# El lado oscuro de la red


Diego J. Romero López
Ingeniero Software en intelligenia
diegojromerolopez@gmail.com

# Índice

# Índice (y 2)

# Índice (y 3)

# 1. Presentación


## Diego J. Romero López

**Ingeniero de Software**


Especializado en desarrollo web en **intelligenia**

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, intelligenia.

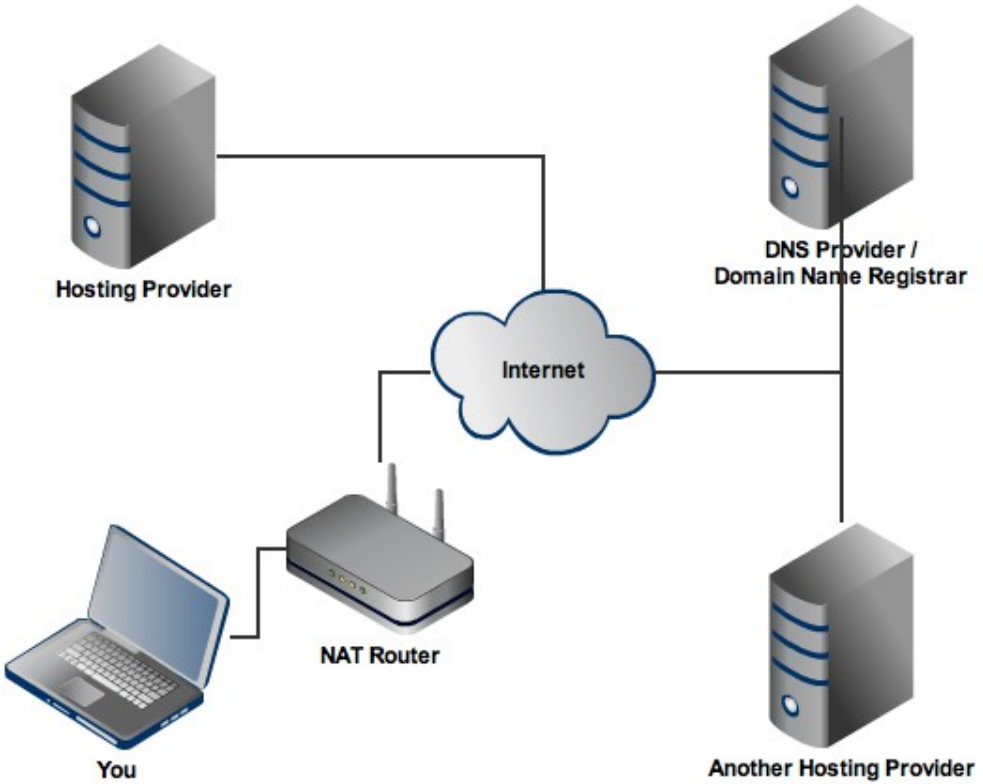
**No soy abogado**, todos los consejos legales que se dan aquí no han de ser tomados como ciertos desde un punto de vista jurídico y ante la duda recomiendo la visita a un abogado especializado.

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

# 2. Qué es internet

## 2.1. Definiciones

**Internet**: *Red de redes de computadores heredera de ARPANET.*



**World Wide Web***: parte de internet accesible a través del protocolo HTTP (S).*

**Protocolo**: “idioma” de comunicación entre equipos conectados a una red.

**Recurso**: cualquier cosa que tenga una URL: imágenes, vídeo, ficheros HTML, etc.

**Navegador**: programa que interpreta recursos y los muestra de forma “amigable”.

**Servidor web**: programa que entrega recursos que pide un navegador.

# 2.2. Historia

- **1969-1980**
  - Desarrollo de ARPANET (inicio de TCP/IP).
  - Multitud de protocolos y redes de comunicación
- **1980s**
  - Definición completa de TCP/IP (1982)
  - Tim Berners-Lee
    - Invención del concepto de hipervínculo
    - Servidor web
    - Navegador web
  - Morris Worm
- **1990**
  - Popularización de internet.
  - eBay
  - Google
  - Yahoo

# 2.2. Historia (y 2)

- **2000**
  - Explosión de la burbuja .com
  - Tecnologías de conexión 3G
  - Skype
  - Bittorrent
  - Facebook
  - Iphone
  - Android
  - Google Docs
  - Reddit
  - Wikileaks
- **2010s**
  - Coursera
  - Popularización de los smartphones con 3G.

# Internet es maravilloso




Online Banking

YouTube

Google



YAHOO!




peer2peer

WIKIPEDIA
The Free Encyclopedia

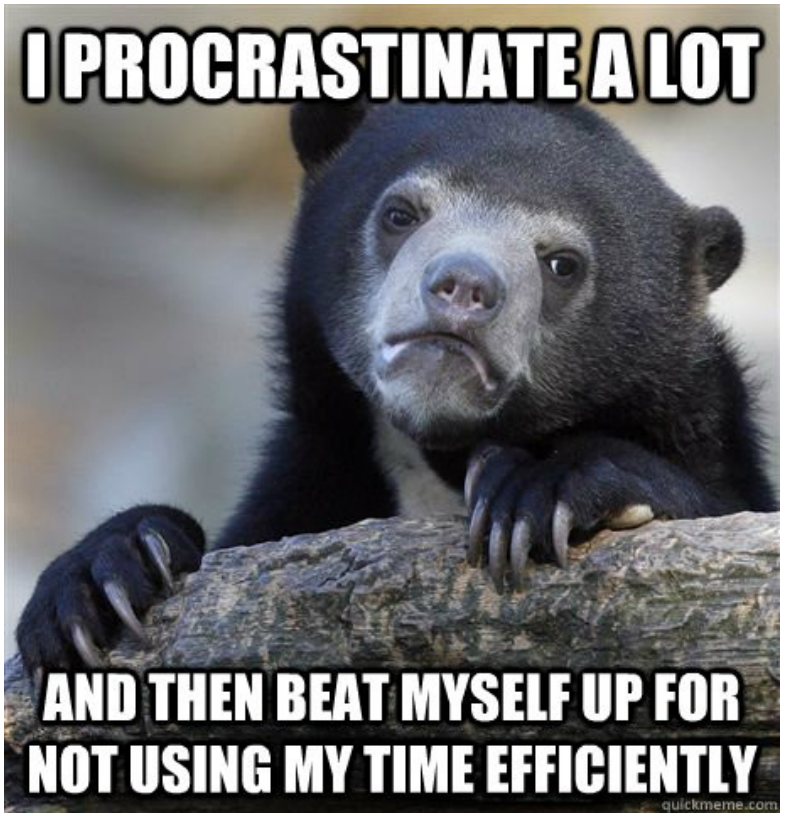
amazon

BitTorrent

# 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.

**Soluciones**
Consultar con especialista.


CBSNEWS Video | US | World | Politics | Entertainment | Health | MoneyW

CBS NEWS / *September 5, 2013, 5:16 PM*

# Hospital-based Internet addiction center to open

# 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.

# Hackers

# En la cultura popular esto son 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?

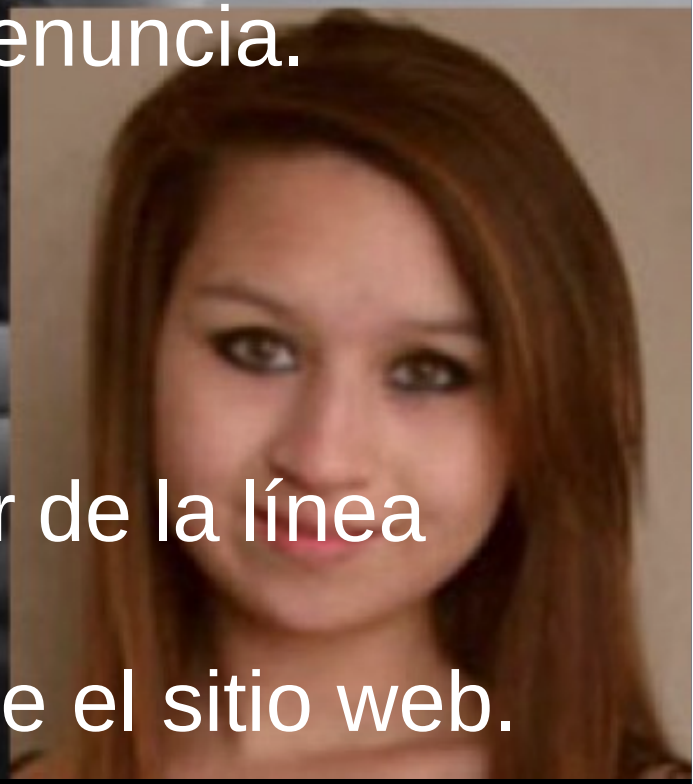
## Cyberacoso

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 suicido.



**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.

## 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”/“Trolear”**

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.

## Deep-web

Red cifrada de equipos basada en el protocolo P2P TOR (The Onion Network).

Usada por criminales:

- Compra-venta de drogas/armas.
- Asesinatos a sueldo
- ...

**Solución**:

- Las fuerzas y cuerpos de seguridad del estado están monitorizando esta red.
- No meterse nunca.

**Contenido peligroso**

Contenido que genera estrés post-traumático al verlo.

La web sólo aloja este contenido, no lo produce.

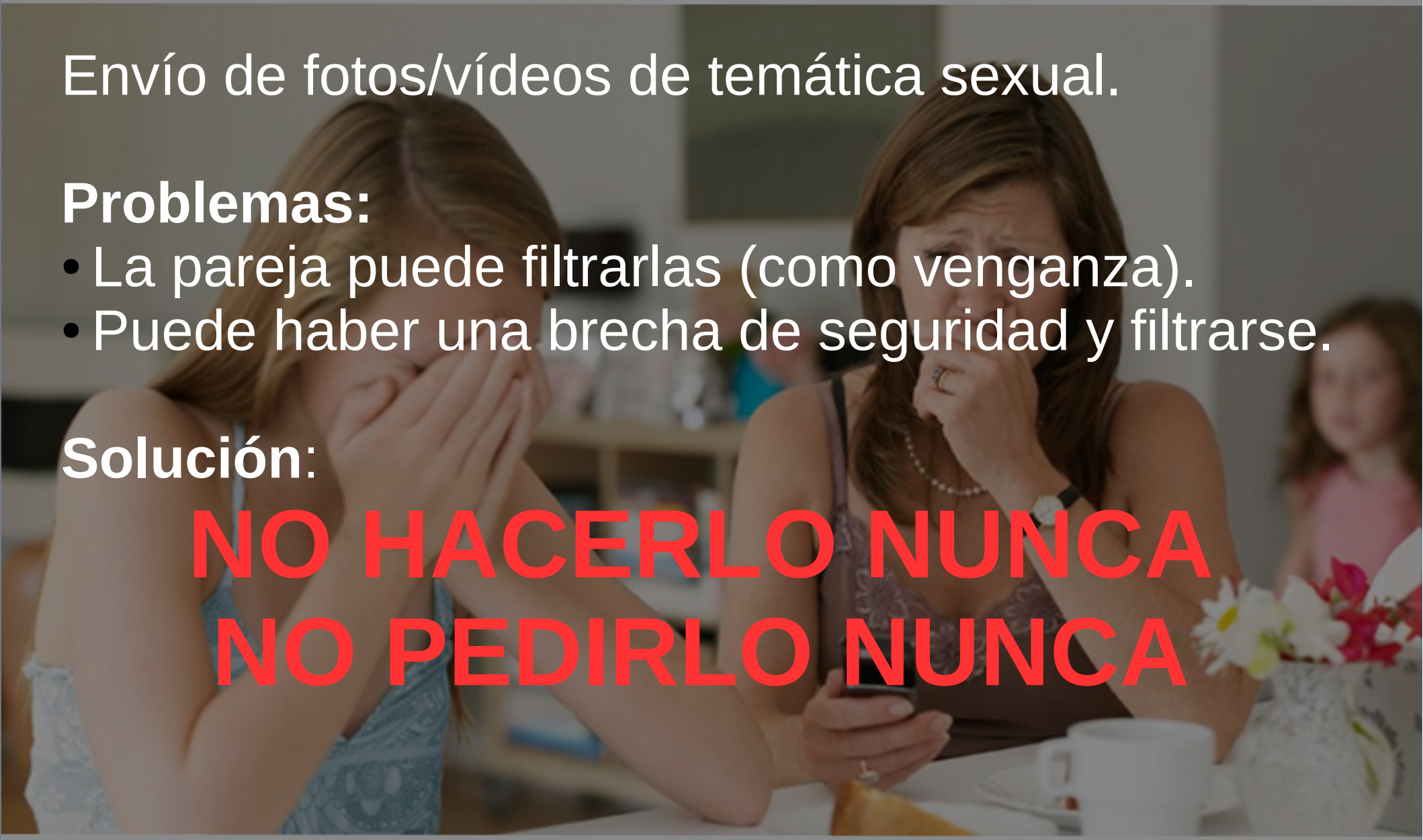
Muchas veces, enlazado *for the loolz,* no por malicia.

**Ejemplo**: vídeos de accidentes mortales (*liveleak*), fotos de fallecimientos, textos mórbidos, etc...

**Solución**:

- Tener cuidado con lo que se ve.
- Evitar contenido NSFW y sobre todo NSFL.

# Sexting



Envío de fotos/vídeos de temática sexual.

**Problemas:**

- La pareja puede filtrarlas (como venganza).
- Puede haber una brecha de seguridad y filtrarse.

**Solución**:

**NO HACERLO NUNCA**

**NO PEDIRLO NUNCA**

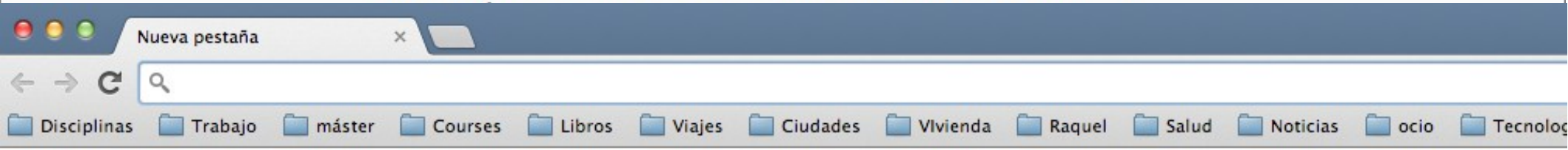
# 5. Comportamiento seguro en la red

## 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 acarrearnos un problema.

No acceder a nuestras cuentas desde equipos ajenos.

Ocultar nuestras *cookies* (reserva de vuelos y alojamientos).

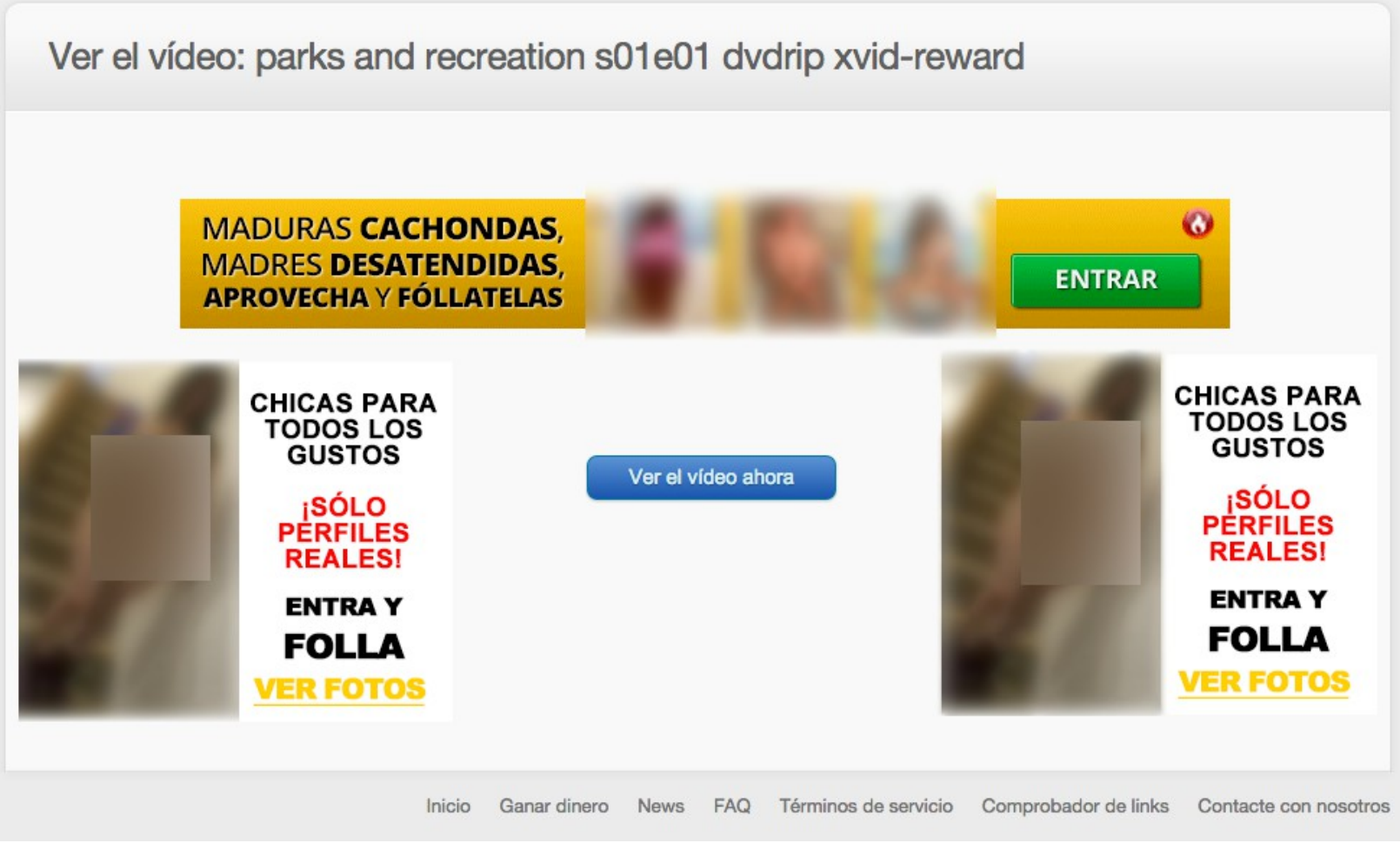




## Has iniciado una sesión de incógnito

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. Bloqueadores de publicidad

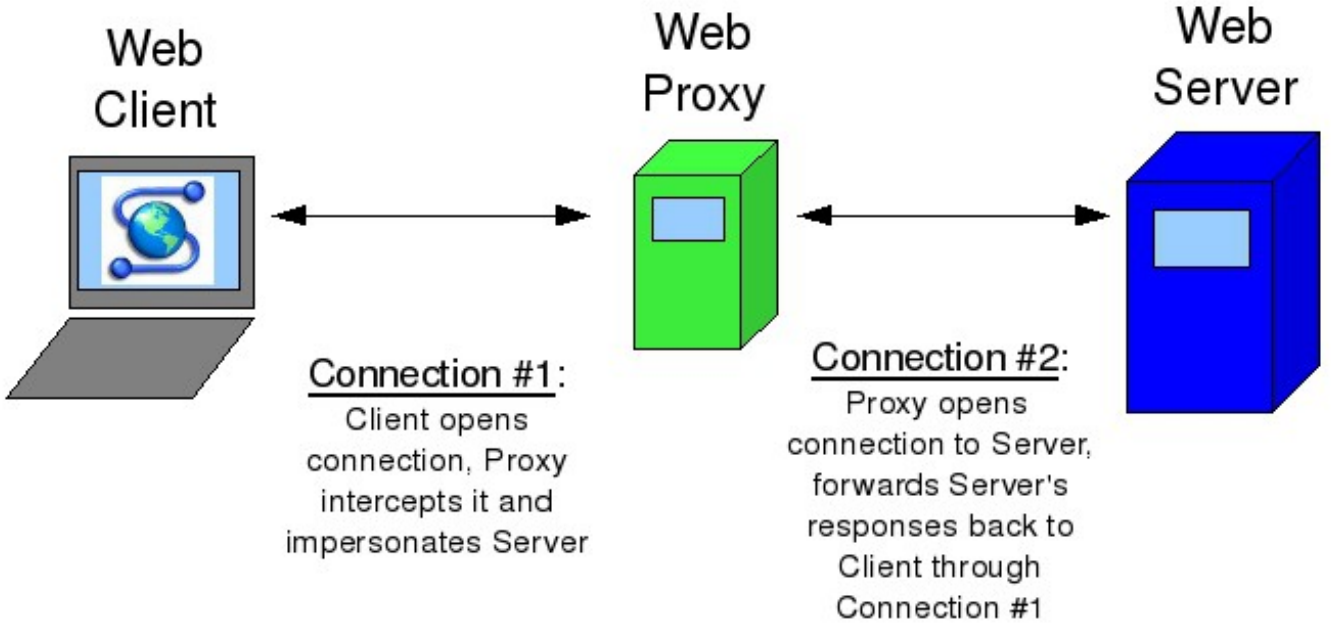
Hay sitios que muestran publicidad de contenido pornográfico. Usar *adblock* u otro bloqueador de publicidad.



# 5.3. Proxies

Hay servidores en internet que proporcionan la funcionalidad de reenviar nuestras peticiones y podemos hacer uso de ellos como “servidores pantalla”.

Si vamos a usar uno, NUNCA iniciar sesión o introducir datos sensibles.



Para evitar saberse qué servidores proxy están activos, hay extensiones que gestionan esto de forma automática:

- ZenMate de Google Chrome que además es VPN.
- FoxyProxy de Mozilla Firefox


# 5.4. Correo electrónico

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

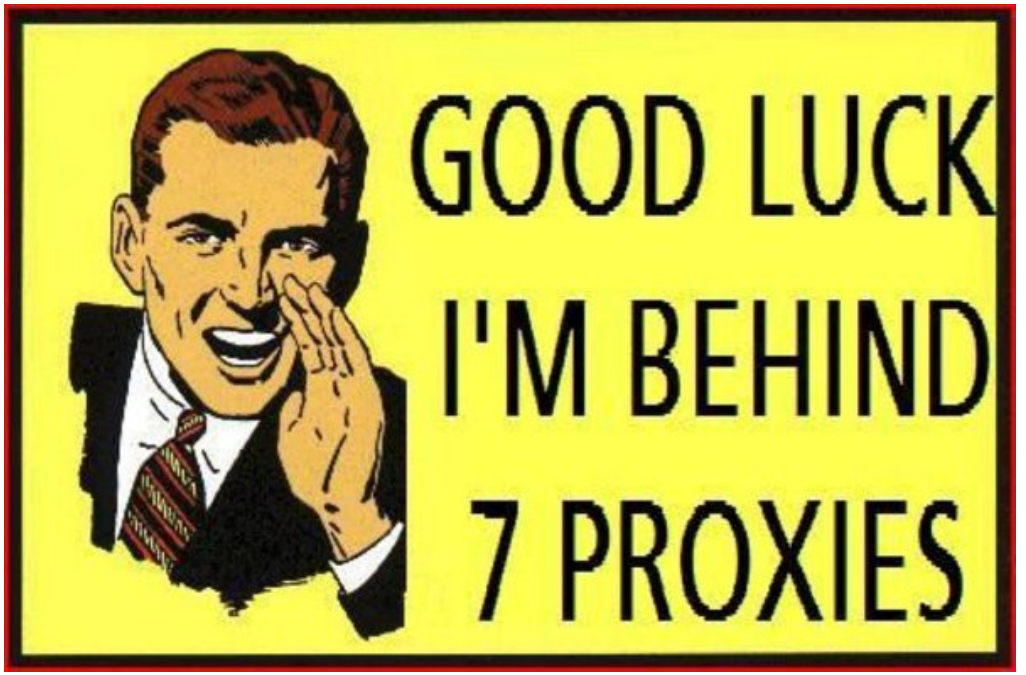
**Timo del prisionero español/Nigeriano**
Un supuesto acudalado hombre necesita de dinero en metálico pero no puede acceder a su fortuna. Tú eres su última esperanza y si le haces una transferencia, te recompensará en un futuro.

**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.

Este mecanismo es usado por los piratas para evitar ser detectados.

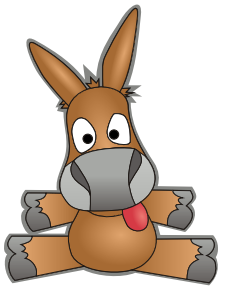


# 5.5. Redes P2P

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 PopcornTime.

**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.

Se dice “humorísticamente” hablando que, *en internet las mujeres son hombres, los hombres son niños, y los niños la policía.*

# 6. Consejos generales

## 6.1. Copias de seguridad

Un fallo hardware, un robo o la destrucción de los datos nos puede arruinar un muchas horas de trabajo.

Usar un sistema de copias de seguridad...

¿En la nube? Sí, si no subes información confidencial. Asume que la NSA lo va a analizar:

- Google Drive
- Microsoft SkyDrive
- Dropbox

Información confidencial:

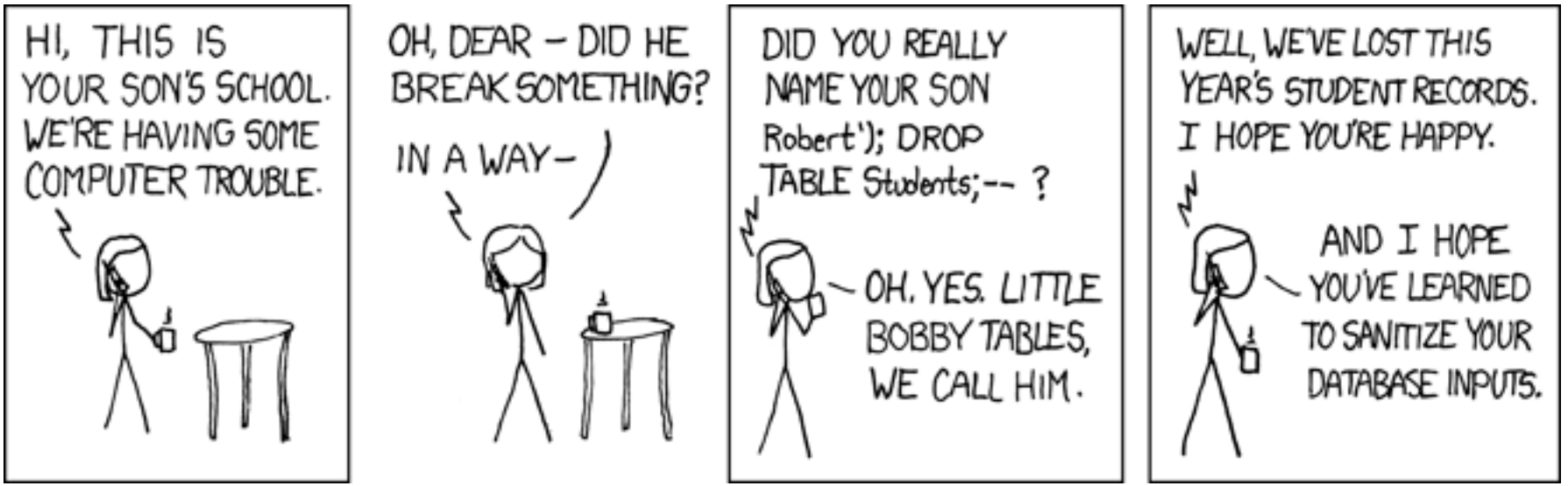
- Varios *pendrive* en lugar seguro.
- Varios discos duros en lugar seguro.
- Ficheros cifrados en la nube (o en local con PGP).

Lo más importante de las copias de seguridad es la **redundancia de la información**.

# 6.2. Mis datos en internet

¿Quién tiene datos míos en internet?

**¿Qué pasa si atacan ese sitio? ¿Son privados mis datos? ¿Tengo copias de seguridad?**



# 6.3. Sistemas operativos

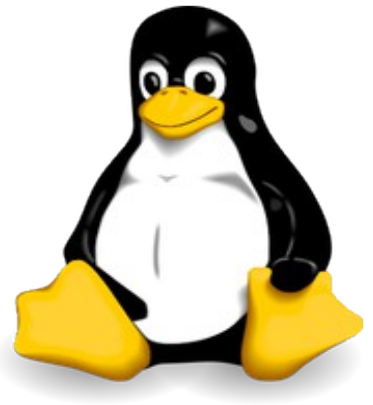
MacOS y Ubuntu tienen menos fallos de seguridad que Windows.

MacOS y Ubuntu tienen menor público por lo que hay menos software malicioso para ellos.

Ubuntu es **gratuito**.

**No usar nunca un Windows pirata. ES DELITO.**





## 6.4. Instalación de software

¿Quién es el autor? ¿Nos da confianza? ¿Tiene buenas opiniones?

¿Qué hace?

¿Qué permisos requiere (si es una aplic. Móvil)?

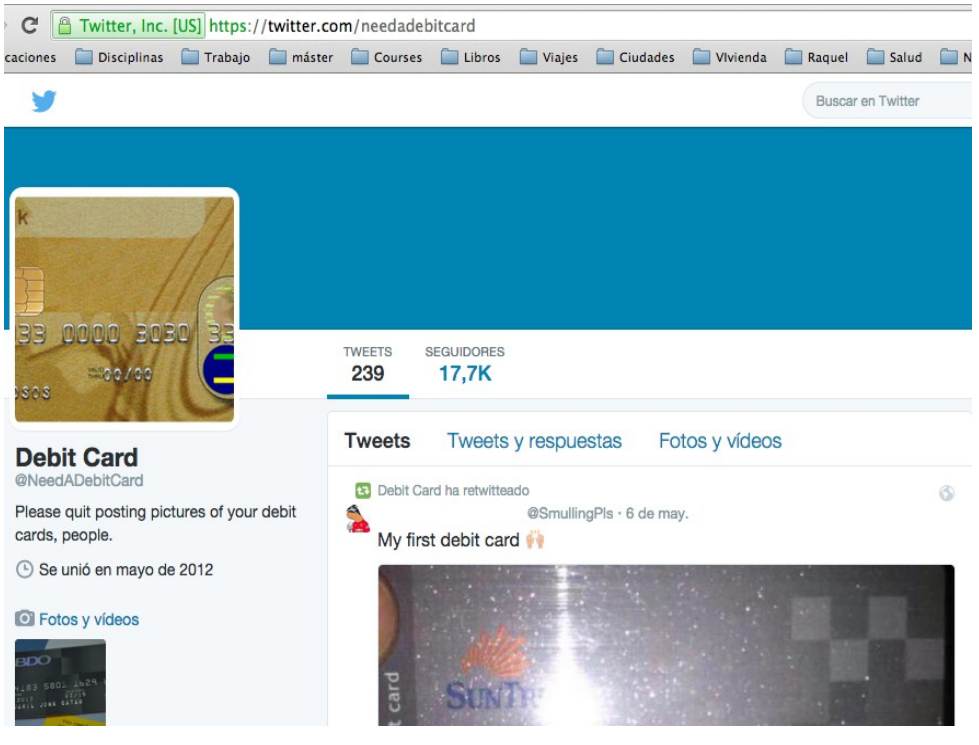
¿De dónde lo hemos descargado?

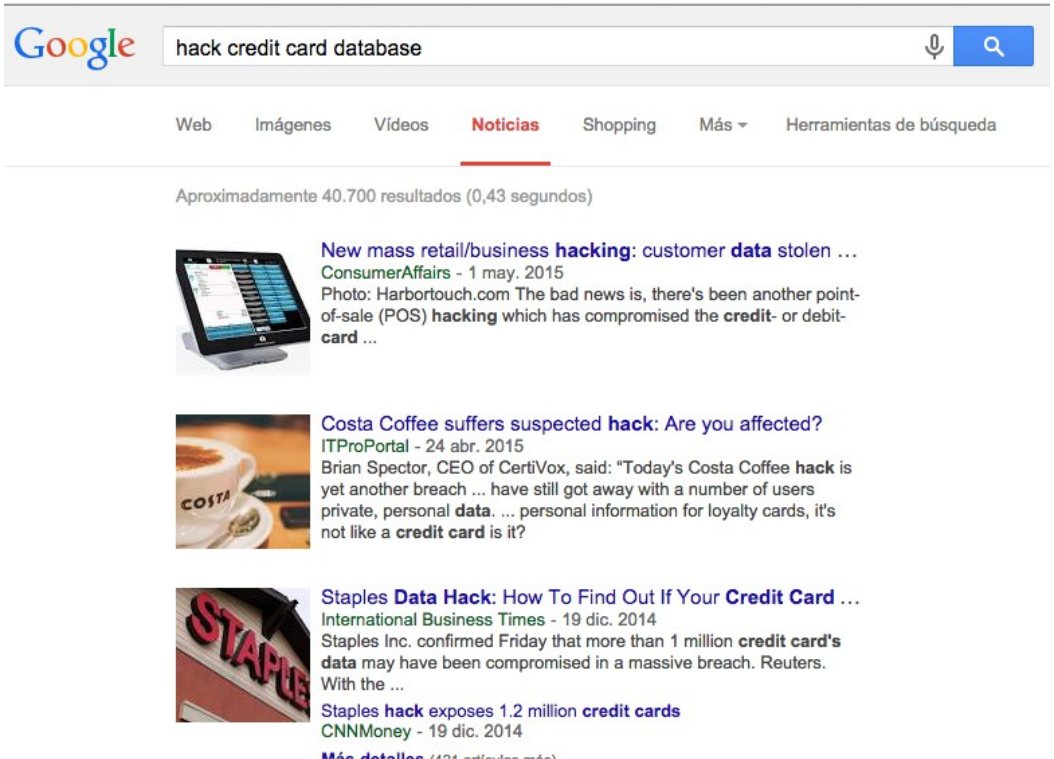
¿Es código abierto, software libre, software privativo? ¿Si es privativo, estoy pagando una licencia? ¿Es software pirata?

# 6.5. Pago *online*

No comprar cosas a tiendas poco conocidas. Confiar sitios con buena reputación. Buscar información sobre ellos en la web, principalmente opiniones.

No introducir tarjeta en ningún sitio desconocido.



Comprobar nombre del propietario de ese TPV.

Si hay un error en el pago no pasa nada, la operación se cancela y el dinero o se devuelve o ni siquiera ha sido transferido. Normalmente hay un límite de 5 min. por compra.

Puede que nuestra tarjeta no admita pagos por internet. Si la operación falla varias veces, ir a nuestra sucursal.

Revisar importe antes de pagar.

Revisar que se está en una conexión **https**.


Comprobar que la web del banco es la real, cuidado con el *Phising*.

No hacer grandes compras si no es un sitio de extrema confianza (amazon.es, por ejemplo).

**El pago por TPV virtual bancario es seguro.**

# 7. 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.

# 8. Preguntas

# Muchas gracias por vuestra atención