas más sensibles como tu cuenta de banco!
Microsoft

Recuerda que una contraseña segura tiene:
- Letras MAYÚSCULAS y minúsculas
- Letras y NÚMEROS
- Otros SÍMBOLOS
- 8-14 caracteres

Maestros colaboradores Red XXI y CFIE Ávila

Junta de Castilla y León

Plan de Seguridad y Confianza Digital
Dirección General de Innovación y Equidad Educativa
Consejería de Educación

ESCANÉAME

Junta de Castilla y León

Autores: Alicia Hernández Moreno, Carmen Bernal Sánchez, Fausto Santamaría Yusta, Fernando Ruiz Úbeda, José Carlos González Blázquez, Julio Sánchez Sánchez

Decálogo de seguridad en Internet

Junta de Castilla y León

Plan de Seguridad y Confianza Digital
Dirección General de Innovación Educativa y Formación del Profesorado
Consejería de Educación

OJO CON LOS RESULTADOS DE LOS BUSCADORES WEB: CONVIENE ESTAR ATENTO Y VERIFICAR A QUÉ SITIOS WEB ESTÁS SIENDO ENLAZADO.

EVITA LOS ENLACES SOSPECHOSOS: ES UNO DE LOS MEDIOS MÁS UTILIZADOS PARA REDIRECCIONAR A SITIOS MALICIOSOS.

ACEPTA SÓLO CONTACTOS CONOCIDOS: DE ESTA MANERA EVITARÁS AMENAZAS COMO MALWARE, SEXTING, CYBERBULLYING... SÉ PRUDENTE EN LA UTILIZACIÓN DE LAS REDES SOCIALES

ACTUALIZA EL SISTEMA OPERATIVO Y LAS APLICACIONES: EVITARÁS LA PROPAGACIÓN DE AMENAZAS (VIRUS, TROYANOS...).

EVITA LA EJECUCIÓN DE ARCHIVOS SOSPECHOSOS: LA PROPAGACIÓN DE MALWARE SUELE REALIZARSE A TRAVÉS DE ARCHIVOS EJECUTABLES; EVITA SU EJECUCIÓN A MENOS QUE CONOZCAS LA SEGURIDAD DEL MISMO Y SU PROCEDENCIA SEA CONFIABLE.

NO OLVIDES EL USO DE MEDIOS DE SEGURIDAD: LOS ANTIVIRUS, FIREWALL Y ANTISPAM PROTEGEN EL EQUIPO ANTE LAS PRINCIPALES AMENAZAS QUE SE PROPAGAN POR INTERNET.

UTILIZA CONTRASEÑAS SEGURAS: SI LA CONTRASEÑA ES SENCILLA O COMÚN, CUALQUIERA PODRÍA ADIVINARLA Y POR LO TANTO ACCEDER INDEBIDAMENTE COMO SI FUERA EL USUARIO VERDADERO.

CUIDADO DESDE DÓNDE DESCARGAS: EN MUCHOS SITIOS SE OFRECEN PROGRAMAS POPULARES QUE SON ALTERADOS, MODIFICADOS O SUPLANTADOS POR VERSIONES QUE CONTIENEN ALGÚN TIPO DE MALWARE.

SI MIENTRAS NAVEGAS DETECTAS ALGO FUERA DE LO COMÚN: AVISA A TUS PADRES O A UN ADULTO DE CONFIANZA.

NUNCA SE DEBEN PASAR DATOS A DESCONOCIDOS A TRAVÉS DE LA RED: EN CASO DE QUE ALGUIEN SOLICITE DATOS PERSONALES, ES CONVENIENTE ABANDONAR LA CONVERSACIÓN CON ESA PERSONA.

DECÁLOGO DE SEGURIDAD EN INTERNET

Navego seguro sí ...

1. Utilizo C0n3.$ñ@$ seguras.

2. Mantengo el navegador y el antivirus actualizado en mi ordenador, tableta digital o Smartphone.

3. Interpreto y contrasto la información que obtengo por internet. No todo lo que está publicado es cierto.

4. Sé que en las redes públicas o sin proteger mis conversaciones pueden ser escuchadas, y en la casa he cambiado la contraseña por defecto.

Recuerda que ...

5. El SENTIDO COMÚN es el mejor antivirus y también nos funciona dentro de la red. Lo que es inadmisible fuera también lo es dentro de la red. Netiquetate!

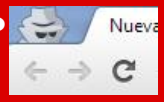
6. IGNORA cualquier comentario que te haga sentir incómodo, BLOQUÉALO y si es necesario DENUNCIALO.

7. PIENSA ANTES DE PUBLICAR. Lo que no llevarías colgado en un cartel en tu camiseta no lo publiques.

Nunca debes ...

8. NUNCA facilitar datos personales ( ,  , donde estudio, vacaciones,  ..).

Al comprar vigila:

- Protocolo: https:
- 

Navegación en incógnito
- Nunca en contestación a un mensaje

9. NUNCA aceptes invitaciones de desconocidos, es una puerta abierta a tus imágenes y datos.

10. NUNCA quedes con desconocidos, no sabes sus verdaderas intenciones.

Junta de Castilla y León

Plan de seguridad y confianza digital
Dirección General de Innovación Educativa y Formación del Profesorado
Consejería de Educación

Para saber más ...

¿Son tus contraseñas seguras? Prueba

Hackeador de contraseñas de Intel

Los gestores de contraseñas 1password, msecure, Lasspass, Keepass, ... u otros) te pueden ayudar en el control de tus contraseñas.

Las Netiquetas

Son las reglas de comportamiento comúnmente aceptadas para navegar. Son como las normas de educación que todos conocemos y con las que nos relacionamos habitualmente .

¿Las conoces?

netiquétate | ¡¡Apúntate a la Netiqueta Joven para Redes Sociales!!

PantallasAmigas

Recuerda

Si te sientes acosado o hay contenido propio o de otros en la red sin tu consentimiento, ilegal o nocivo:

DENUNCIA.

protegeles.com

91 7 400 019

o a través de la App anónimamente

Algunas Webs de interés:

http://www.protegeles.com/
http://www.educa.jcyl.es/ciberacoso/es
http://www.pantallasamigas.net/
http://navegacionsegura.es/
http://www.infanciaytecnologia.com/
http://www.deaquinopasas.org/
http://www.osi.es/proteccion-de-menores/
https://sites.google.com/site/tallerid11/
http://www.netiquetate.com/

Junta de Castilla y León

Plan de seguridad y confianza digital
Dirección General de Innovación Educativa y Formación del Profesorado
Consejería de Educación

Para más información visita las siguientes páginas:

- Identidad digital y reputación:

  www.proteccionprivacidad.com

  www.e-legales.net

  www.cuidatuimagenonline.com

- Netiquetas

  www.alia2.org

  www.abogacia.es

- Riesgos y peligros

  www.sexting.es

  www.stopgrooming.wordpress.com

- Respeto y creatividad de la obra privada

  http://es.creativecommons.org/blog/licencias/

  www.copyright.gov/help/spanish_faq/index.html

Junta de Castilla y León

Plan de seguridad y confianza digital
Dirección General de Innovación y Equidad Educativa
Consejería de Educación

DISFRUTA DE LA RED

PERO CON CUIDADO !!

- APRENDE
- INFÓRMATE
- ESTUDIA

- VISITA SITIOS SEGUROS
- CONTRASTA LA INFORMACIÓN

- COMUNÍCATE
- NETIQUETAS

- USO DE REGLAS
- SÉ RESPETUOSO
- UTILIZA UN LENGUAJE CORRECTO

- COMPARTE
- RELACIÓNATE

- SÓLO CONTACTOS SEGUROS
- PROTEGE TU PRIVACIDAD

- NO TENGAS MIEDO
- INFORMA A TUS PADRES/PROFESORES
- DENUNCIA

- ACOSO, CIBERBULLYING, SEXTING, GROOMING…

- SÉ CREATIVO
- INVENTA
- DISEÑA

- COPYRIGHT
- LICENCIAS
- RESPETO

Seguridad y dispositivos móviles.

CONDUCTAS DE RIESGO

- Dispositivos desprotegidos.
- Instalación de software de procedencia no certificada.
- Ficheros recibidos a través de redes sociales.
- Respuesta a correo electrónico malicioso.
- Clic en publicidad falsa o engañosa de las apps.
- Páginas web contaminadas.
- Actuaciones del usuario (fotos geolocalizadas,...).

CONSEJOS PARA USO DE MÓVILES Y/O TABLETAS

- Protección por contraseña de acceso.
- Instalar gestor que permita borrar datos.
- Uso de sistema de cifrado.
- Verificación en dos pasos en las cuentas que lo permitan.
- Instalación de Apps de confianza.
- Atención a los permisos solicitados por las Apps.
- Haz un backup de datos e imágenes sensibles periódicamente.

WIFI PÚBLICA

- Conecta la Wifi sólo cuando la utilices.
- No transfieras nunca información sensible con conexión a Wifis públicas o abiertas (correo, cuenta bancaria, compras en línea, redes sociales,.....)

Junta de Castilla y León

CONTRASEÑAS

- Longitud mínimo 8 caracteres.
- Números, letras y símbolos.
- Frase que sólo tú conozcas.
- No almacenar.

GEOLOCALIZACIÓN

- Ten cuidado con las imágenes o vídeos que publiques o en las que te etiqueten, pueden dar pistas del lugar en el que te encuentras.
- Destruye la información que ofreces de forma pública.

ACTUALIZACIÓN

- Utiliza siempre PIN y bloqueo automático.
- Apaga la pantalla y el dispositivo.
- Utiliza antivirus.
- Mantener el software actualizado.
- Actualiza tus aplicaciones sólo desde sitios oficiales.

Algunas Premisas.

- En España se roba un móvil cada dos minutos[1].
- 279.319 denuncias por sustracción de móviles en 2014.
- En España hay 50 millones de líneas móviles de los que el 81% de los dispositivos son smartphones[2].
- En España más del 80% de los usuarios de Internet se conecta a través de un dispositivo móvil.

1.– Cinco Días (4-3-2015).

2.– Observatorio nacional de las Telecomunicaciones y de la SI (Abril-2015).

Junta de Castilla y León

Plan de Seguridad y Confianza Digital en el ámbito educativo

5 PASOS PARA TENER

Una WIFI segura en tu casa

Configuración

Cambia la contraseña de administración

Utiliza una seguridad WAP o WAP2

No uses contraseñas recurrentes

Desactiva el SSID

Usa un filtrado MAC

Junta de Castilla y León

Plan de Seguridad y Confianza Digital en el ámbito educativo.

Dirección General de Innovación y Equidad Educativa
Consejería de Educación

Maestros colaboradores Red XXI Ávila | CFIE de Ávila.