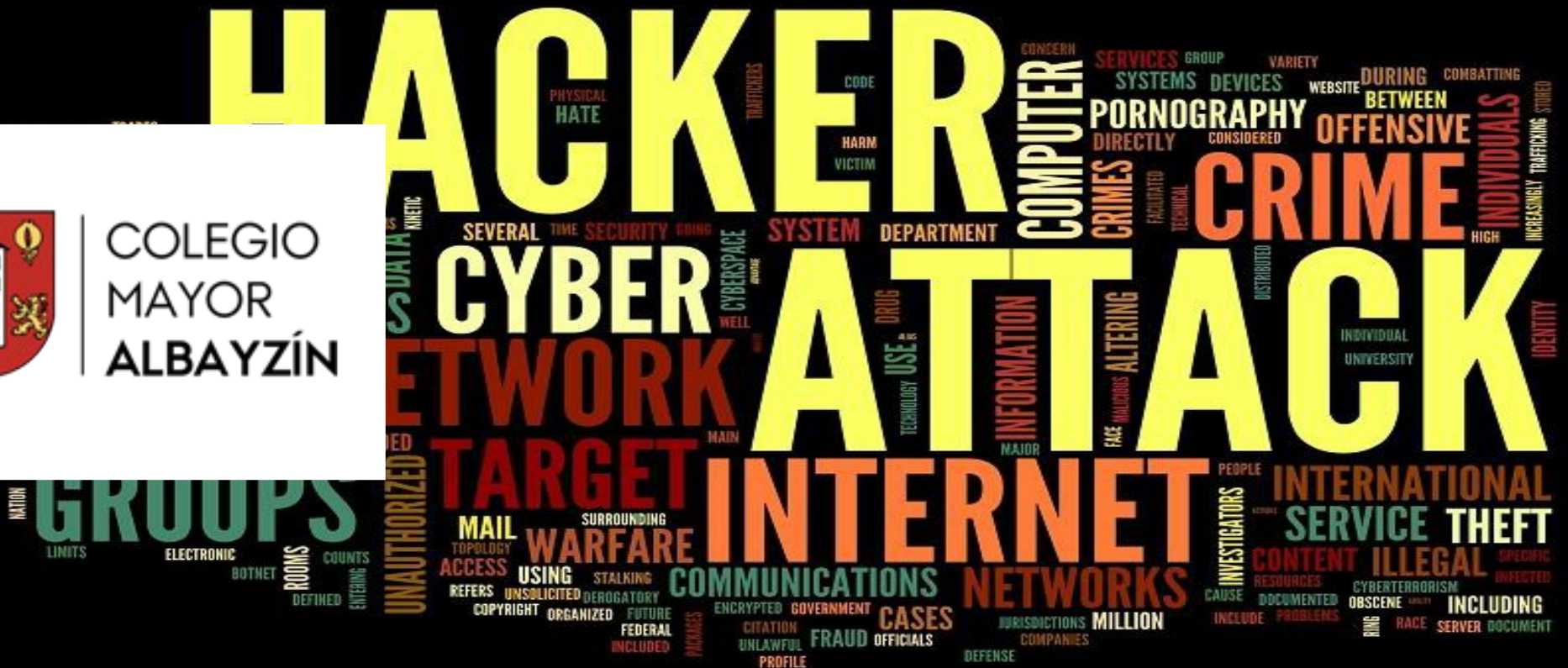


Seguridad en la red



COLEGIO
MAYOR
ALBAYZÍN



Diego J. Romero López

Ingeniero Software en inteligencia

diegojromerolopez@gmail.com

Índice

1. Presentación
2. Qué es internet
3. Cómo nos afecta la red
 1. Procrastinación
 2. Adicción a internet
 3. Infoxicación
4. Amenazas y peligros
 1. Automáticas
 2. Humanas
 1. Piratas informáticos
 2. Cyberacoso
 3. Trolling

Índice (y 2)

5. Comportamiento seguro en la red

1. Modo incógnito
2. Bloqueadores de publicidad
3. Correo electrónico
4. Redes P2P
5. Redes sociales
6. Menores de edad

6. Conclusiones

7. Preguntas

1. Presentación

Diego J. Romero López
Ingeniero de Software

Especializado en desarrollo web en
inteligencia

Ing. Informática (Ms. Eng.)
MSc. Re. Ingeniería del Software
M. Eng. Dirección y Gestión de
Proyectos Software (Est. en 2016)

diegojromerolopez@gmail.com
<https://github.com/diegojromerolopez/>
<https://es.linkedin.com/in/diegojromerolopez>



Avisos y exención de responsabilidad

El **contenido** de esta charla es **sólo** refleja **mis puntos de vista e ideas**. No son de ninguna manera las de mi empleador, inteligencia.

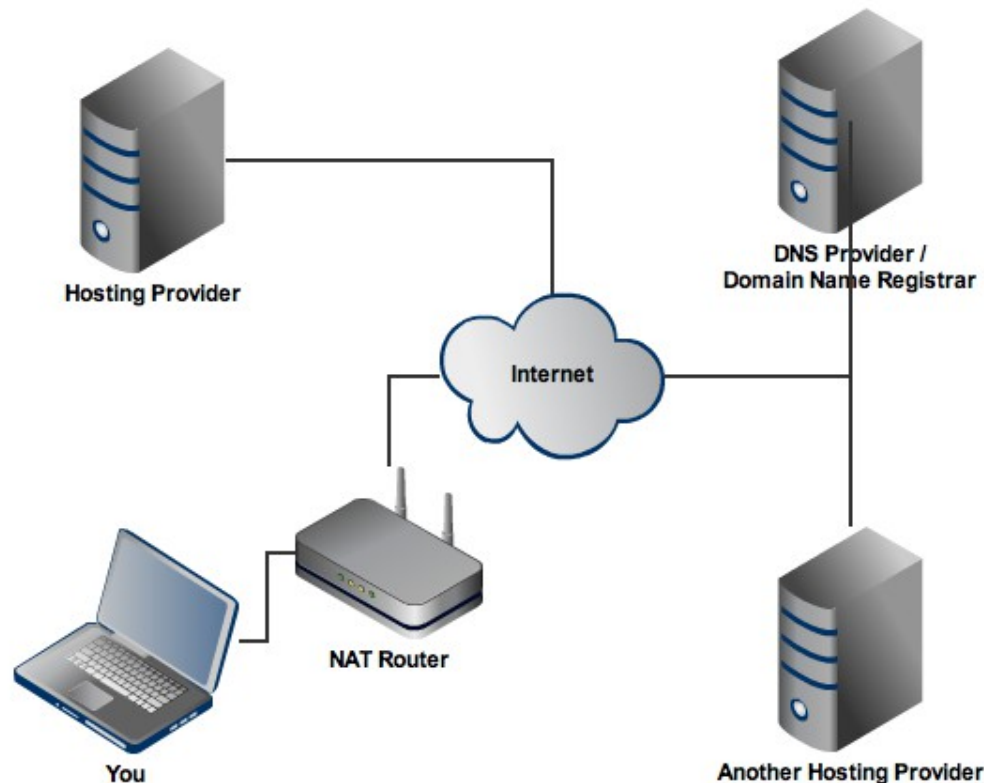
No soy abogado, todos los consejos legales que se dan aquí no han de ser tomados como ciertos desde un punto de vista jurídico y ante la duda recomiendo la visita a un abogado especializado.

Me declaro exento de la responsabilidad de cualquier posible daño o perjuicio causado por el contenido de esta presentación.

2. Qué es internet

Internet: red de redes de computadores heredera de ARPANET.

World Wide Web: sistema de distribución de hipertexto que hace uso de internet.



La web es maravillosa



3. Cómo nos afecta la red

3.1. Procrastinación

Retrasar actividades por otras más placenteras.

Debida a interrupciones constantes y a falta de concentración.

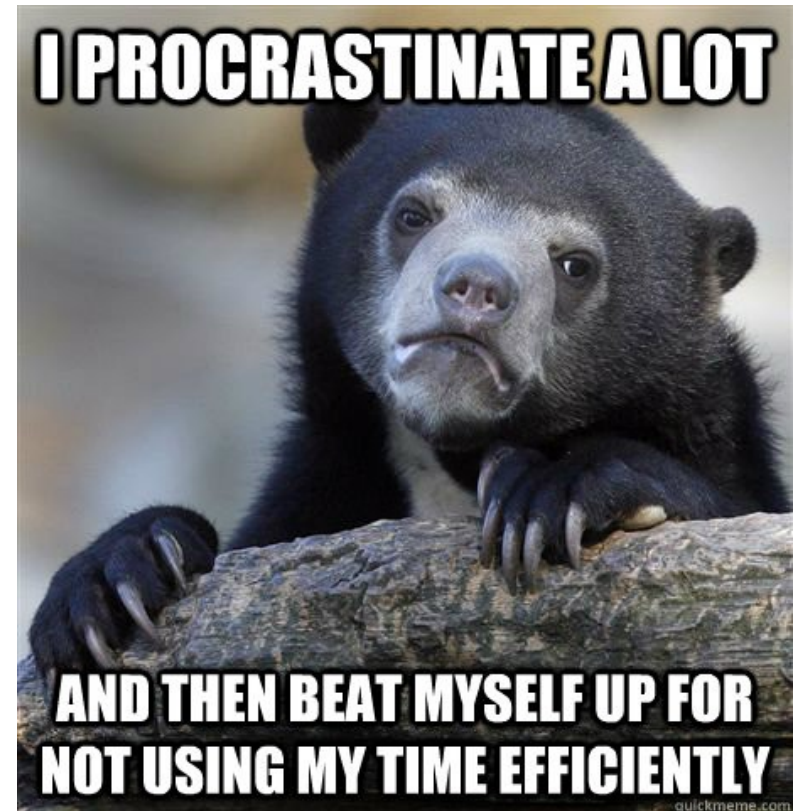
Los mayores causantes son las redes sociales (facebook, twitter, reddit, etc).

Soluciones

Gestión del tiempo (Técnica Pomodoro, Cajas de tiempo)

Descansos adecuados

Bloqueo de webs que nos hacen perder el tiempo.



3.2. Adicción a internet

No reconocido por algunos psiquiatras, sí por otros. Normalmente la adicción no es a “internet” como tal. *Internet proporciona al adicto el contacto con su adicción.*

Las más comunes son adicción a la pornografía, juegos de azar y contenidos.

Residencias de desintoxicación en EE. UU y China.



3.3. Infoxicación

No-intencionada

En un mundo en el que hay tanta información, ¿cuál es la verdadera? ¿cómo seleccionarla? ¿Cuál es la de realmente importante?

Intencionada

Astroturfing.

Generar información falsa, copando el espacio de comunicación hasta hacer creer al otro que lo que se repite es verdad.

Usada de forma maliciosa como arma de guerra (Ucrania).

Soluciones

Busca siempre **la fuente más cercana a la fuente primaria.**

4. Amenazas y peligros en la red

4.1. Automáticas

Amenazas que atacan de forma automática al usuario. No hay una persona detrás.

Software malicioso

Programas que se instalan en nuestro equipo y realizan una de estas acciones:

- Destrucción
- Obtención de información
- Secuestro de información
- Espionaje
- Utilización de recursos de nuestro equipo



Solución: No instalar nada cuya fuente no sea fiable.

¿Cómo acceden a nuestro equipo?

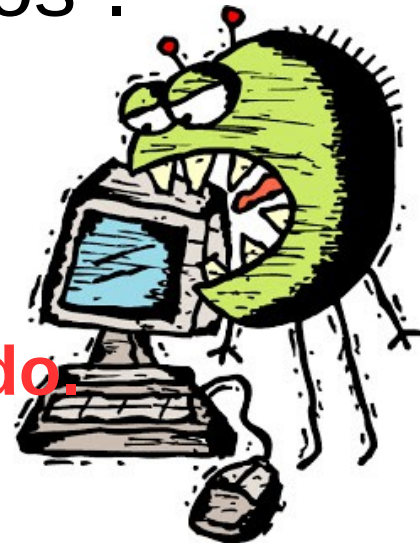
- A través de la red (red local, adjunto en un correo-e, fichero compartido de Dropbox, app móvil...).

¿Cómo se instalan en nuestro equipo?

- Los instalamos nosotros por error.
- Aprovechan vulnerabilidades de nuestro sistema operativo o navegador y se “instalan solos”.

Solución:

- **No instalar nada cuya fuente no sea fiable.**
- **Tener el software de nuestro equipo actualizado.**
- **No tener ficheros compartidos en nuestra red.**



Leyendas urbanas

- × Un sitio web te puede infectar.
 - ✓ A menos que aproveche una vulnerabilidad del navegador no.
 - ✓ Los navegadores en principio son entornos aislados (*sandbox*) que interpretan HTML, CSS, JS, etc.
- × Internet Explorer es el mejor navegador.
 - ✓ Ha tenido fallos de seguridad en repetidas ocasiones.
- × *Mi ordenador ha dejado de funcionar después de meterme en este sitio web.*
 - ✓ Puede que haya ocurrido a la vez, pero *normalmente* no es la causa.

Leyendas urbanas (y 2)

- × No pasa nada por instalar software pirata (eMule, TPB).
 - ✓ **Nadie hace nada gratis**, el software pirata puede llevar “regalos”.

- × No pasa nada por tener un sistema operativo pirata.
 - ✓ El no tener acceso a las actualizaciones de seguridad implica que serás vulnerable a fallos conocidos.

- × Teniendo un software antivirus estoy totalmente protegido.
 - ✓ El software se descarga sólo y exclusivamente del proveedor oficial.

4. Amenazas y peligros en la red

4.2. Humanas

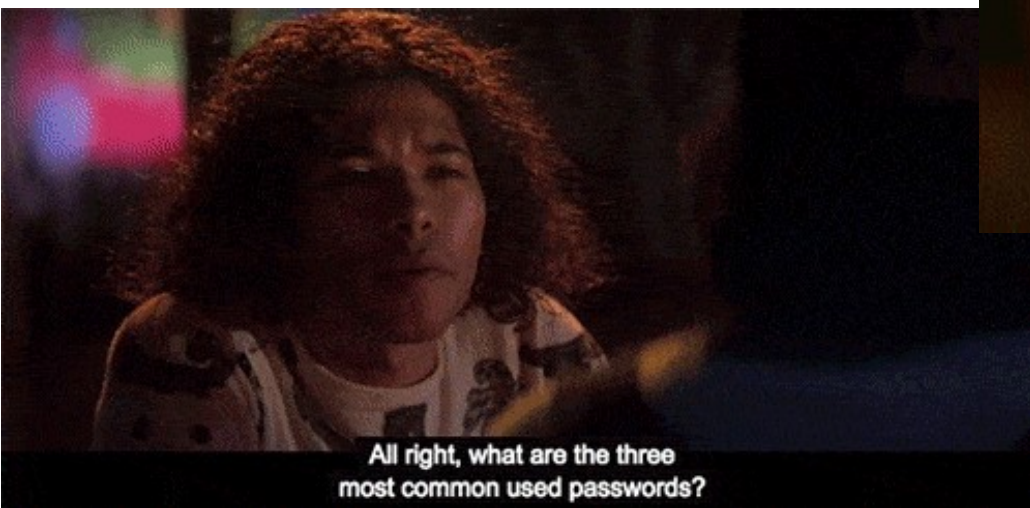
Hackers (White-Hat Hacker)

Humanista en el campo de las ciencias y tecnología con una pasión insaciable por la resolución de problemas complejos.

Crackers (Black-Hat Hacker)

Hacker que usa su talento para su beneficio sin importar las leyes que viole o los principios éticos que rompa.

En la cultura popular esto son hackers



Hackers



Por lo general, los crackers (o piratas cibernéticos) atacan a grandes organizaciones...

Salvo que tomen el control de tu equipo usando un malware y lo conviertan en un **zombi**, pudiéndolo usar para realizar ataques DDOS y otras acciones ilegales.



Volviendo a eso de las “grandes organizaciones”,
¿me tiene que preocupar?

Un sitio web ↔ una contraseña

- ¿Qué contenidos míos tiene cada web?
- Ante una noticia de un ataque a una web, cambiar mis datos personales y si uso esa contraseña en otro sitio, cambiarla.

¿Cómo se producen estos ataques?

Cyberacoso

Acoso en el que se usan medios conectados a la red.

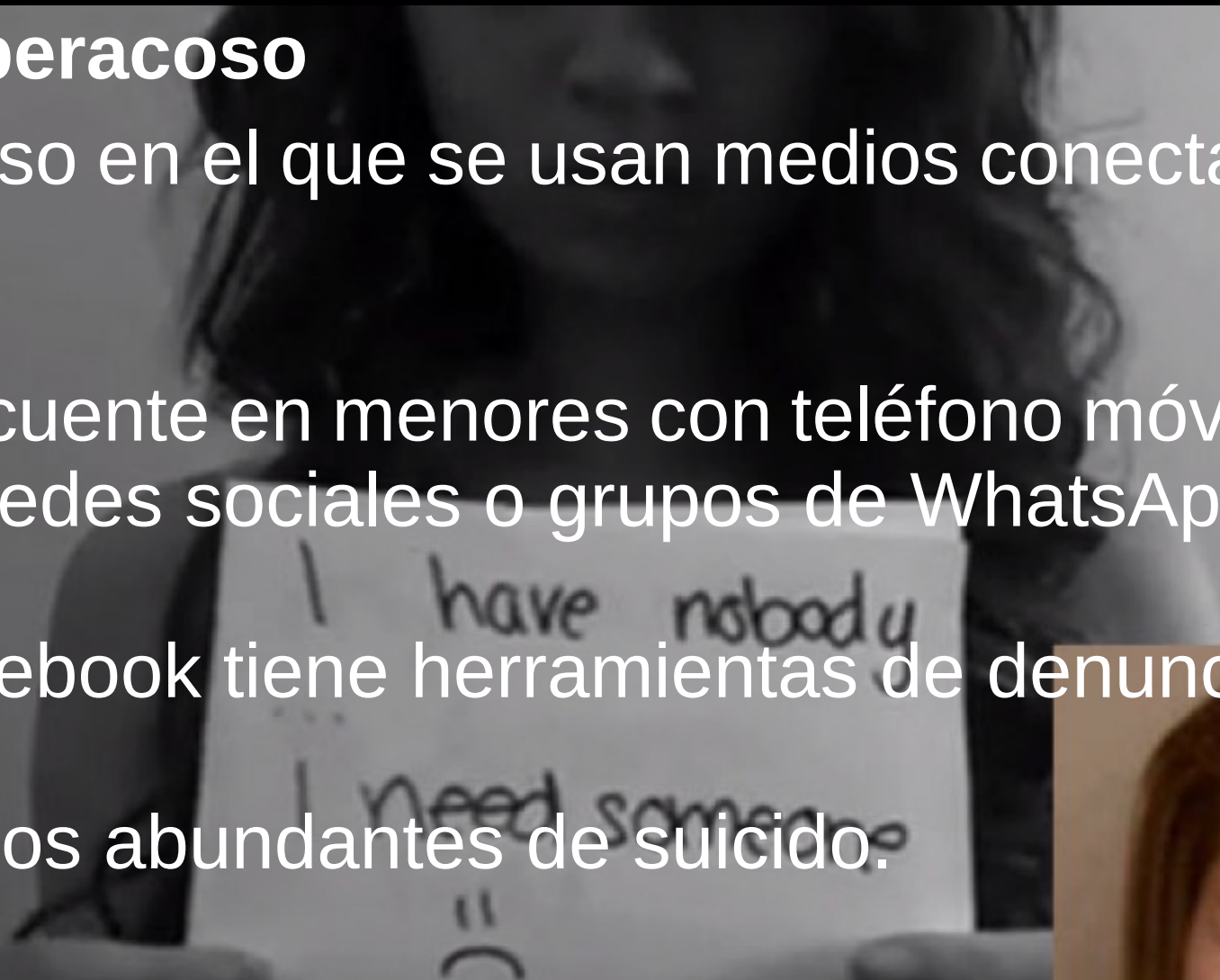
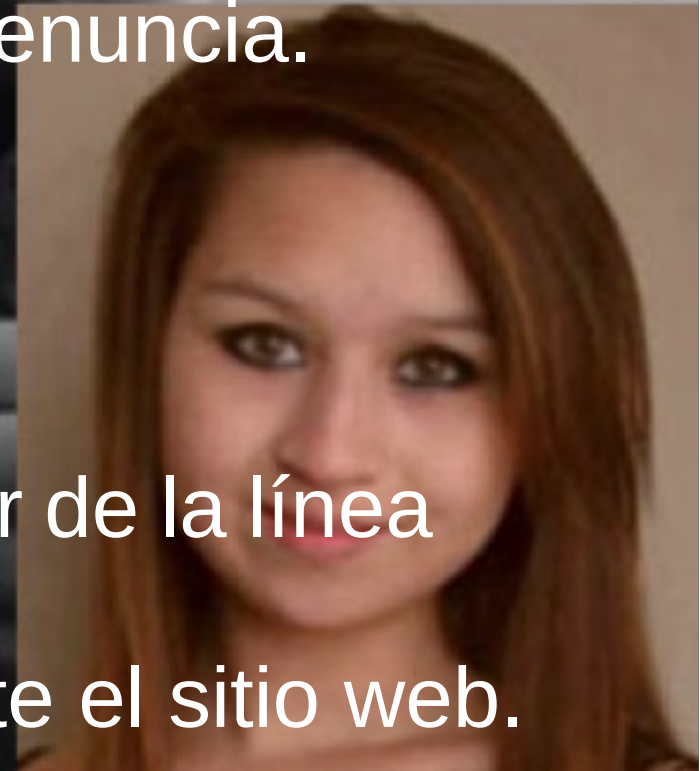
Frecuente en menores con teléfono móvil propio y en redes sociales o grupos de WhatsApp.

Facebook tiene herramientas de denuncia.

Casos abundantes de suicidio.

Solución:

- Denuncia ante CNP o GC al titular de la línea telefónica (o cuenta en RR. SS.).
- Bloqueo de perfiles, denuncia ante el sitio web.



Una forma de cyberacoso: doxing

Publicación de todos los datos públicos de una persona, incluyendo teléfonos, dirección del domicilio, patrones horarios, datos completos de allegados, etc.

Originario de 4chan.



Busca *asustar* a la víctima y que alguien “se tome la justicia por su mano”.

Prevención:

- No publicar NUNCA información personal en redes sociales de forma pública.
- Buscarnos y si en algún sitio hay información pública nuestra, solicitar su retirada.

“Trolling”/“Troleear”

Interacción de una persona para con otra o una comunidad con la intención de provocar una respuesta negativa.

Tan viejo como el mundo.

Busca que la víctima pierda los nervios y mostrarla de una forma negativa. También, busca, crear *discordia* y destruir la comunidad.

Solución:

- Ignorarlos.
- Desenmascararlos como troll.
- Denunciar su usuario.
- Eliminar sus mensajes.



Ingeniería social

Obtención de información usando técnicas de manipulación.

No sólo se da en la red. La red es el medio.

Prevención:

- No se fíe de nadie.



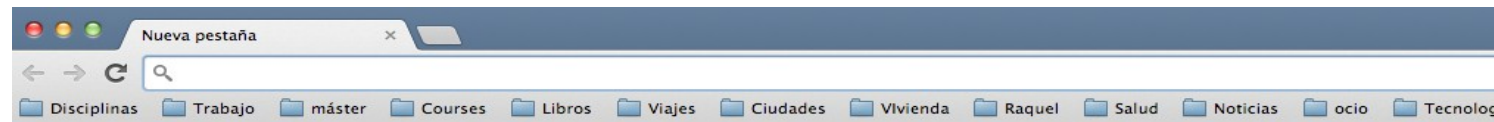
5. Comportamiento seguro en la red

5.1. Modo incógnito

Un olvido de una sesión abierta en un PC público (o que no esté bajo nuestro control [un equipo en el trabajo, por ejemplo]) puede acarreararnos un problema.

No acceder a nuestras cuentas desde equipos ajenos.

Ocultar nuestras *cookies*



Has iniciado una sesión de incógnito

Las páginas que aparezcan en las pestañas de incógnito no se guardarán en el historial del navegador, en el almacén de cookies ni en el historial de búsquedas una vez que hayas cerrado **todas** tus pestañas de incógnito. Se mantendrán los archivos que descargues o los marcadores que crees. [Más información sobre la navegación en modo incógnito](#)



5.2. Usar copias de seguridad *online*

Ante un “desastre” en el equipo, la única solución para recuperar nuestros datos suele ser la copia de seguridad.

Usa un servicio de copia de respaldo:

- Google Drive
- Microsoft OneDrive
- Dropbox

5.3. Bloqueadores de publicidad

Hay sitios que muestran publicidad de contenido pornográfico, juegos de azar, anuncio de instalación de software malicioso, etc

Solución: usar bloqueadores de publicidad.



5.4. Correo electrónico

SPAM

No poner nuestro correo tal cual en internet (para evitar SPAM).

Timo del prisionero español/Nigeriano

Un supuesto acudalado hombre necesita de dinero en metálico pero no puede acceder a su fortuna. Tú eres su última esperanza y si le haces una transferencia, te recompensará en un futuro.

SCAM

Engaño en el que se usa un correo electrónico. Una chica rusa, un piso en alquiler muy barato, etc.

HOAX

Correo en cadena con información supuestamente real.

Correo en cadena

Correo que se envía a muchos contactos como forma de obtención de direcciones de correo electrónico.

5.5. Redes P2P

En España no es ilegal la descarga de contenido bajo derechos de autor para uso privado no lucrativo. Eso sí, puede ser ilícito civil (recordad, esto no es consejo legal).

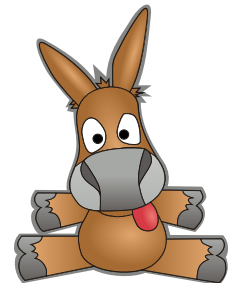
Series/Películas de TV

Usar ThePirateBay.

Red edonkey

Cuidado con los ficheros comprimidos, si contienen contenido ilegal, denunciarlos a la GC.

Cuidado con los *fakes*.



5.6. Redes sociales

Con un poco de búsqueda por internet, he logrado saber mucho sobre la vida de alguna gente. ¿Te imaginas si fuera alguien con malas intenciones?

Consejos:

- Mínimo contenido público.
- No tener fotos comprometidas ni en público, ni en privado, ni compartidas. **Que no existan.**
- No escribir mensajes ofensivos o comprometidos.
- Antes de escribir, pensar que eso que escribimos nos define como persona.

5.7. Menores de edad

Muy influenciables por el contenido y usuarios maliciosos (hay redes de captación de niños).

Navegación con presencia paterna.

Horarios de uso del equipo “normales”.

Contrato entre padres e hijos para el uso de internet.

Nada de teléfono 3G ni de PC en su habitación.

Los CEO de empresas del *Silicon Valley* son de esta opinión.

6. Conclusiones

Internet es como la vida, hay cosas buenas y malas.

Hay que estar atento y saber qué se está haciendo. Leerlo todo muy bien y comprenderlo.

Desconfiar por defecto.

No instalar software de cuyo origen no se confía.

7. ¿Más preguntas?



Muchas gracias por vuestra atención

