Navegando por Internet de forma segura: riesgos, buenas prácticas y herramientas

Ricardo J. Rodríguez

rjrodriguez@unizar.es

Centro Universitario de la Defensa Zaragoza

7 de febrero, 2018

Jornadas de Internet Segura

Facultad de CCSS y del Trabajo, Universidad de Zaragoza

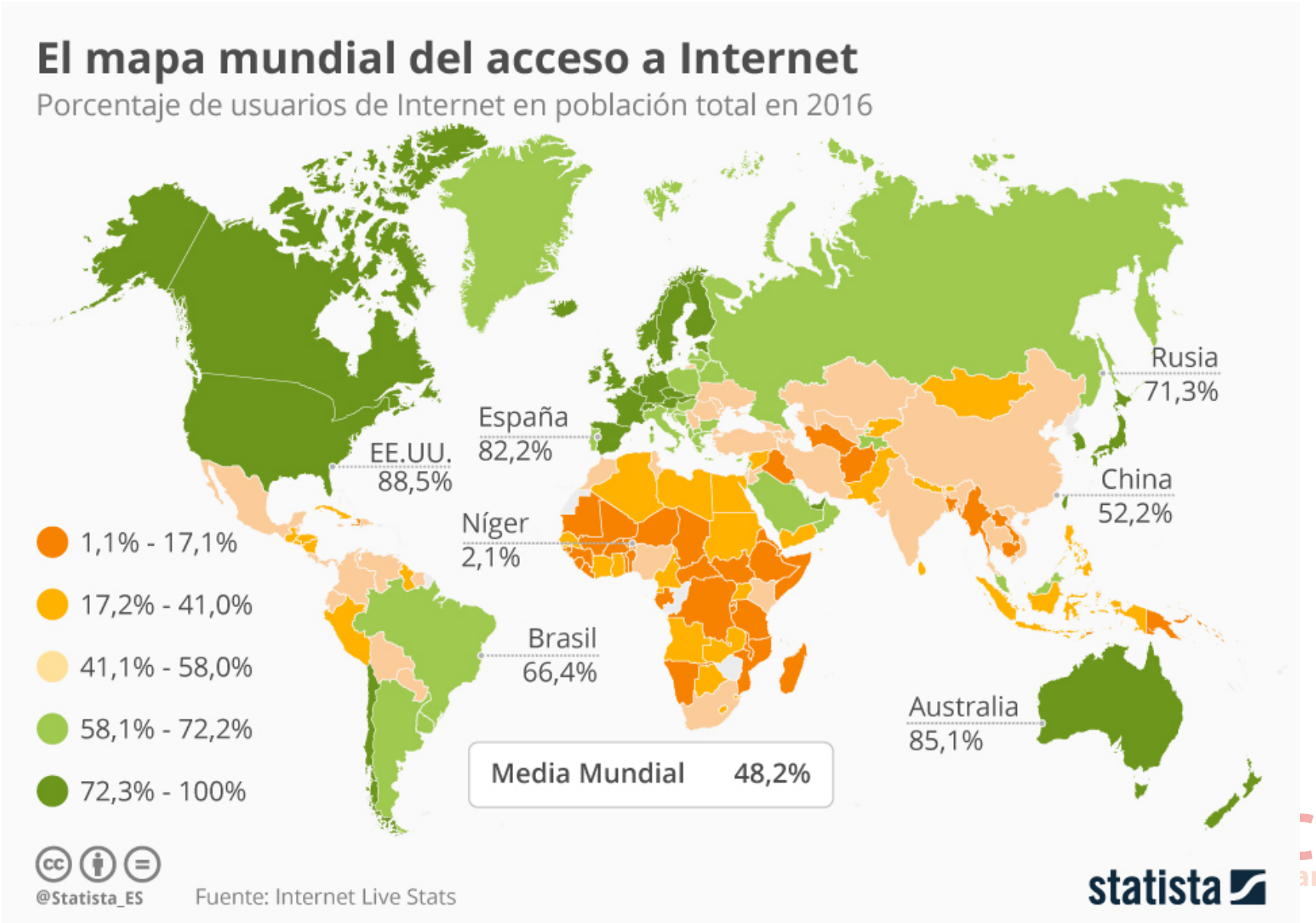
$whoami

- Miembro de CLS (2001)
- **Ph.D. en Informática** (2013)
- Profesor Ayudante Doctor en Centro Universitario de la Defensa, Academia General Militar (Zaragoza)
- Líneas de investigación
  - Security-(performance/safety-)driven engineering
  - Análisis de malware
  - Seguridad RFID/NFC
- No procesado ¨‿
- Ponente/trainee habitual en conferencias del sector de seguridad informática

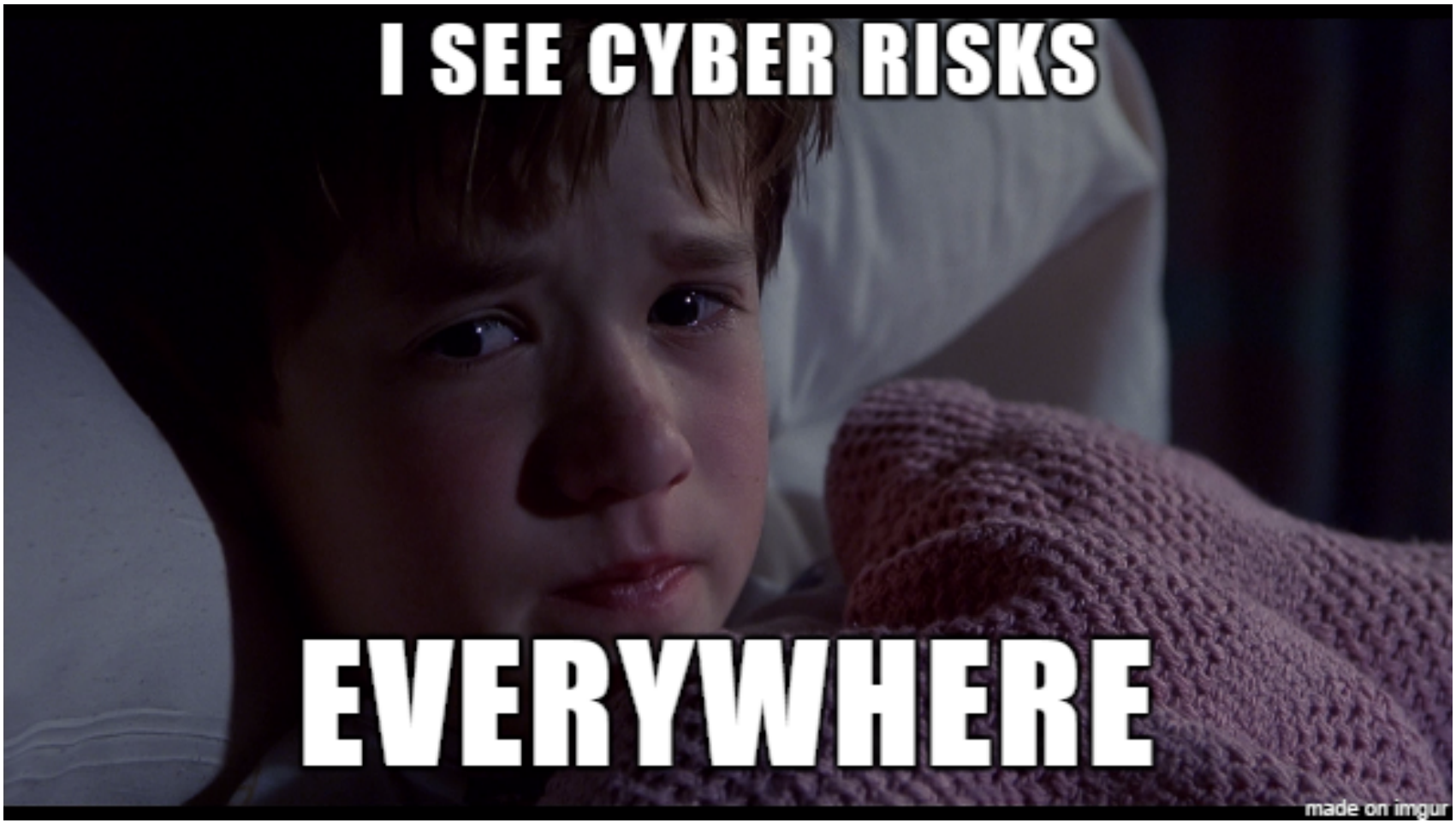
CUD Zaragoza

Introducción

Internet, la red de redes

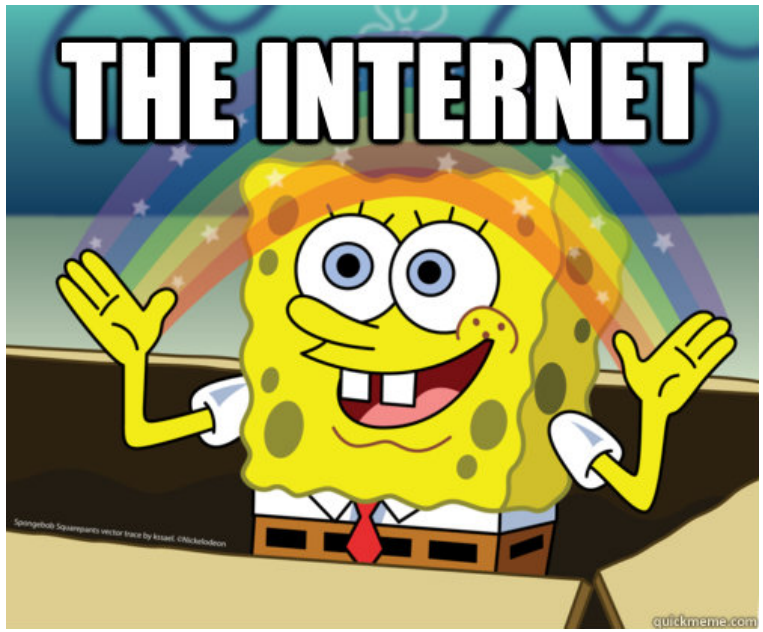


Introducción



Introducción

Internet, la red de riesgos



- **Seguridad**
  - **Cibercrimen**: malware, fraudes de pago, robo de información, etc.
  - Ciberterrorismo
  - Otros: coerción sexual, extorsión de menores, acoso, etc.
- **Privacidad**
  - Redes sociales (*sé lo que hiciste el último sábado. . .*)
  - Datos personales
  - *Profiling* (usando nuestra traza de actividad en Internet)

Introducción

- **Navegación segura**
- **Conectividad segura**
- **Buenas prácticas**

Introducción

- **Navegación segura**
- **Conectividad segura**
- **Buenas prácticas**

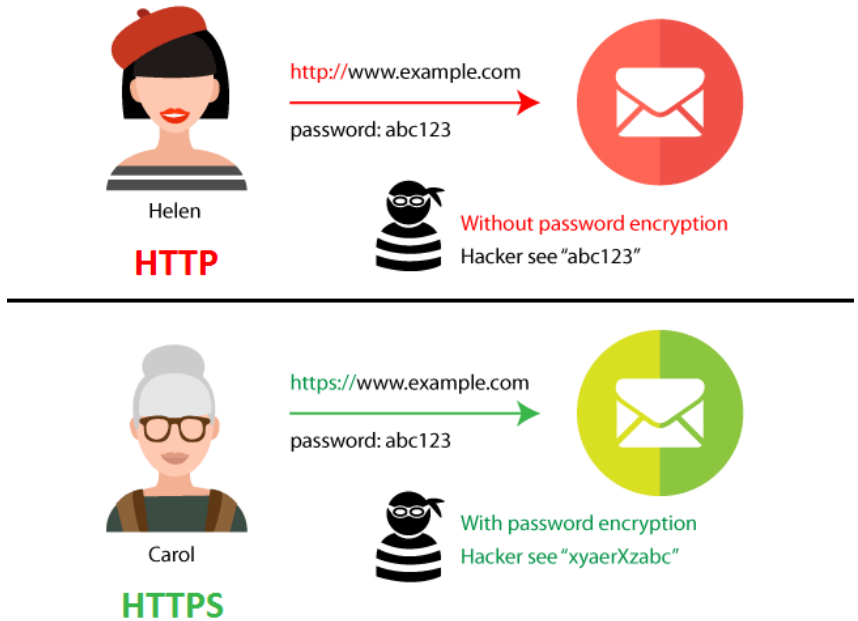
Agenda

1. Navegación segura
2. Conectividad segura
3. Otras buenas prácticas
4. Conclusiones

Agenda

Navegación segura

HTTP vs. HTTPS



- Hyper Text Transfer Protocol vs. Hyper Text Transfer Protocol **Secure**
- **Conexión cifrada** entre el servidor y el navegador
  - El "candadito" de la barra de direcciones
- **Certificados SSL/TLS**. Aspectos a considerar:
  - Cadena de confianza (verificación de autenticidad)
  - Emitidos por una autoridad reconocida
  - Período de validez

Navegación segura

HTTP vs. HTTPS

- Muchos servicios HTTP **redireccionan automáticamente** al mismo servicio, pero sobre HTTPS
  - Ejemplos: Google, Wikipedia, Twitter, . . .
  - **Debería de ser obligatorio**
- Cambio de **política de los navegadores en el último año**: reforzamiento positivo vs. reforzamiento negativo
  - Aviso cuando la conexión **no es segura**
  - En algunos casos, incluso, el navegador no permite la conexión

Si es posible elegir, visitad siempre la web con el "candadito"

Navegación segura

HTTP vs. HTTPS – demos

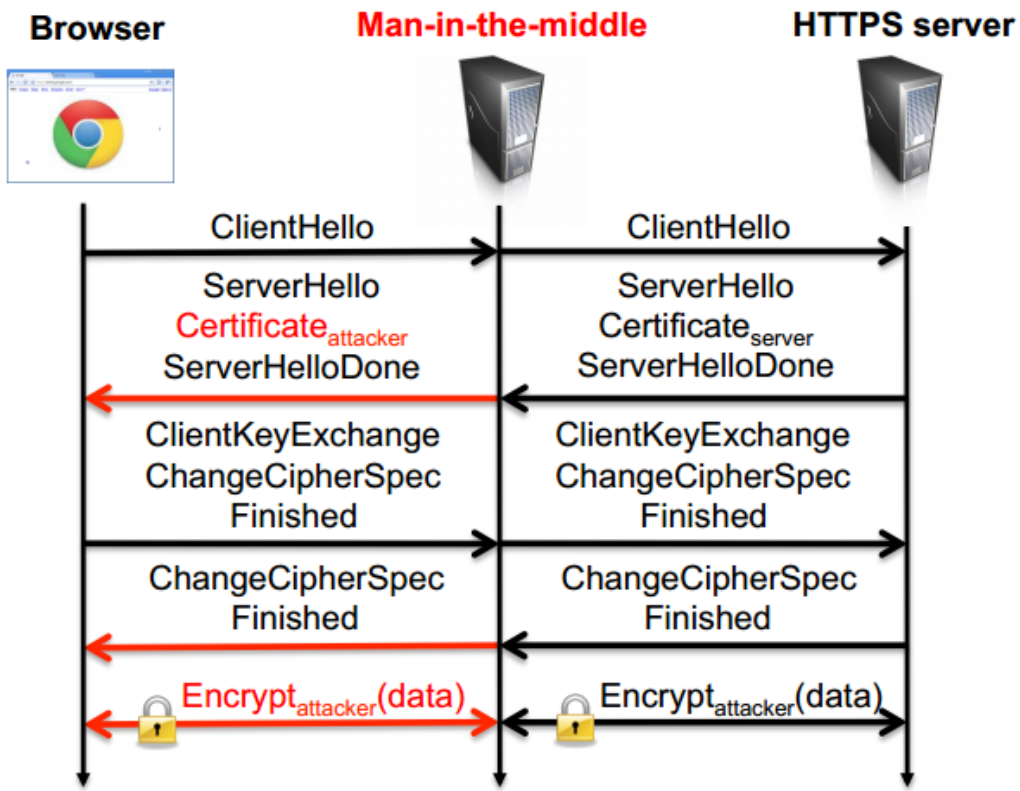
1. *HTTP vs. HTTPS: ejemplo práctico*
2. *Chequeo de propiedades de certificados en diferentes webs y navegadores*

Navegación segura

HTTP vs. HTTPS

¿Por qué es importante (algunas veces) verificar las propiedades?

- HTTPS por sí mismo no previene de posibles fugas de información: **ataques *man-in-the-middle* con certificados comprometidos**

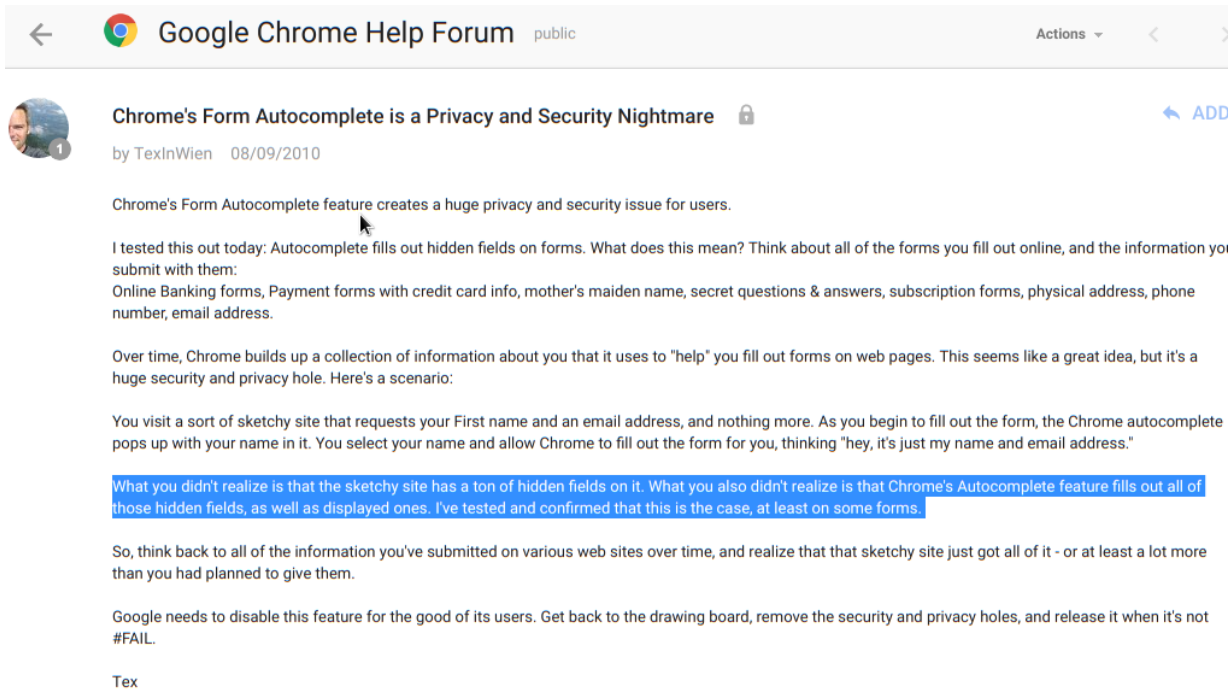


Fuente: `http://resources.infosecinstitute.com/cybercrime-exploits-digital-certificates/`

Navegación segura

Autocompletación de formularios

- Diferente web, quizás primera visita: ¿por qué funciona el autocompletar?
  - Nombres de los campos del formulario idénticos (e.g., “name”, “email”, etc.)
- **Problema**: algunos campos del formulario pueden ser ocultos y solicitar más información al navegador. ¡El autocompletar la proporciona encantado!



Google Chrome Help Forum public Actions

Chrome's Form Autocomplete is a Privacy and Security Nightmare

by TexInWien 08/09/2010

Chrome's Form Autocomplete feature creates a huge privacy and security issue for users.

I tested this out today: Autocomplete fills out hidden fields on forms. What does this mean? Think about all of the forms you fill out online, and the information yo submit with them:
Online Banking forms, Payment forms with credit card info, mother's maiden name, secret questions & answers, subscription forms, physical address, phone number, email address.

Over time, Chrome builds up a collection of information about you that it uses to "help" you fill out forms on web pages. This seems like a great idea, but it's a huge security and privacy hole. Here's a scenario:

You visit a sort of sketchy site that requests your First name and an email address, and nothing more. As you begin to fill out the form, the Chrome autocomplete pops up with your name in it. You select your name and allow Chrome to fill out the form for you, thinking "hey, it's just my name and email address."

What you didn't realize is that the sketchy site has a ton of hidden fields on it. What you also didn't realize is that Chrome's Autocomplete feature fills out all of those hidden fields, as well as displayed ones. I've tested and confirmed that this is the case, at least on some forms.

So, think back to all of the information you've submitted on various web sites over time, and realize that that sketchy site just got all of it - or at least a lot more than you had planned to give them.

Google needs to disable this feature for the good of its users. Get back to the drawing board, remove the security and privacy holes, and release it when it's not #FAIL.

Tex

Ejemplo: `https://i.kinja-img.com/gawker-media/image/upload/tvg8bbgqdrj9gkuh97g0.gif`

Desconfiad de los formularios autocompletados

Navegación segura

Redirecciones JavaScript

- JavaScript (JS): lenguaje de programación web
  - Ejecución en el lado cliente (scripts). Es decir, **tu navegador**
- Fuente de **múltiples vulnerabilidades y problemas no deseados**

- Muy usado en el cibercrimen: **redirección a páginas maliciosas** que identifican navegador y sistema operativo, y si pueden, explotan alguna vulnerabilidades
- **Redirección a páginas de ads** (publicidad)
- Habitual en páginas web que sirven contenidos con PI de manera gratuita

Se puede evitar instalando:

- ***Bloqueadores de scripts JS (uBlock Origin, AdBlock, etc.)***
- ***Cambiadores de* User-Agent *del navegador***

CUD Zaragoza

Navegación segura

Redirecciones JavaScript – demos

1. Detección de navegador:

   `http://vagabundia.blogspot.com/2010/02/detectar-el-navegador-de-los-visitantes.html`;

   `http://ejemplocodigo.com/ejemplo-php-detectar-navegador-de-los-visitantes/`

2. *Redirecciones JS (en función del navegador)*: `http://1337x.to/`

Navegación segura

Cookies

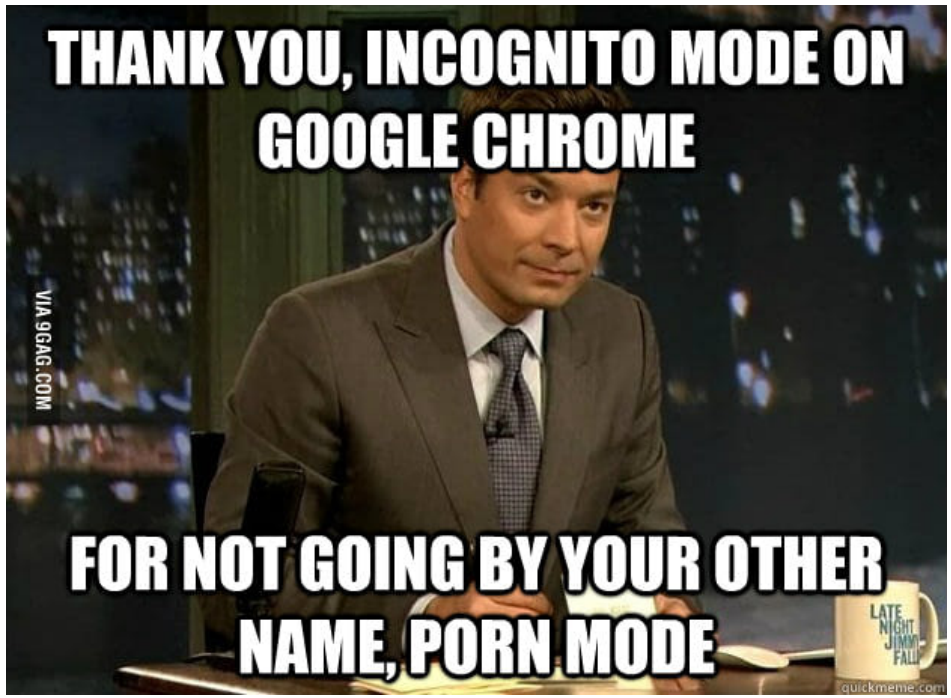
- **Pequeño "rastro" en el dispositivo de la actividad en Internet**
  - ¿Privacidad?
- Servicios web obligados (*EU Cookie Law*) a avisar que guardan una cookie (el almacenamiento sucede en el lado del cliente)
- Pueden ser de **autenticación**: nuestra sesión ya está iniciada la siguiente vez que accedemos al servicio web
  - **Problema: robo de cookies**

Navegación segura

Cookies – navegación en modo incógnito

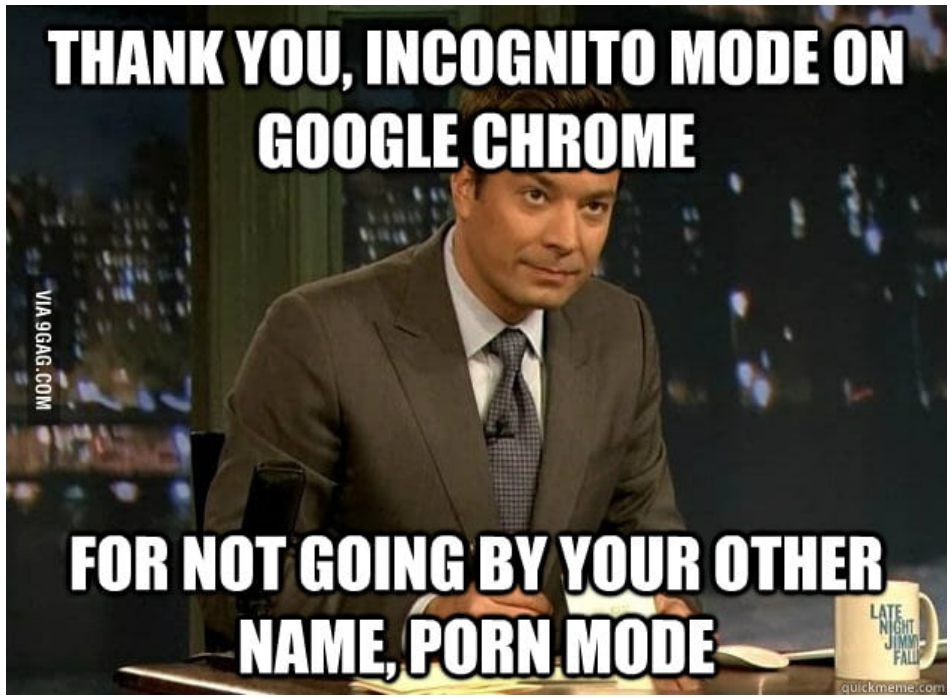
Navegación segura

Cookies – navegación en modo incógnito



Navegación segura

Cookies – navegación en modo incógnito



- **Permite no almacenar el historial de navegación**
  - Historia y cookies desaparecen al cerrar **la ventana de incógnito**
  - **OJO: Diferentes ventanas de incógnito en la misma sesión de navegación comparten todo**
- Problemas:
  - No se guarda lo que tienes abierto entre diferentes dispositivos
  - Si se cierra el programa con error, se pierden las páginas abiertas

Navegación segura

¿Qué sabe Google de ti?

- Mercado de Android en dispositivos móviles, **cerca del 80 %**
- La mayoría de los usuarios usa una **cuenta asociada con Google**
  - Filosofía del “Bueno, bonito y barato”
  - *If you’re not paying for it, you become the product*

CUD Zaragoza

Navegación segura

¿Qué sabe Google de ti?

- Mercado de Android en dispositivos móviles, **cerca del 80 %**
- La mayoría de los usuarios usa una **cuenta asociada con Google**
  - Filosofía del “Bueno, bonito y barato”
  - *If you’re not paying for it, you become the product*

`https://myactivity.google.com`

Agenda

Conectividad segura

Redes WiFi públicas: riesgos

Robo de datos

- Captura de paquetes de datos
  - WiFi funciona por ondas. Cualquiera en el medio puede “verlas” y recopilar los datos
  - Posterior análisis y filtrado. Caso famoso: TJX Companies, 2008 (Albert Gonzalez)
- Puntos de acceso WiFi falsos
  - Pregunta al local si tienen WiFi, antes de conectarte a “su” WiFi
- Ataques *man-in-the-middle*
  - Conexiones sin cifrado serán visibles si interceptan tu comunicación
- Robo de cookies de autenticación no cifradas (*sidejacking*)

CUD Zaragoza

Conectividad segura

Redes WiFi públicas: riesgos

Infección de dispositivos

- Explotación de vulnerabilidades en el cliente conectado

Seguimiento de actividad

- Identificación del tráfico del usuario y captura selectiva
- Creación de un perfil. ¿Primera fase de un ataque más avanzado?

Suplantación de identidad

- Conexiones débiles (no cifradas) a redes sociales, correo, banco, etc.

Conectividad segura

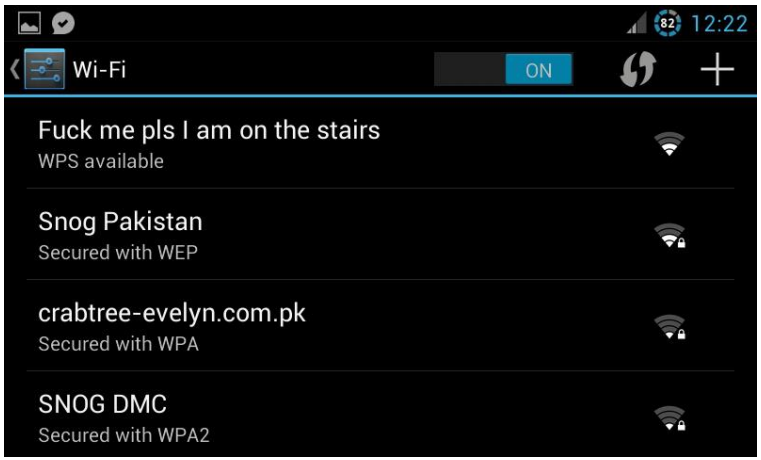
Redes WiFi públicas: algunos consejos. . .

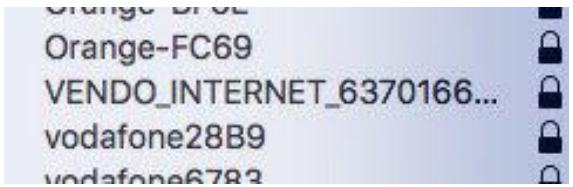
- **Desconfía/evita redes sin clave** (o con cifrado débil como WEP)
- **Desconecta la WiFi del dispositivo**
  - **Ojo con la integración entre dispositivos** (e.g., MacOS y iOS)
- **Evita acceder a páginas sin cifrado**
  - **Verifica el certificado!**
- **Evita realizar servicios/acciones con riesgo potencial**
  - Pagos, redes sociales
  - Descarga de aplicaciones o actualizaciones

CUD Zaragoza

Conectividad segura

Red WiFi en casa: algunos consejos...

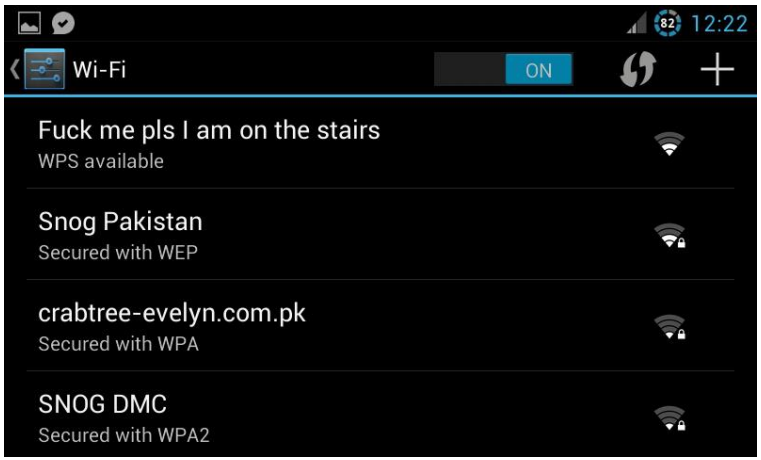


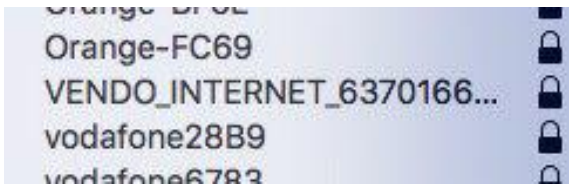


- **Usar WPA2 como cifrado** (como mínimo por ahora)
- **Desactivar el Wi-Fi (un)Protected Setup (WPS) del router**
- **Cambiar la contraseña de acceso al router**
- **Seleccionar una contraseña fuerte**
  - Evita palabras de diccionario
  - Usa símbolos, números y caracteres adicionales

Conectividad segura

Red WiFi en casa: algunos consejos...





- **Usar WPA2 como cifrado** (como mínimo por ahora)
- **Desactivar el Wi-Fi (un)Protected Setup (WPS) del router**
- **Cambiar la contraseña de acceso al router**
- **Seleccionar una contraseña fuerte**
  - Evita palabras de diccionario
  - Usa símbolos, números y caracteres adicionales
- **Más avanzados**:
  - Direcciones IP fijas (desactivar servidor DHCP)
  - Filtrado de dirección MAC

Agenda

Otras buenas prácticas

Contraseñas seguras

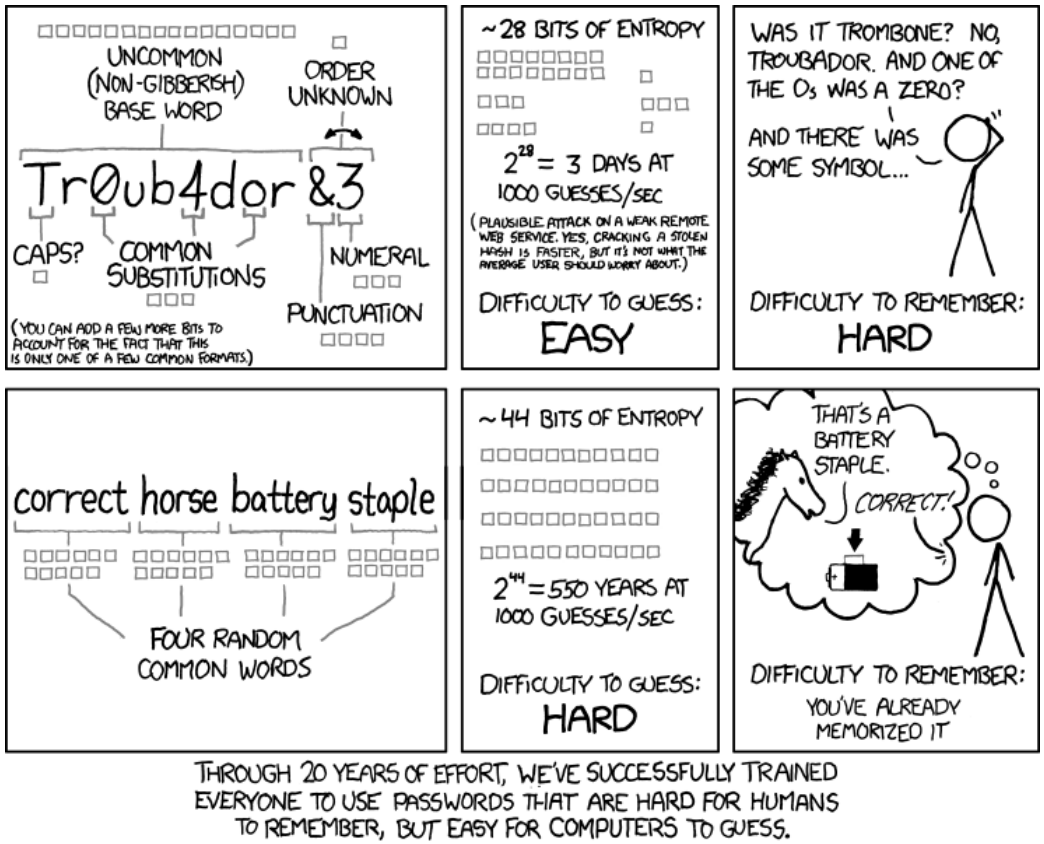
PASSWORD $\longrightarrow$ PASSPHRASE

- **Longitud considerable**
- **Evita palabras de diccionario y fechas** (e.g., “ricardo1985”)
  - Símbolos
  - Números
  - Caracteres adicionales (e.g., ñ, Á, ö, . . .)
- **Ojo con las preguntas de recuperación**:
  - Respuestas no esperadas (o esperadas pero escritas de forma diferente)

CUD Zaragoza

Otras buenas prácticas

Contraseñas seguras

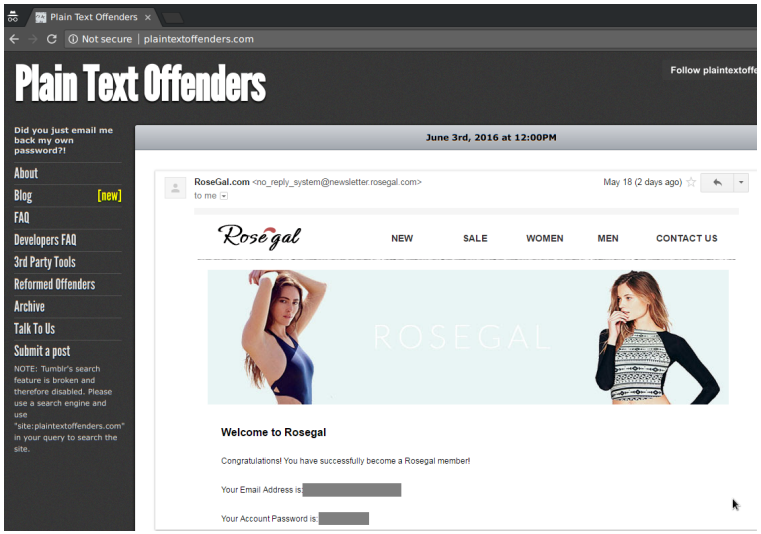


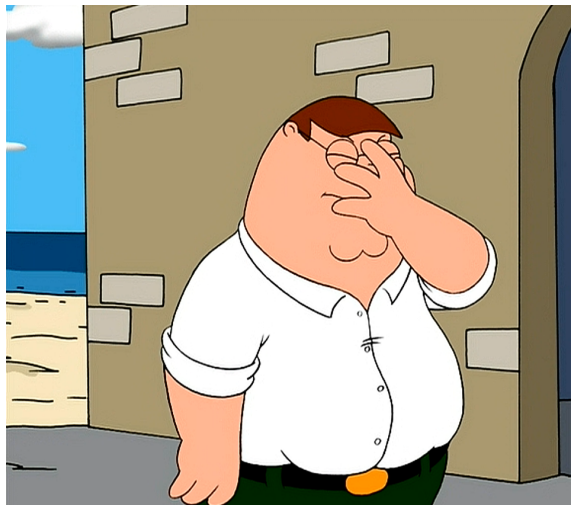
Mejor todavía: “c0rr3ct_hOrs3_B4ttery_stAplE”

Cuantas más elementos tenga el alfabeto, más tiempo de cómputo (más difícil)

Otras buenas prácticas

Contraseñas seguras – ¡ojo!



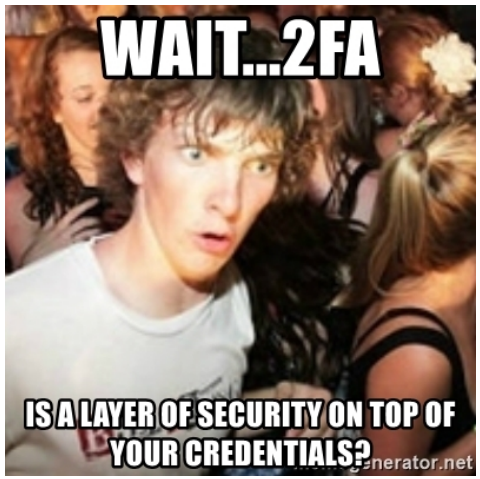


- **Algunas páginas web guardan las contraseñas EN CLARO**: `http://plaintextoffenders.com/`
  - **Evítalas**
  - **Usa contraseñas generadas aleatoriamente**
    - `https://www.random.org/passwords/`, `https://strongpasswordgenerator.com/`
- **¿Gestor de contraseñas?**: `KeePass`, `KeePassXC` (en local)
  - **Usa una contraseña segura (léase fuerte) para acceder a él**
  - En la nube, e.g., Google (`http://passwords.google.com`, siempre pide login)

CUD Zaragoza

Otras buenas prácticas

Doble factor de autenticación



- **Factores de autenticación**:
  - Algo que **el usuario sabe** (password, pin, palabra de paso, etc)
  - Algo que **el usuario tiene** (USB, teléfono, tarjeta, etc.)
  - Algo que **el usuario es** (huella dactilar, iris, reconocimiento facial, etc.)
- **Medida de seguridad adicional**
  - Cuando se observa una conexión extraña (e.g., de un dispositivo nuevo o desde una ubicación no habitual), se solicita un código para acceder al servicio
  - Normalmente, envío de código al correo electrónico o al móvil (SMS) – ¿privacidad?
- Implementado en banca, con transferencias de cuantía elevada
- **Disponible en muchos servicios de Internet** (Google, Twitter, Facebook)

Otras buenas prácticas

Correos de spam/phising

- **Adjuntos con “regalo”**
- **Redirección a páginas que explotan vulnerabilidades**

- **No ejecutes adjuntos de remitentes desconocidos**
  - Ojo con los ficheros ejecutables, PDF, ZIP, o DOC(X)
- **No pinches en enlaces extraños**
  - Lo mismo navegando: si iba a descargar un PDF, ¿por qué ahora se baja un EXE?
- **El servicio del SICUZ (u otros) nunca te va a solicitar tu contraseña**
  - Y menos todavía, en un formulario de Google Docs ⌣̈

Otras buenas prácticas

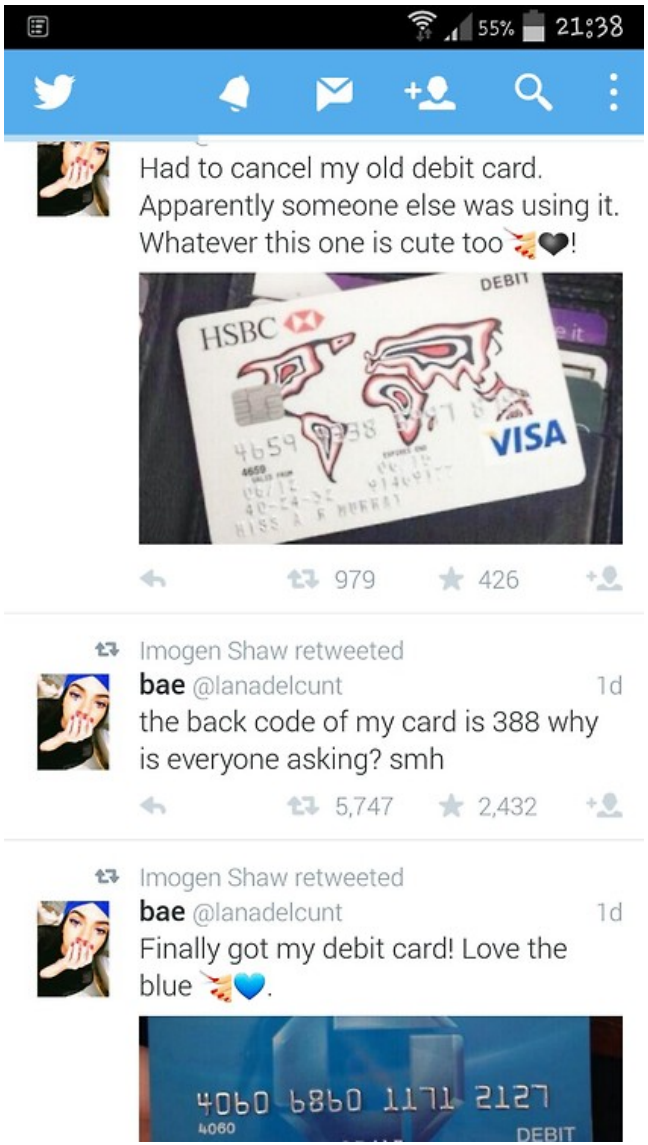
Patrones de acceso a dispositivos

- **Evita acceso físico no autorizado al dispositivo**
  - Pérdida del dispositivo (valor económico)
  - **Pérdida de la información sensible y personal** (mayor valor económico)
    - Datos de contactos, fotos, conversaciones de chats, etc.
    - Las apps de tu móvil guardan una "autorización", lo que evita que tengas que poner tu contraseña cada vez que accedes a la app
- Si sólo proteges la tarjeta SIM (con PIN), **todo el contenido del teléfono será accesible cuando se quite la SIM**

- **Bloqueo con código de acceso robusto**
  - **Código numérico (6 a 8 dígitos recomendado) o huella dactilar**
- **Cifrar contenido de la tarjeta SD** (o información sensible del disco duro)
  - Si no, tan fácil como sacar la tarjeta SD e insertarla en un lector...
- **Activar opciones de localización y bloqueo remotos** (si se puede)

Otras buenas prácticas

Redes sociales



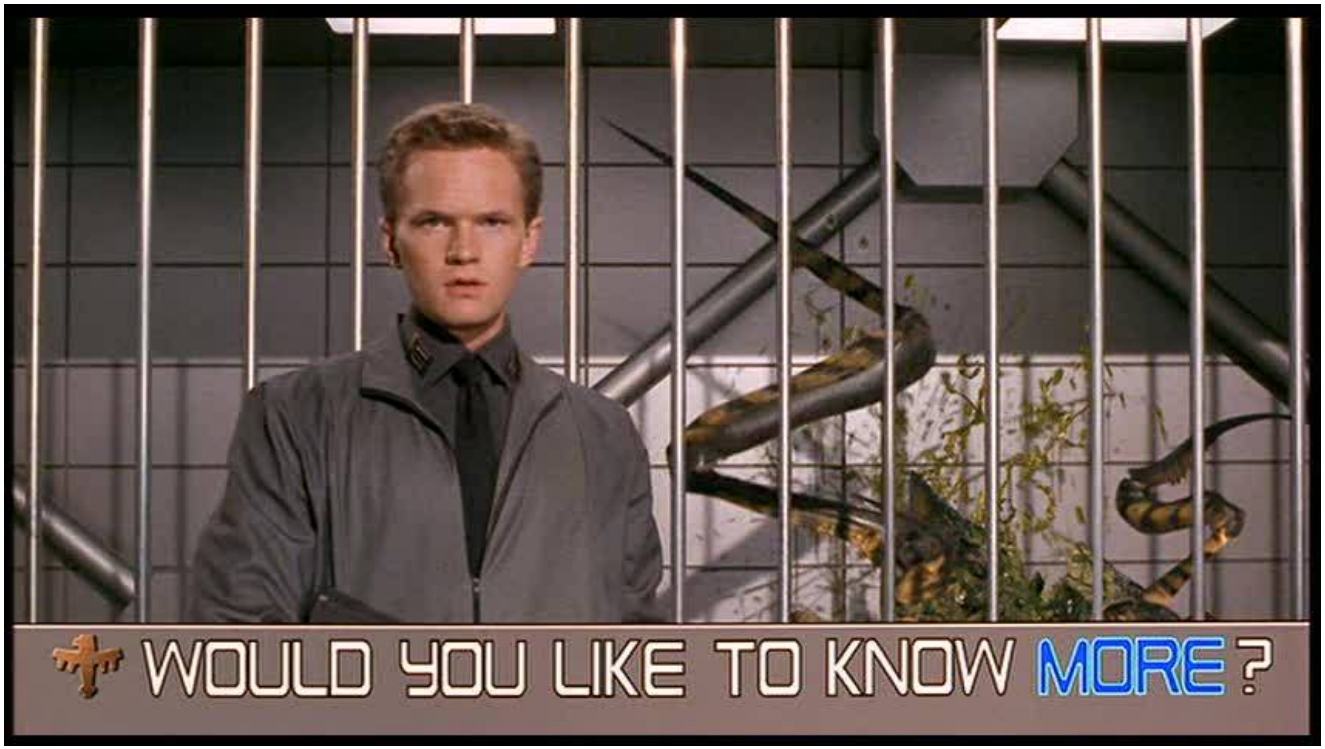
- **Fotos de carácter privado/comprometido**
  - Que sólo la compartas con tus amigos no quiere decir que sólo tengan acceso tus amigos...
  - `https://twitter.com/needadebitcard`
- **Informar sobre tus movimientos** (e.g., cuando te vas de vacaciones)
  - Das pistas de que probablemente tu casa sea un blanco fácil
- Comentarios y elementos compartidos sirven para hacer un ***profiling*** **del usuario**
  - Publicidad selectiva
  - Primera fase de un ataque más sofisticado

Otras buenas prácticas

Consejos más generales

- **Actualiza tu SO y aplicaciones**
  - Usa software legal. ¿Conoces **todo lo que te proporciona el SICUZ**?
- **Descarga de software de Internet**
  - Verifica que la descarga la estás haciendo de la página oficial del producto
  - Lo dicho, ojo con el software pirata ☺
- **Resultados de las búsquedas**
  - Intenta observar la dirección destino
  - Sospecha de repeticiones de texto en la descripción, mal transcripciones, etc.
- **Usa productos de seguridad (anti-virus)**
  - Alternativamente, puedes usar SSOO menos atacados (e.g., Linux) – no es tan difícil ☺

CUD Zaragoza



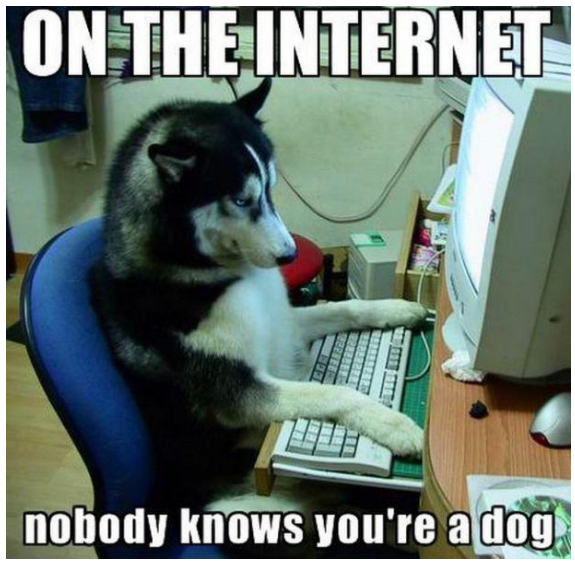
https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet

CUD Zaragoza

Agenda

Conclusiones

Desconfiad. Pensad. Seguid navegando (o no).



https://www.youtube.com/watch?v=h8-27iLvyS4

Conclusiones

That's all, folks!

Navegando por Internet de forma segura: riesgos, buenas prácticas y herramientas

Ricardo J. Rodríguez

rjrodriguez@unizar.es

Centro Universitario de la Defensa Zaragoza

7 de febrero, 2018

Jornadas de Internet Segura

Facultad de CCSS y del Trabajo, Universidad de Zaragoza