Seguridad

Fernando Bobillo

Resumen de contenidos

- Malware
- Herramientas contra el malware
- Contraseñas
- Actualizaciones
- Cifrados
- Redes
- Móviles y otros dispositivos
- Navegación
- Correo electrónico: *spam*, bulos y *phishing*
- Redes sociales y mensajería instantánea

Malware

Malware

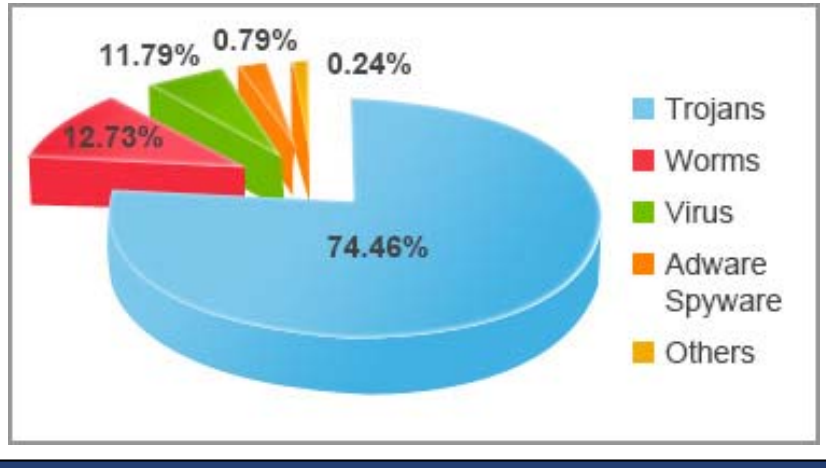
- Malware *(Malicious software)*
  - Software cuyo objetivo es dañar un ordenador o infiltrarse en él sin el consentimiento de su usuario
- Más grave en unos sistemas operativos que otros
  - Por ejemplo, Linux es mucho más seguro que Windows
  - Pero no es cierto que no haya virus para Mac y Linux

Hacker

- Hacker (de sombrero blanco): experto en seguridad informática
  - Bueno y ético, solo le interesa el conocimiento
  - Inofensivo, solo le interesa comprender el funcionamiento
- Cracker (de sombrero negro): ciberdelincuente
  - Malo y no ético, rompe sistemas de seguridad para sacar beneficio económico o de otro tipo, para hacer daño…

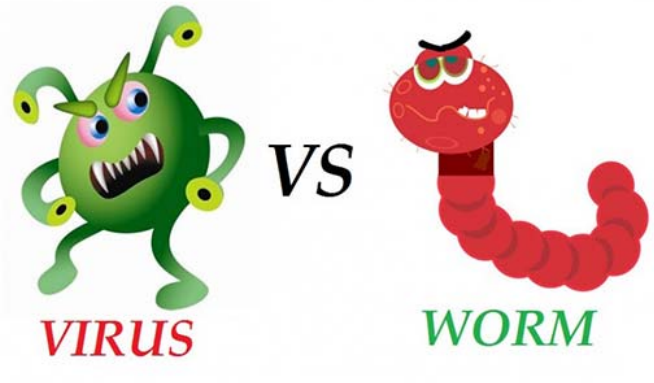
Tipos de malware

- Infeccioso: virus, gusanos
- Oculto: troyanos, puertas traseras, *rootkits*
- Publicidad: *spyware, adware, hijackers*
- Llamadas telefónicas: *dialers*
- Robo de información: *keylogger, stealers*
- Secuestro de información: *ransomware*



Malware infeccioso

- Virus: capaz de propagarse infectando otros archivos
- Gusano (*worm*): capaz de autoduplicarse y transmitirse en red
- El virus necesita intervención humana, el gusano no
- El gusano está en memoria y no necesita modificar ficheros
- Ambos pueden cometer daños serios en el equipo, como por ejemplo borrar todos los ficheros del disco duro
- Ambos pueden reenviarse a nuestros contactos por e-mail



Virus Cookie

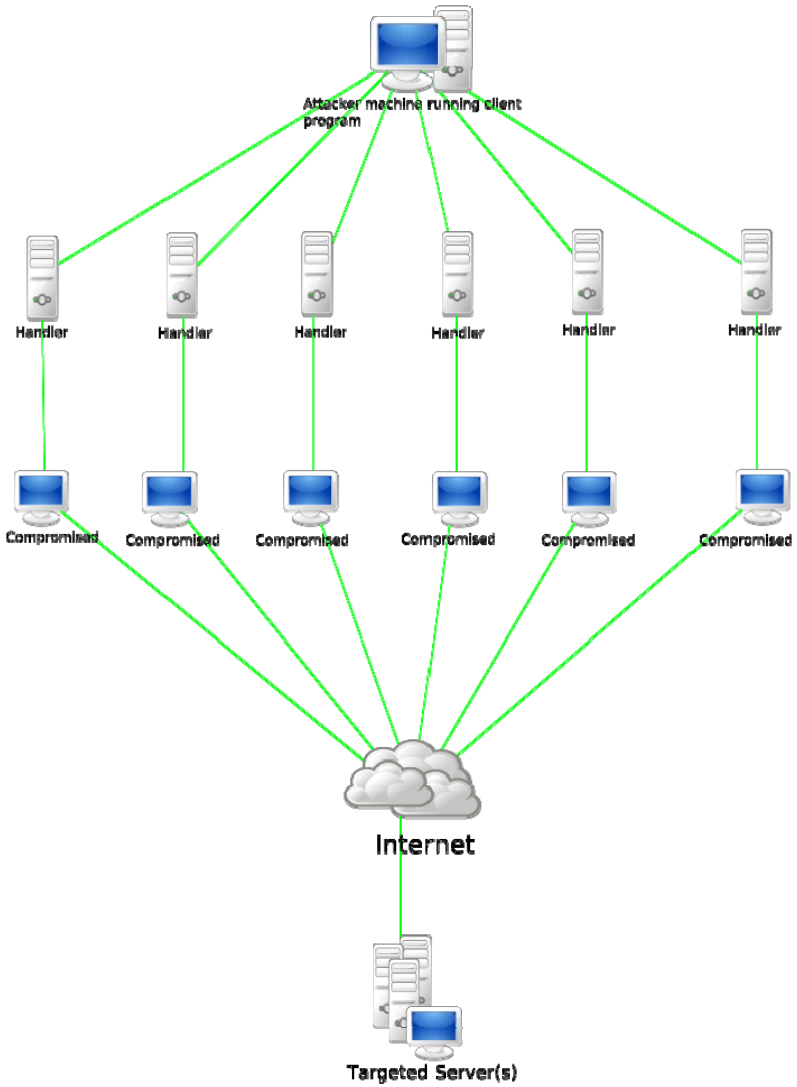
Virus poco peligroso, se recupera el acceso al ordenador tecleando “Cookie”

Malware oculto

- Puerta trasera (*backdoor*): malware que permite el acceso remoto a un ordenador de un ordenador de forma oculta
- Troyano o caballo de Troya: malware con aspecto inofensivo en apariencia pero que incluye código malicioso
  - No se reproduce como los virus, suele usar una backdoor
- *Rootkit*: malware diseñado para obtener acceso a zonas no permitidas del SO y también enmascarar su existencia

Zombies y botnets

- Zombi: ordenador infectado por algún malware que puede ser usado por una tercera persona distinta al propietario
- Botnet: conjunto o red de bots informáticos, posiblemente zombies, que se ejecutan de manera autónoma y automática
- Denegación de servicio distribuida (*Distributed Denial of Service*, DDoS): ataque por el que una botnet agota el ancho de banda de un servidor Web provocando su caída



Malware publicitario

- *Spyware* (programa espía): malware dedicado a recopilar información sobre la actividad del usuario y distribuirlo a alguna empresa u organización interesada
  - Páginas web visitadas, *cookies*, direcciones de e-mail...
- *Adware*: malware que muestra publicidad intrusiva al usuario
  - Algunos programas shareware permiten la instalación gratuita a cambio de publicidad, pero no siempre se avisa al usuario con suficiente claridad
- *Hijacker*: cambia la configuración del navegador Web
  - Cambiar la página de inicio
  - Lanzar ventanas emergentes
  - Redireccionar los resultados de los buscadores

Cookies

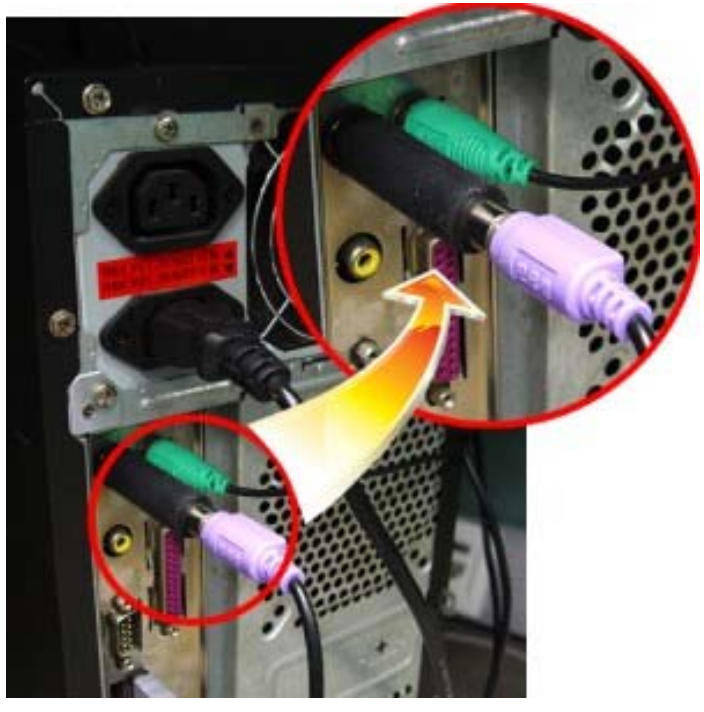
- Cookie: información enviada por un sitio Web y almacenada en un archivo por el navegador que permitirá conocer la actividad previa del usuario y personalizarle contenidos Web

Dialer

- Malware que marca un nº de teléfono usando el módem del ordenador o el propio teléfono móvil
  - Generalmente, números de tarificación especial
- Hoy es poco peligroso en ordenadores porque la conexiones por módem son muy poco frecuentes
  - Ahora las páginas piden al usuario que llame a un nº de teléfono o mande un sms para acceder a los contenidos
- ¡Sigue siendo muy peligroso en móviles!

Malware para robo de información

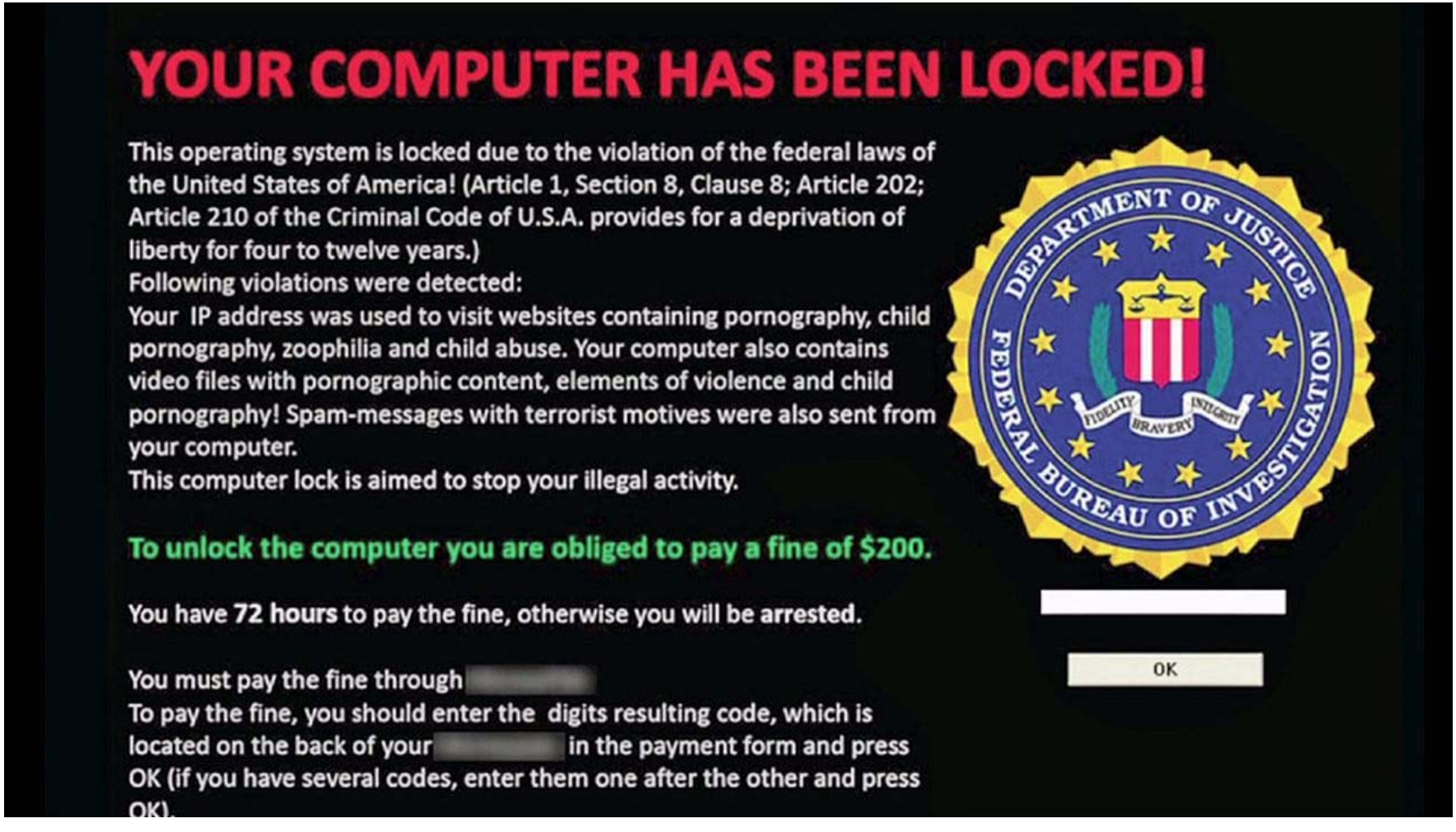
- *Keylogger*: malware que monitoriza las pulsaciones del teclado y las almacenan para enviarlas más tarde al creador
  - Ejemplo: contraseñas, nº de tarjeta de crédito, conversaciones privadas…
  - También se hace con hardware
- *Stealer*: malware que roba información privada almacenada en el ordenador
  - Ejemplo: contraseñas recordadas por los navegadores Web, logs de las conversaciones de chat…



Malware para secuestro de información

- *Ransomware* (criptovirus o secuestradores): cifra archivos importantes del usuario, haciéndolos inaccesibles, y pide pagar un rescate a cambio de la contraseña para descifrarlos
- Ejemplo: Wannacry, mayo de 2017
- No ceder al chantaje
  - No hay garantía de recuperar los datos
  - Quedamos identificados como gente dispuesta a pagar
  - Se financia una actividad delictiva
- Los primeros ransomwares se hacían pasar por la policía y argüían que el usuario había infringido alguna ley
  - En Virginia, un pedófilo se autoincriminó al FBI
  - ¿Roma no paga a traidores?

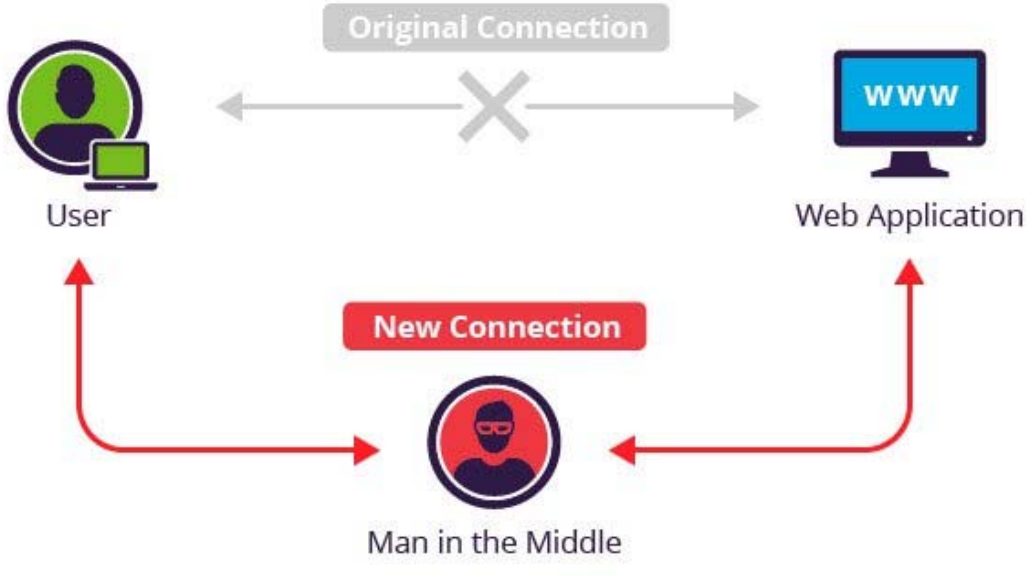
Malware para secuestro de información



Malware para secuestro de información

Ataque del intermediario

- El ataque del intermediario (*man in the middle*) consiste en interceptar las comunicaciones entre el emisor y el receptor pudiendo leer, añadir, borrar o modificar el contenido



- Puede obtenerse la contraseña del usuario, decirle que se ha equivocado al escribirla, reanudar la conexión normal y el usuario repetirá la contraseña y se conectará sin sospechar

Origen del malware

- Modos de contagio
  - Simplemente por estar conectados a la red
  - Visitando páginas web maliciosas
  - Ejecutando programas normales infectados
  - Abriendo ficheros infectados
- Internet (e-mail, P2P, Web…) o no (memoria USB, CD…)
- Muchos formatos de ficheros
  - Ejecutables: .bat, .cmd, .com, .exe, .dll, .msi…
  - Documentos de Microsoft Office: .doc(x), .ppt(x). .xls(x)…
  - Páginas Web: .htm, .html
  - Otros: .ini, .inf, .lnk, .pif, .scf, .scr, .vb, .vbe, .vbs…

Ingeniería social

- Ingeniería social: manipulación psicológica de la gente para que realicen acciones o divulguen información confidencial
  - Los humanos son el eslabón más débil en la seguridad

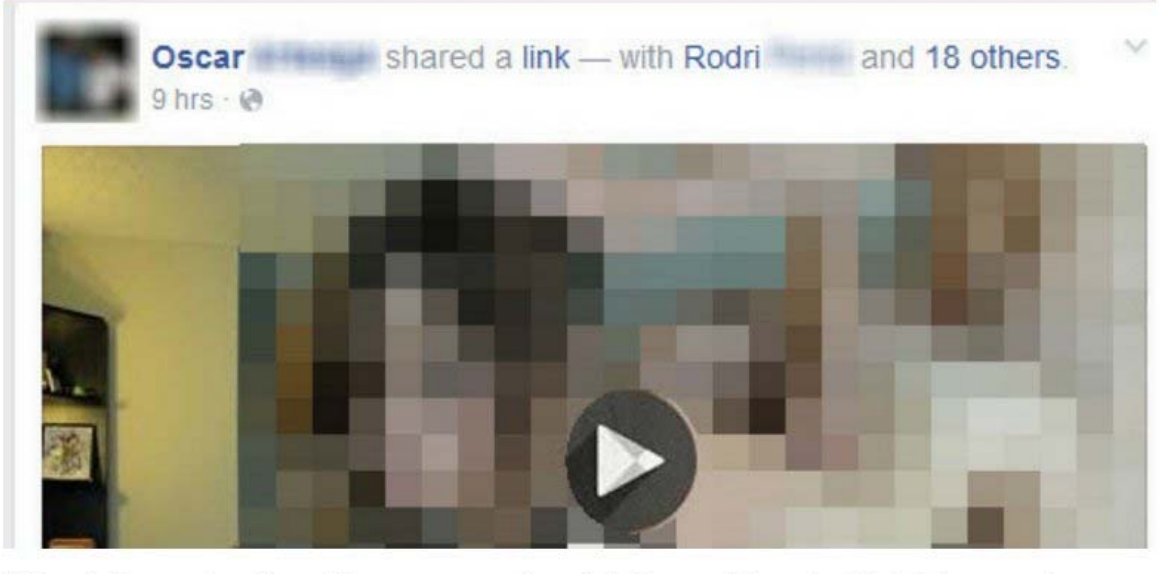
Falsos antivirus infectados

Ganchos útiles/divertidos/interesantes

TECNOLOGÍA | 2015/02/09 15:00

Video porno falso propaga virus en Facebook

Miles de usuarios de la red han caído en una trampa de los ciberdelincuentes al intentar visualizar un supuesto contenido sexual en el que son etiquetados.



Los delincuentes cibernéticos se aprovechan de la incansable curiosidad de los usuarios.

Herramientas contra el malware

Herramientas: precaución

- Cualquier programa de origen desconocido que ejecutemos es potencialmente peligroso
  - Incluso los aparentemente útiles/divertidos/interesantes
- No ejecutar programas o abrir ficheros del exterior sin cuidado
  - Desconfiar
  - Preguntar
  - Buscar
- Lo mejor:
  - De alguna página reconocida
  - Que esté disponible el código fuente
- Usar herramientas contra el malware

Herramientas: antivirus

- Antivirus
  - Prevenir, detectar y eliminar software malicioso
  - No solamente virus, también otros tipos de malware
  - Es básico tener actualizada la base de datos de virus
  - Detección heurística: búsqueda automática de patrones de código parecidos a los de los virus
  - Pueden dar falsos positivos (detección de un virus que no es tal), pero son preferibles a los falsos negativos
  - Oficial en la UZ: ESET

\\Psfunizar3.unizar.es\SoftwarePC

www.eset.es

Virus Total

http://www.virustotal.com

- Servicio gratuito que analiza archivos y URLs sospechosas con varios antivirus diferentes evitando falsos positivos

Herramientas: cortafuegos y respaldo

- Cortafuegos (*firewall*)
  - Gestión del tráfico de la red
  - Permite bloquear accesos no autorizados
  - Cuidado: el usuario da permiso a ciertos accesos
  - El hardware también puede actuar como cortafuegos
  - Ejemplo: cortafuegos de Windows y Mac

- Software de respaldo
  - Prevención de problemas software y hardware
  - Realizar copias de seguridad periódicas (*backup*)
  - Cuidado con el sentido de la copia
  - Ejemplo: Time Machine en Mac

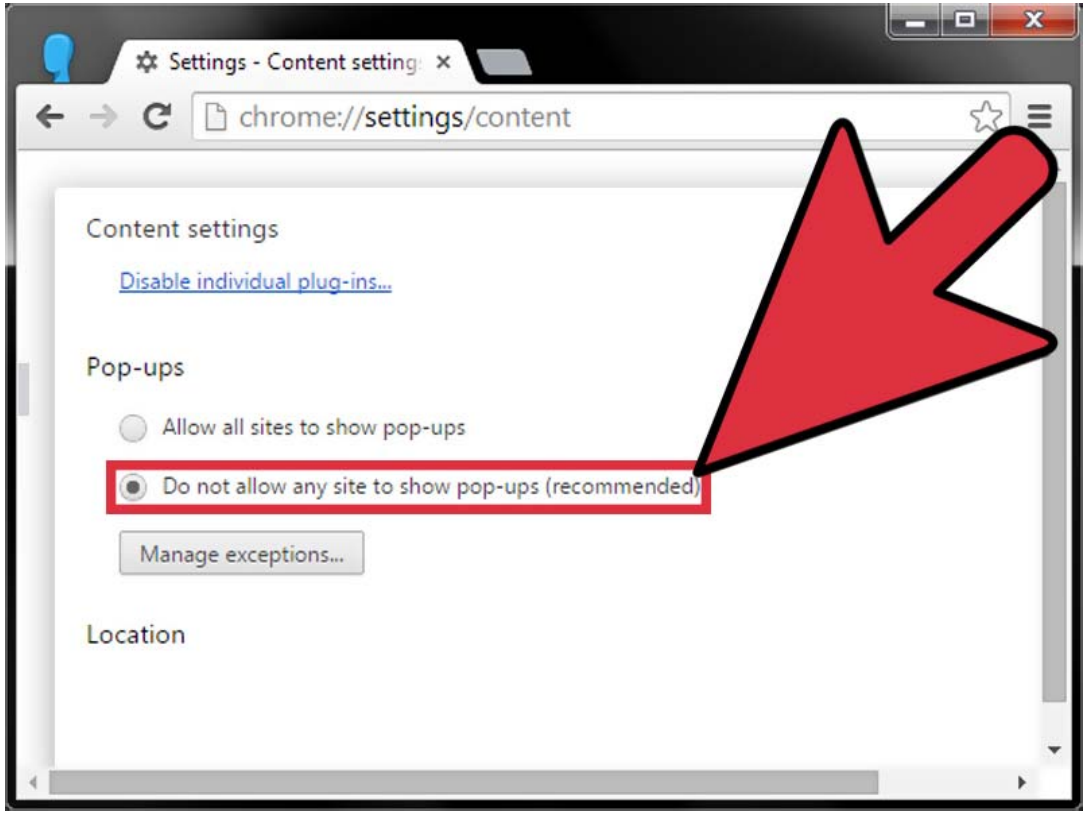
Espionaje a través de la webcam

- Es una buena idea tapar la webcam del ordenador o móvil para que nadie pueda grabarnos sin nuestro consentimiento

☹ Si nos roban no podremos tratar de fotografiar al ladrón

Bloquear las ventanas emergentes

- Los navegadores permiten bloquear por defecto las ventanas emergentes (*pop-us*)
  - Podemos desbloquearlas a mano o indicar excepciones



Contraseñas

Contraseñas

Nadie serio (los bancos para esto lo son) nos pide la contraseña por email

Usar contraseñas seguras

Europa Press

12 de marzo de 2015 ·

Me gusta esta página

A Santiago Segura le hackearon Twitter porque usaba "amiguetes" de contraseña.

Portaltic.es te cuenta cómo el actor y director descubrió el hackeo

A Santiago Segura le hackean su cuenta de Twitter, protegida con la contraseña "amiguetes"

En una entrevista concedida al portal de televisión 'Vertele', el director de cine y humorista Santiago Segura ha querido aclarar todos los detalles acerca de...

EUROPAPRESS.ES

Usar contraseñas seguras

Usar contraseñas seguras

Contraseñas más habituales

Contraseñas seguras

- Combinación de letras y números
- Combinación de mayúsculas y minúsculas
- Si se permite, uso de símbolos no alfabéticos como $#!?
- Longitud mínima de 8 caracteres (mejor 10-12)
- No usar palabras que estén incluidas en un diccionario
- No usar nombres propios
- No usar la misma en varios sitios
  - Pueden perderla otros (el servidor que guarda las claves)
- Cambiarlas con cierta frecuencia
- Comprobar su calidad con alguna herramienta para tal fin

http://www.passwordmeter.com

The Password Meter

http://www.passwordmeter.com

Test Your Password		Minimum Requirements
Password:	3tTtte1t.1T,2T,3T,te1t.¿Q	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	29	+ 116
Uppercase Letters	Cond/Incr	+((len-n)*2)	6	+ 46
Lowercase Letters	Cond/Incr	+((len-n)*2)	9	+ 40
Numbers	Cond	+(n*4)	6	+ 24
Symbols	Flat	+(n*6)	8	+ 48
Middle Numbers or Symbols	Flat	+(n*2)	12	+ 24
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	24	- 4
Consecutive Uppercase Letters	Flat	-(n*2)	1	- 2
Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.

Sufficient: Meets minimum standards. Additional bonuses are applied.

Warning: Advisory against employing bad practices. Overall score is reduced.

Failure: Does not meet the minimum standards. Overall score is reduced.

El tamaño importa (y el contenido también)

Nº de elementos de la clave	Millones (M) de combinaciones	10 M claves/s	100 M claves/s	1000 M claves/s
10 (números)	100	10 s	Inmediato	Inmediato
26 (caracteres)	200.000	348 m	35 m	3.5 m
52 (may. + min.)	53 M	62 d	6 d	15 h
62 (nos + caract.)	218 M	253 d	25.25 d	60.5 h
96 (+ símbolos)	72.000 M	23 a	2.25 a	83.5 d

- 10 M claves/s: PC de gama alta
- 100 M claves/s: varios PCs o clúster de ordenadores
- 1000 M claves/s: supercomputadora o red a gran escala

Contraseñas seguras

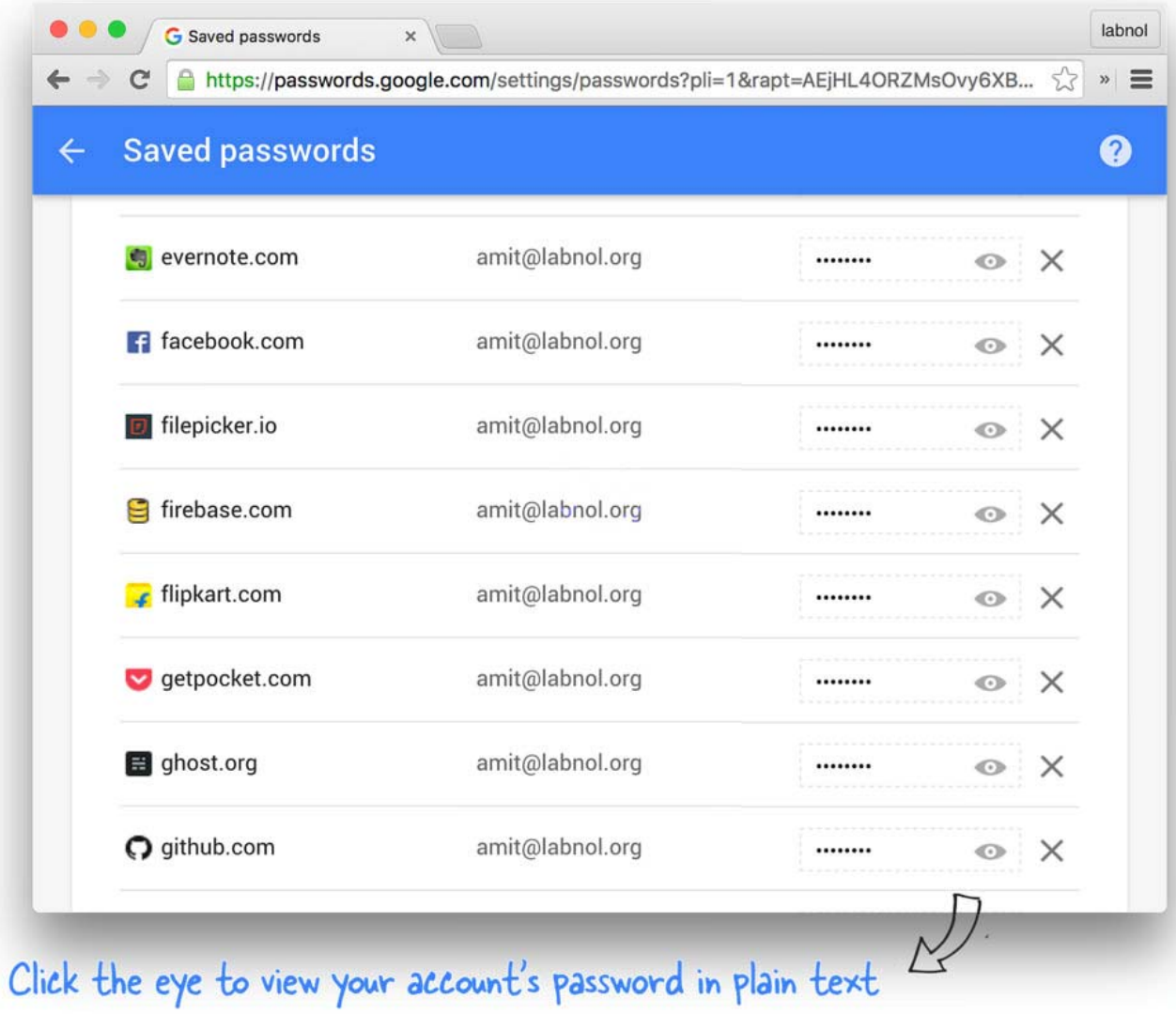
- Además, debe ser fácil de recordar
  - Riesgo de olvidarla y no poder usarla
  - Si la apuntamos, riesgo de que alguien más la vea
- Conviene usar mnemotécnicos
  - Podemos construir contraseñas a partir de frases usando nuestras propias reglas
- Ejemplo:
  - Tres tristes tigres triscaban trigo en un trigal. Un tigre, dos tigres, tres tigres, trigaban en un trigal. ¿Qué tigre trigaba más?
  - Resultado: 3tTtte1t.1T,2T,3T,te1t.¿QTt+?

Contraseñas

Gestor de contraseñas

- Gestor de contraseñas (*password manager*): software que facilita el almacenamiento de contraseñas para no olvidarlas
  - Es importante que las almacene cifradas
  - Puede no estar en el ordenador: Internet (a través de aplicación Web), dispositivo extraíble (memoria USB)…

Gestor de contraseñas



Autenticación en dos pasos

- Usar dos criterios para decidir si usuario es quien dice
- Algo que tiene, algo que sabe, algo inseparable de él…
- Ejemplo: para sacar dinero de un cajero se le pide algo que tiene (la tarjeta de crédito) y algo que sabe (el número PIN)
- Envío de códigos de confirmación por email o por SMS
  - Usado para compras por Internet o registrarse en páginas

Detección de uso de nuestra cuenta

- Google muestra el lugar y SO de las conexiones a la cuenta

  http://myaccount.google.com/security

- Incluso envía emails de aviso ante actividad sospechosa

☹ Para Google, el aula L1.2 del Ada Byron está en Alemania

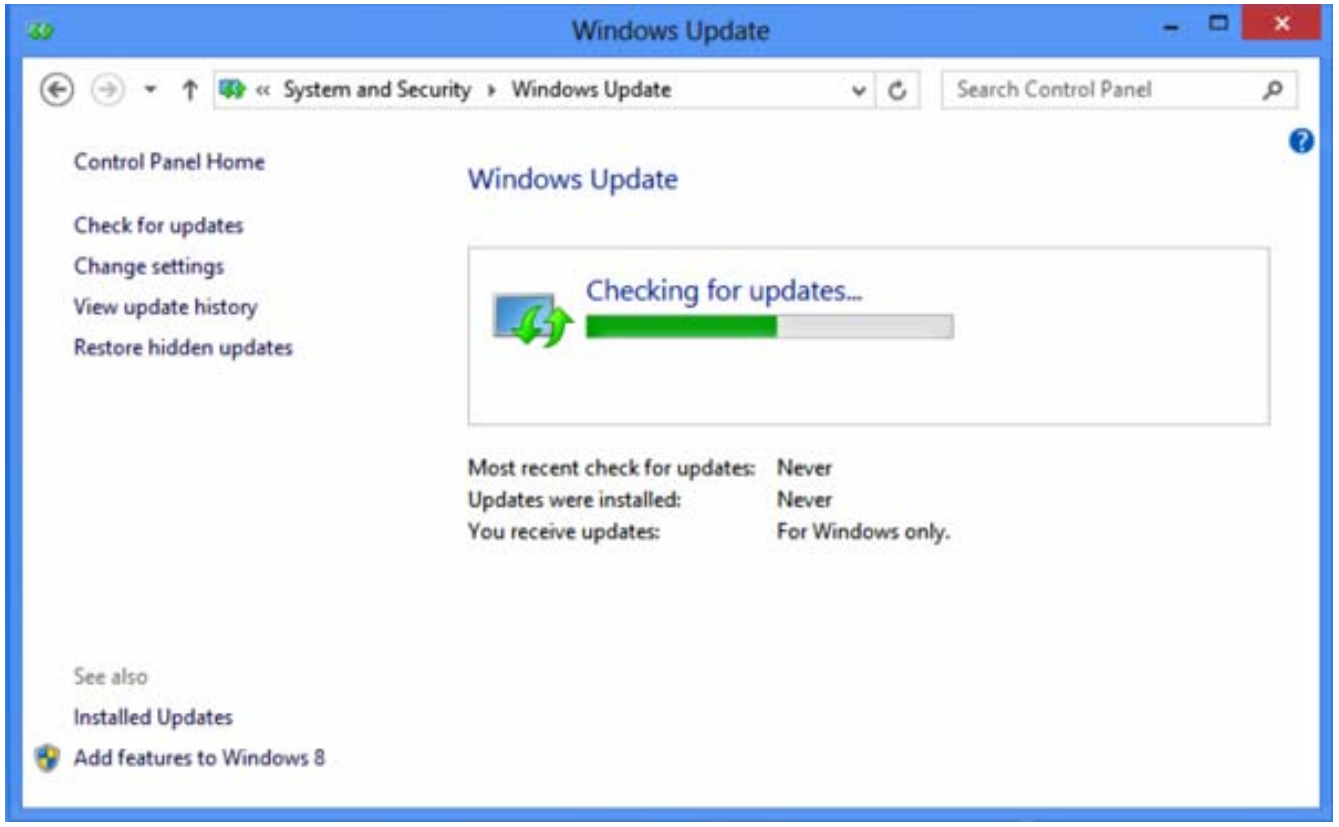
Actualizaciones

Actualizaciones

- Se descubren fallos de seguridad en el software de manera permanente, por lo que es muy importante actualizarlo
- El fabricante del software proporciona un programa (parche) de pequeño tamaño que corrige los fallos detectados
- Normalmente, las actualizaciones automáticas suelen venir activadas por defecto: mantenerlas o activarlas si no lo están
- Es importante
  - Utilizar el servicio del fabricante
  - Seguir las instrucciones (por ejemplo, reiniciar)
  - Esperar a que termine
  - Asegurarse de que todo ha ido bien

Actualización de Windows

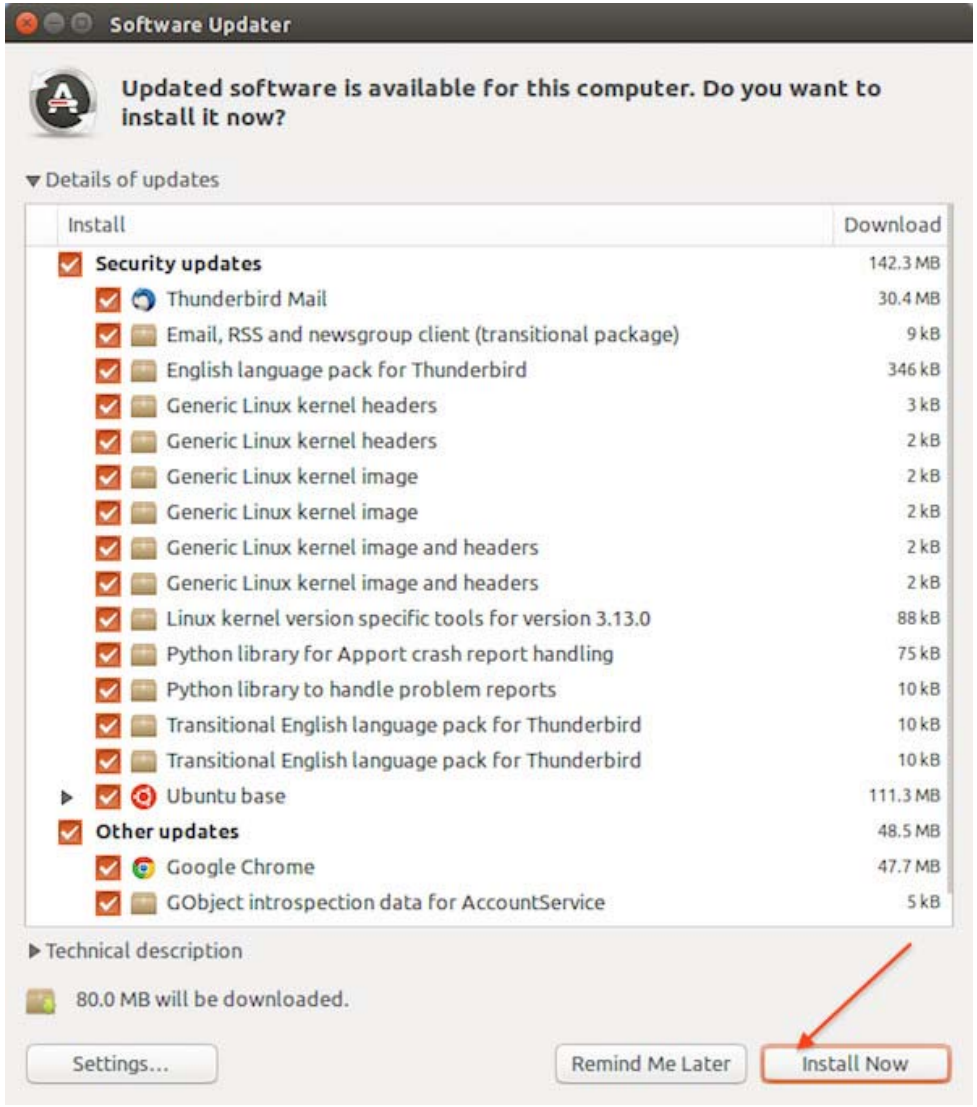
- http://windowsupdate.microsoft.com (con Internet Explorer)
- Antes las actualizaciones eran el segundo martes de cada mes, ahora se hacen cuando estén disponibles



Actualización de los programas

- No solamente el SO debe ser actualizado
- Importante: navegador y sus plugins

Actualización en Mac OS X y Linux



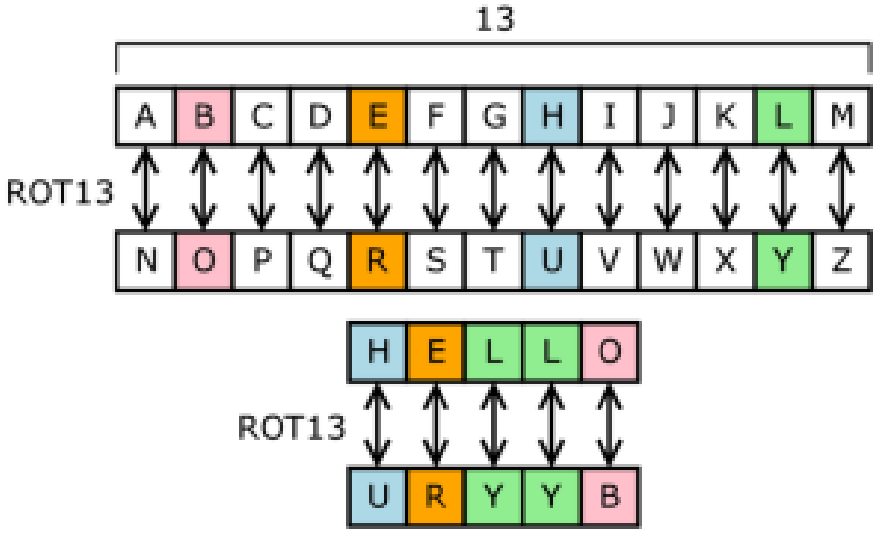
No solamente los ordenadores

- En móviles, configurar para que avise de las actualizaciones disponibles pero descargarlas manualmente (con una WiFi)

Cifrado

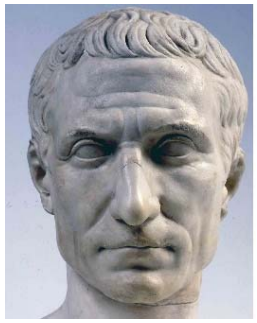
Cifrados ROT13 y César

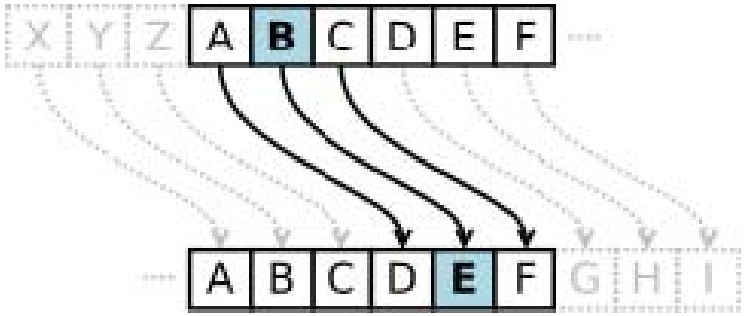
- ROT13: cada letra se desplaza *13* posiciones en el alfabeto



Para romperlo por fuerza bruta, probar 1 posibilidad

- César: cada letra se desplaza k posiciones en el alfabeto

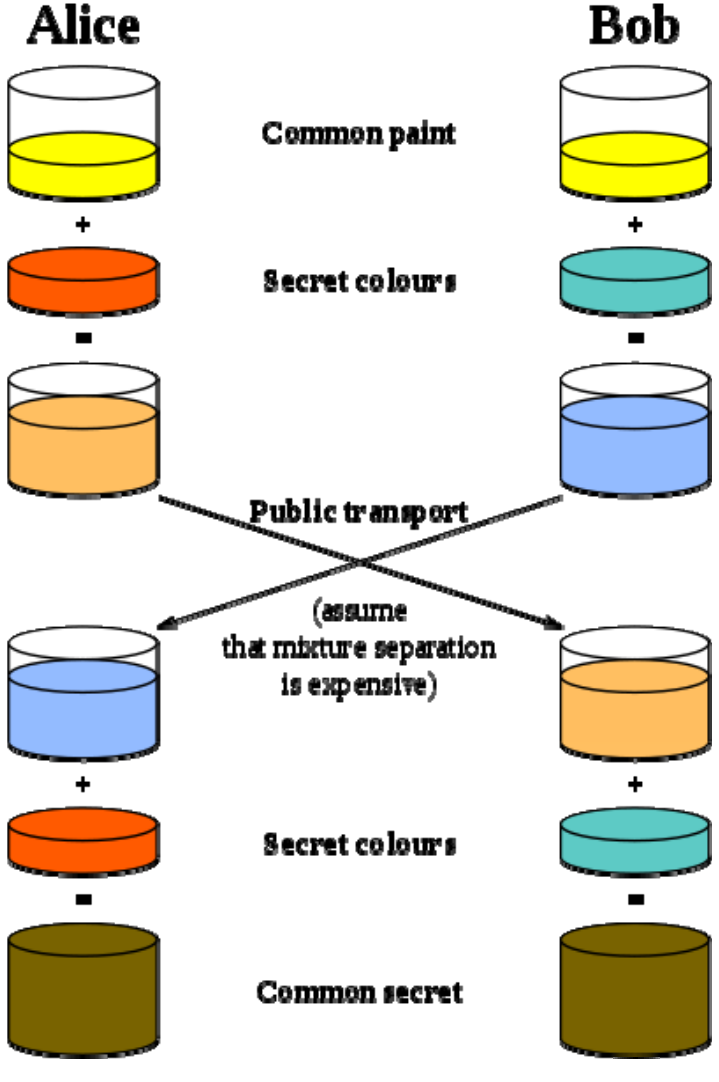




Para romperlo por fuerza bruta, probar 26 posibilidades (alfabeto inglés)

Protocolo de Diffie-Hellman

- Criptografía asimétrica o de clave pública: todo usuario tiene 2 claves
  - Pública, para la autenticación del emisor de un mensaje
  - Privada, para encriptar mensajes
- Protocolo de Diffie-Hellman: permite el establecimiento de claves (acordar el valor de una información secreta compartida) para intercambiarlas de modo seguro sobre un canal público
  - Funciona por el desconocimiento de algoritmos eficientes para poder deshacer las operaciones

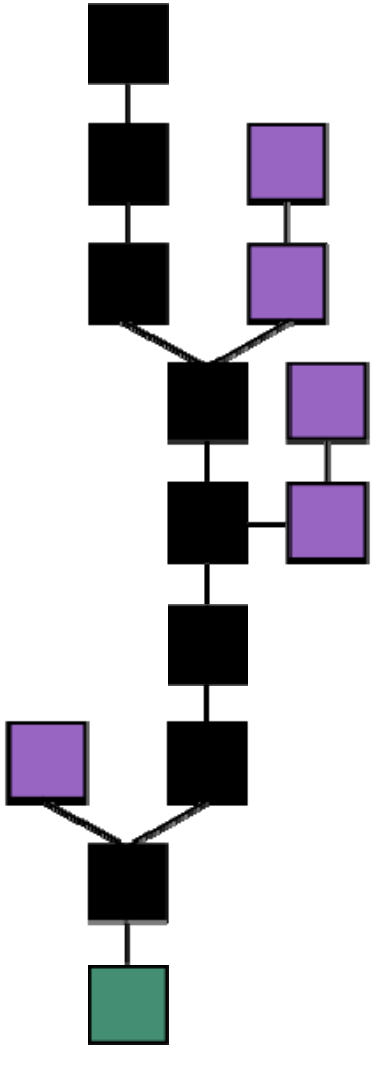


Cifrado RSA

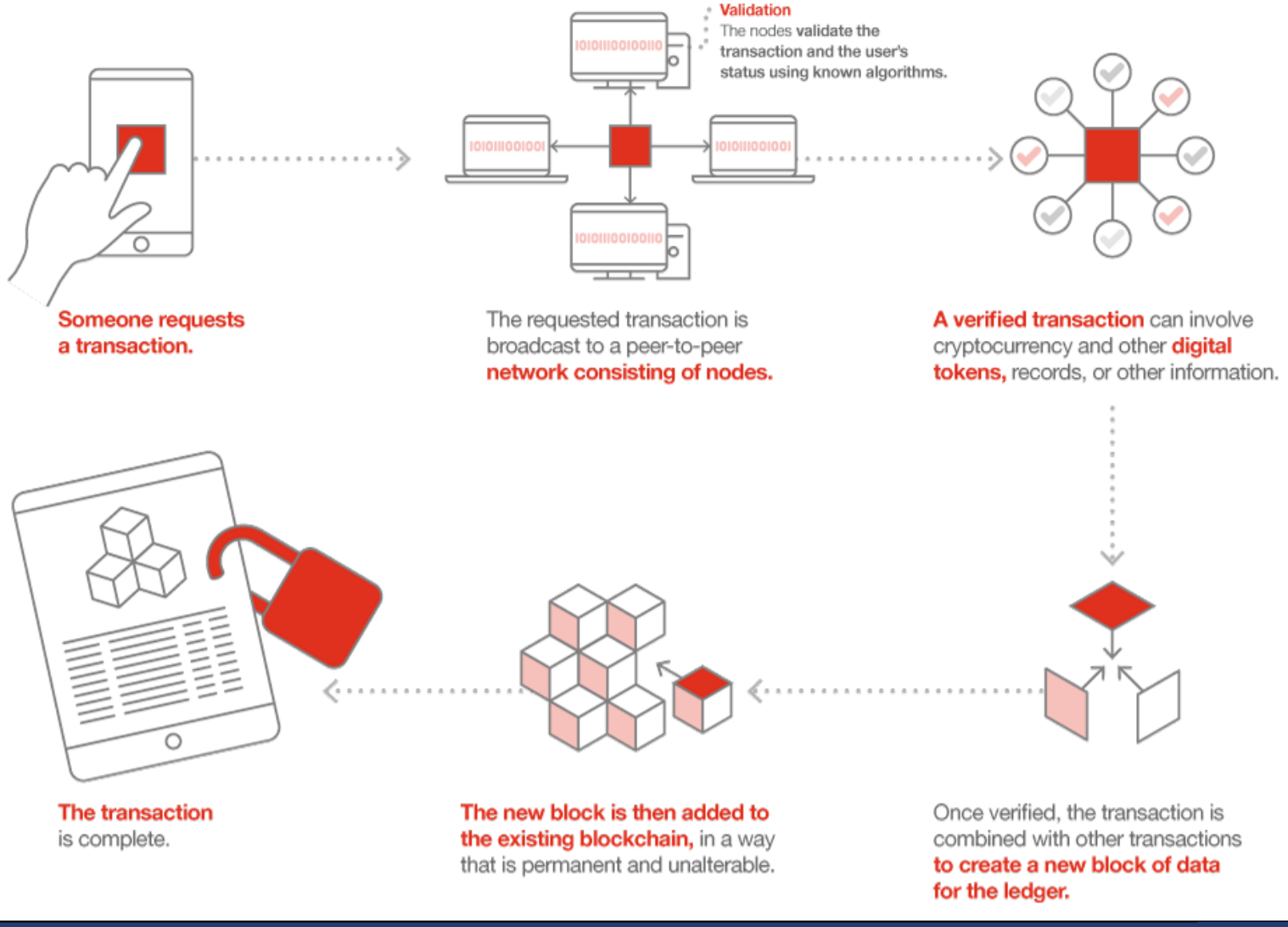
- Cada usuario tiene 2 claves, una pública y otra privada
  - Ambas claves están relacionadas matemáticamente y se calculan a partir del producto de 2 números primos grandes
- El emisor de un mensaje lo cifra usando la clave pública del receptor
- El receptor lo descifra usando su clave privada
- Por qué funciona:
  - Las claves se escogen de modo que se permita cifrar con una y descifrar con la otra
  - Se conocen algoritmos eficientes para calcular productos, potencias y restos de números grandes
  - No se conocen algoritmos eficientes para descomponer números grandes en productos de números primos

Cadenas de bloques

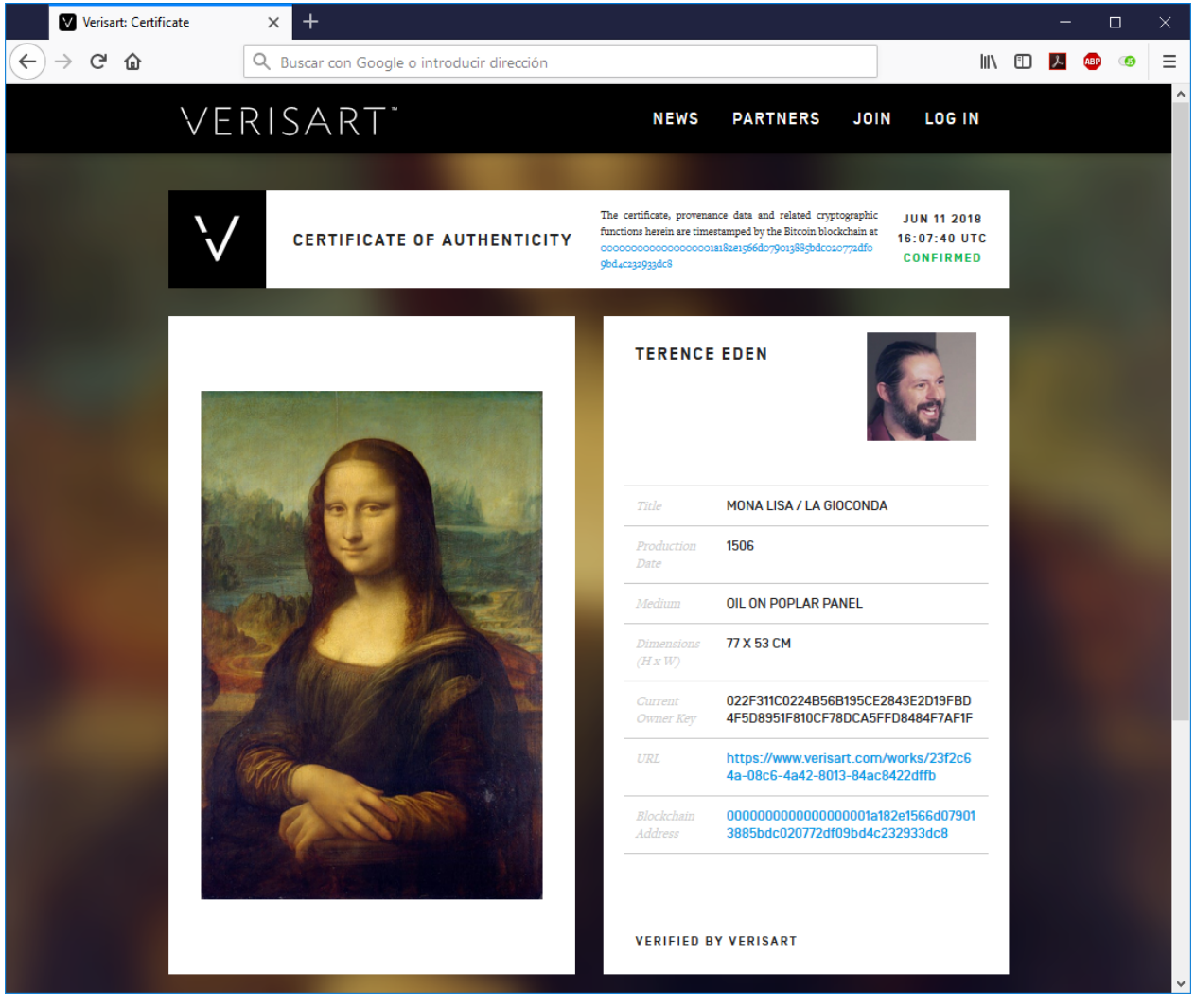
- Cadena de bloques (*blockchain*): base de datos distribuida de gran tamaño con todos los registros (bloques) enlazados y cifrados para garantizar seguridad y privacidad
- Diseñado para que los bloques no se puedan modificar ni revisar en el futuro
- Debe haber usuarios participantes que validen cada nuevo bloque a través de un consenso sin necesidad de una autoridad central
- Primer uso en la criptomoneda bitcoin
- Aplicaciones: gestión de pagos, gestión de identidad, gestión del voto, registro de eventos, registros médicos…



Cadenas de bloques



Cadenas de bloques



"I don't understand the blockchain hype. A startup has certified my artwork & placed their verification on the bitcoin blockchain. Now art dealers & auctioneers can feel secure that I am the original artist. One small problem… I am not Leonardo da Vinci!"

(Terence Eden, 2018)

http://www.verisart.com/works/23f2c64a-08c6-4a42-8013-84ac8422dffb

Redes

WiFi propia

- No dejar la red abierta
  - No usar WEP, muy fácil de romper
  - Usar configuración WPA2 si es posible
- Cambiar las claves por defecto
  - La de administración del router
  - La de la conexión a la red
  - Cambiarlas periódicamente
- Si tenemos que compartirla (en un negocio)
  - Utilizar dos redes: propia e invitados
  - Que sea fácil de reconocer

Protocolos de cifrado en WiFis

- WEP (*Wired Equivalent Privacy*)
  - Objetivo: privacidad comparable a la de redes con cable
  - Actualmente se puede romper en pocos minutos
- WPA (*WiFi Protected Access*)
  - Solución intermedia para hardware que no soporta WPA2
- **WPA2**
  - Mucho más seguro que los anteriores
  - Varios sistemas de cifrado de claves
    - TKIS: poco seguro
    - **AES**: el más seguro
    - TKIS/AES: menor seguridad y mayor compatibilidad

WiFi ajena

- Usar solo conexiones https o vpn
- Conectarse solamente a redes “conocidas”

Móviles y otros dispositivos

Consejos para móviles

- Conocer el IMEI (para saberlo: *#06#)
  - Permite bloquear el dispositivo si es necesario
- Activar el bloqueo automático
  - Y utilizar un pin, patrón de desbloqueo, huella digital...
- Hacer copias de seguridad
- Tener el contenido cifrado
- Instalar un antivirus
- Cuidado con apps alternativas o no instaladas a través del mecanismo oficial
- Cuidado con llamadas desconocidas
- Recordar que es fácil perderlos

Ubicación del móvil

- Se puede conocer la ubicación del móvil: GPS, radio…
- Historial de ubicación: almacena la información de todos los lugares en que el móvil ha estado
- Geoetiquetado: añade a las fotos información (metadatos) sobre el lugar donde se tomó
- Es recomendable desactivar la ubicación para todo el móvil
- Si desactivamos la localización para la cámara, no se podrá mostrar automáticamente ubicación al compartir una foto
- Ventajas e inconvenientes
  - ✓ Seguridad y privacidad
  - ✗ Se desactivarán funciones útiles

Gestión de dispositivos

- Diferentes dispositivos para diferentes funciones
  - Portátil para trabajo, móvil para ocio…
- Si un dispositivo se usa para cosas serias
  - No instalar otros programas
  - No navegar (si el trabajo no lo requiere)
  - No jugar
- Como mínimo, utilizar diferentes usuarios
  - Privilegios de administrador solo si hace falta: cuantos menos privilegios tenga el malware, menos daño hará
  - Un usuario diferente para hacer pagos

Navegación

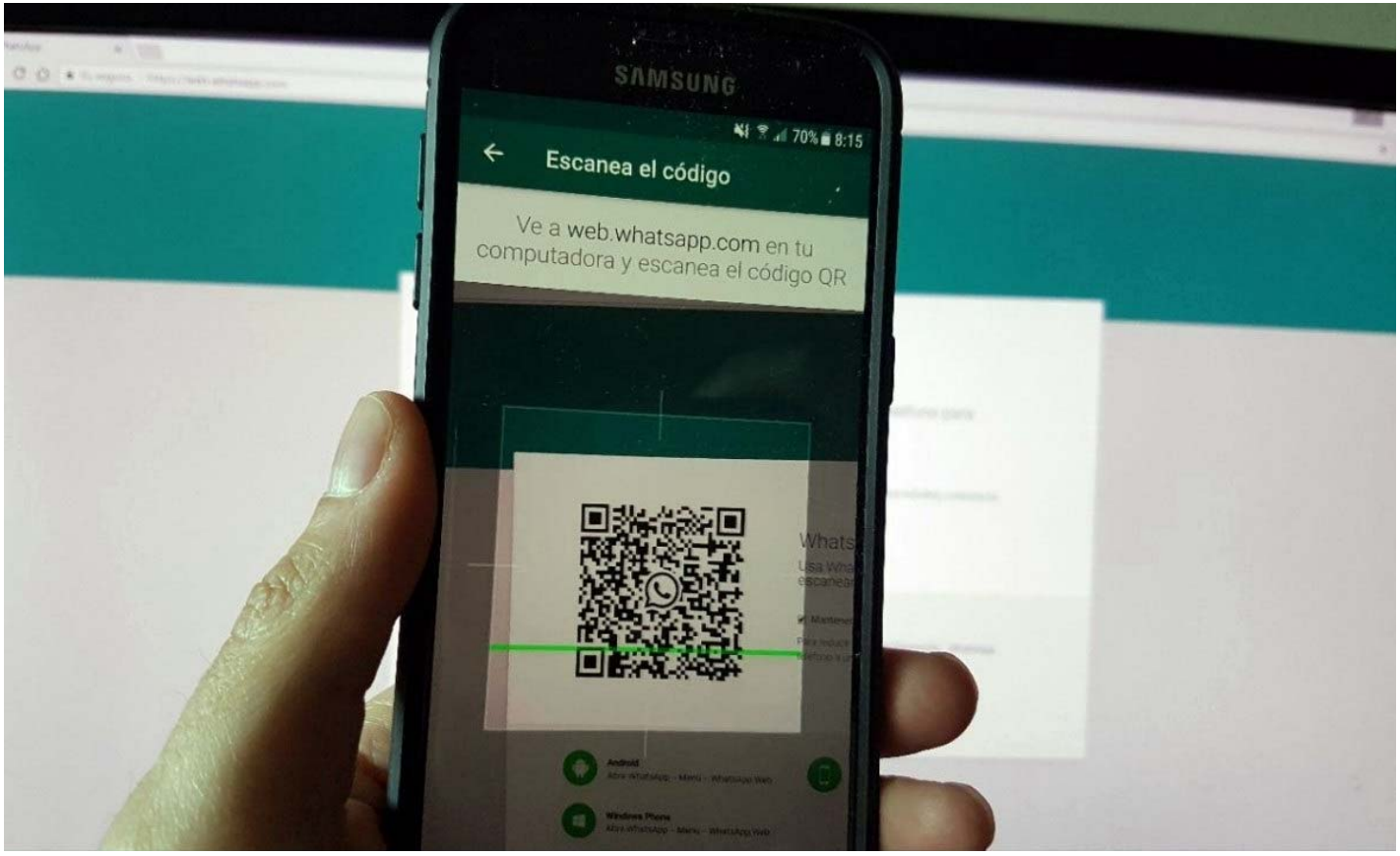
Conectarnos a sitios confiables

Instalar programas desde sitios confiables

Cuidado incluso en sitios confiables

Whatsapp Web

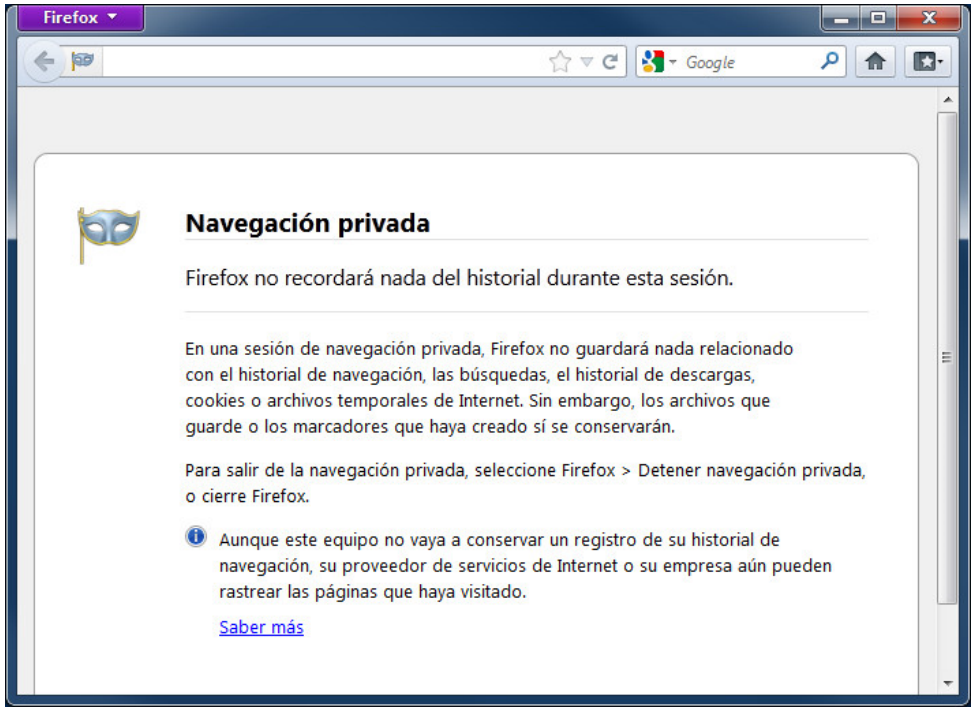
- Permite usar Whatsapp desde el navegador de un ordenador
- Requiere conexión a Internet en el móvil y el ordenador



Whatsapp Web

Ventanas privadas

- Ventanas privadas o de incógnito: ventanas especiales del navegador Web que casi no almacenan datos de navegación
  - No recuerda historial, búsquedas, formularios, cookies…
- Para nueva ventana y para abrir enlace en nueva pestaña



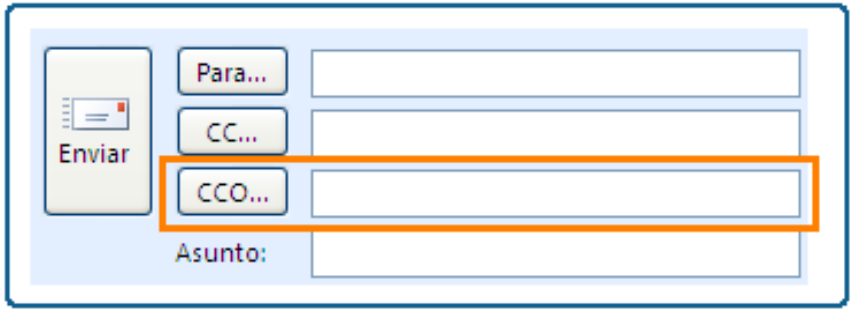
Pagos electrónicos

- PayPal y similares evitan dar nos de cuenta o de tarjeta
- Para pagar
  - Siempre con protocolos seguros (https)
  - Usar una tarjeta virtual para Internet (cibertarjeta)
  - Ver si todo es razonable: avisos legales, contacto...
  - Buscar en la Web quién lo está usando
  - Hacer pruebas con pequeñas cantidades de dinero
- Para cobrar
  - Usar una cuenta bancaria solo para cobros
  - Pasarela de pago: tecnología para pago telemático de los usuarios, el banco proporciona códigos para configurarla
  - ¿Pagos por transferencia, contra reembolso...?

Correo electrónico

Envíos y reenvíos de emails

- Nunca enviar información sensible por email
- Reenviar solamente los correos legítimos
- ¿Mostrar la dirección del remitente del mensaje reenviado?
  - Al reenviar un correo se añade automáticamente como parte del cuerpo del mensaje, pero la podemos borrar
- ¿Dejar que los destinatarios vean la dirección de los demás?
  - Cuidado, es incluso un delito sancionable
  - Evitarlo con copia de carbón oculta (CCO o BCC)



Spam

Cialis©/Viagra©		**Customer Notice: Renewal** - Cialis© & Viagra© Joint-Corporate Reminder of Re-Order/Renewal. As a valu	18-Mar
Ed Store	»	**Relax and take the time** - VIAGRA If you have a problem getting or keeping an erection, your sex life can	17-Mar
Isiah Young	»	**Why be an average guy any longer** - Several millions men have been helped with the potent ingredients	17-Mar
Ed Store	»	**Relax and take the time** - VIAGRA If you have a problem getting or keeping an erection, your sex life can	17-Mar
Viagra	»	**Sex can be enjoyable** - VIAGRA If you have a problem getting or keeping an erection, your sex life can su	17-Mar
Angelic Phillips		**mertv dogadatsia** - to greet my friend the tin woodman." for ned was so absorbed in business that he igno	17-Mar
Trey Spangler		**The Deal on OEM Software?** - And still my mind goes groping in the mud to bring Cascading snowflakes	17-Mar
Weight Loss	»	**Brazilian Weight Loss** - BugreLife™ - Weight Loss Secret From Brazil: Faster Metabolism Better Circulat	17-Mar
Lane Jackson	»	**Need S0ftware?** - OEM software: - don`t need packing case - save your money. - instant download instead	17-Mar
Elizabeth	›	**Fun dates** - Find women from your state to date. http://www.geocities.com/vymedisy84761 is the weaker s	17-Mar
Ernest	›	**Tommy Lee uses Man XL** - EnlargeYourPenis! http://www.geocities.com/sabedavu78497 Studies show if	17-Mar
Brennan Richardson	»	**Vlsta, 0fflce 2007 & Acrobat 8 79$ at Darr's** - All Titles On Speclal on Mar 16 00:30:00 MSK 2007 MICR0S	17-Mar
Luis	›	**Customer service** - Get all of your medical supplies here. http://www.geocities.com/vydudyse77204 Our pr	17-Mar
Clarence Miller	›	**Think I Can Help You With This** - space "No, hourly teaching count," worry replied Monte Cristo taking th	17-Mar
Gregory Ward		**Sorry For Being Late** - sorry, but i can't this time. don't you worry; iof saxifrage.jinjur take possession of ..	17-Mar
BugreLife	»	**Brazilian Weight Loss** - BugreLife™ - Weight Loss Secret From Brazil: Faster Metabolism Better Circulat	17-Mar
Oliver Johnson	»	**She will love you more than any other guy** - Several millions men have been helped with the potent ingr	17-Mar
me	»	**[Bucks place] Please moderate: "Certain Blogs are driving me mad"** - A new comment on the post #	17-Mar
ForumsMac DWI	»	**Attract any woman!.** -	17-Mar
Naren Stratton	»	**VISTA, 0FFICE & ACR0B8T 4less from Juliet** - All Titles On Speclal on Mar 17 04:30:00 MSK 2007 MICR(	17-Mar
Mem-Turbo	»	**Instructions To Increase PC and Internet Speed** - Your PC may be suffering from serious memory leaks	17-Mar
Tona Meyer	›	**Important For Tomorrow** - I do." "Is hid government sky it then so vesical terrible a poison?" "The ...	17-Mar
rogio	›	**Do her right every night with Viagra Professional.** - Viagra Pro is the combination of the best and the n	17-Mar
Viagra	»	**Sex can be enjoyable** - VIAGRA If you have a problem getting or keeping an erection, your sex life can su	17-Mar
Gabriel Garcia	»	**Three Steps to the Software You Need at the Prices You Want** - OEM software - throw packing case, l	17-Mar
Nancy		**Check out profiles of women looking for dates** - Chat and meet with ready, willing and able women from	17-Mar
Chris		**DO you hit her pleasure zone** - EnlargeYourPenis! http://www.geocities.com/vibycyxi39504 Studies show	17-Mar

Spam

- Spam: mensajes no solicitados y no deseados, normalmente de tipo publicitario, enviados en cantidades masivas a múltiples usuarios
- Los servidores de correo tienen mecanismos (imperfectos) para identificarlo automáticamente
  - Revisar la carpeta por los falsos positivos
- Ayudar al aprendizaje del servidor
  - Indicar falsos positivos: no es spam
  - Indicar falsos negativos: marcar como spam
- Responder puede ser contraproducente (aunque sea para anular la subscripción): estamos confirmado que la dirección de e-mail se usa

Bulo

- Bulo (*hoax*): noticia falsa, quiere ser divulgada masivamente
- ¡No crearlos ni difundirlos!
- Algunos posibles objetivos:
  - Obtener direcciones de e-mail o contraseñas
  - Manipular la opinión pública (e.g., fomentar el racismo)
  - Normalmente, no hay objetivo económico directo (pero se puede pretender perjudicar la imagen de un competidor)
- Algunas pistas que deben hacer sospechar:
  - No tienen fuentes o no son fuentes fiables
  - Redacción atemporal para que pervivan mucho tiempo
  - Errores ortográficos o gramaticales
  - Solicitud de reenvío de la información

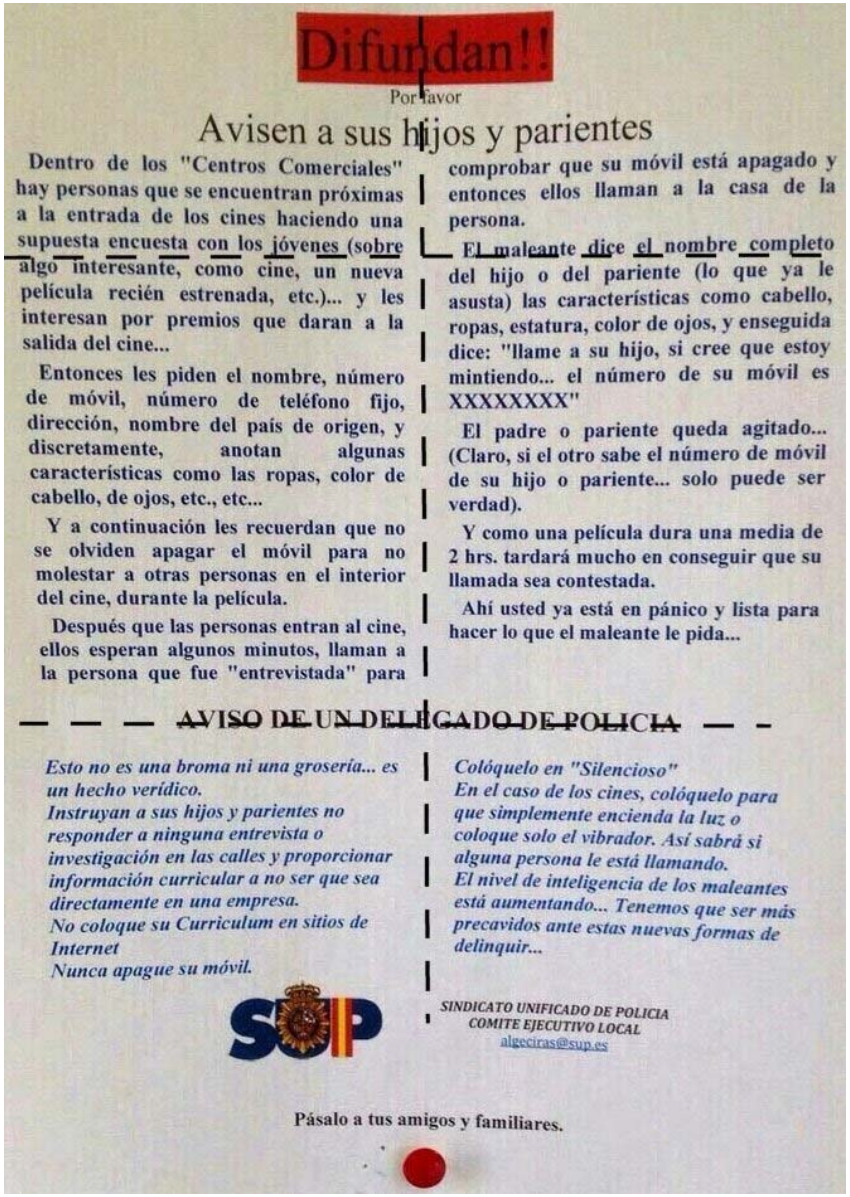
Bulo


... Y SI NO REENVÍAS ESTA CARTA A POR LO MENOS 15 AMIGOS, TENDRÁS VARIOS AÑOS DE MALA SUERTE...
www.klip7.cl

Bulo


December 12 at 12:59pm · Duisburg, Germany ·
Aus dem aktuellen IKEA-Katalog 2016 und kostet 88€
See Translation
29k Likes 22k Comments 11k Shares
Like
Comment
Share

Bulo



Difundan!!

Por favor

Avisen a sus hijos y parientes

Dentro de los "Centros Comerciales" hay personas que se encuentran próximas a la entrada de los cines haciendo una supuesta encuesta con los jóvenes (sobre algo interesante, como cine, un nueva película recién estrenada, etc.)... y les interesan por premios que daran a la salida del cine...

Entonces les piden el nombre, número de móvil, número de teléfono fijo, dirección, nombre del país de origen, y discretamente, anotan algunas características como las ropas, color de cabello, de ojos, etc., etc...

Y a continuación les recuerdan que no se olviden apagar el móvil para no molestar a otras personas en el interior del cine, durante la película.

Después que las personas entran al cine, ellos esperan algunos minutos, llaman a la persona que fue "entrevistada" para comprobar que su móvil está apagado y entonces ellos llaman a la casa de la persona.

El maleante dice el nombre completo del hijo o del pariente (lo que ya le asusta) las características como cabello, ropas, estatura, color de ojos, y enseguida dice: "llame a su hijo, si cree que estoy mintiendo... el número de su móvil es XXXXXXXX"

El padre o pariente queda agitado... (Claro, si el otro sabe el número de móvil de su hijo o pariente... solo puede ser verdad).

Y como una película dura una media de 2 hrs. tardará mucho en conseguir que su llamada sea contestada.

Ahí usted ya está en pánico y lista para hacer lo que el maleante le pida...

— — — AVISO DE UN DELEGADO DE POLICIA — —

Esto no es una broma ni una grosería... es un hecho verídico.
Instruyan a sus hijos y parientes no responder a ninguna entrevista o investigación en las calles y proporcionar información curricular a no ser que sea directamente en una empresa.
No coloque su Curriculum en sitios de Internet
Nunca apague su móvil.

Colóquelo en "Silencioso"
En el caso de los cines, colóquelo para que simplemente encienda la luz o coloque solo el vibrador. Así sabrá si alguna persona le está llamando.
El nivel de inteligencia de los maleantes está aumentando... Tenemos que ser más precavidos ante estas nuevas formas de delinquir...

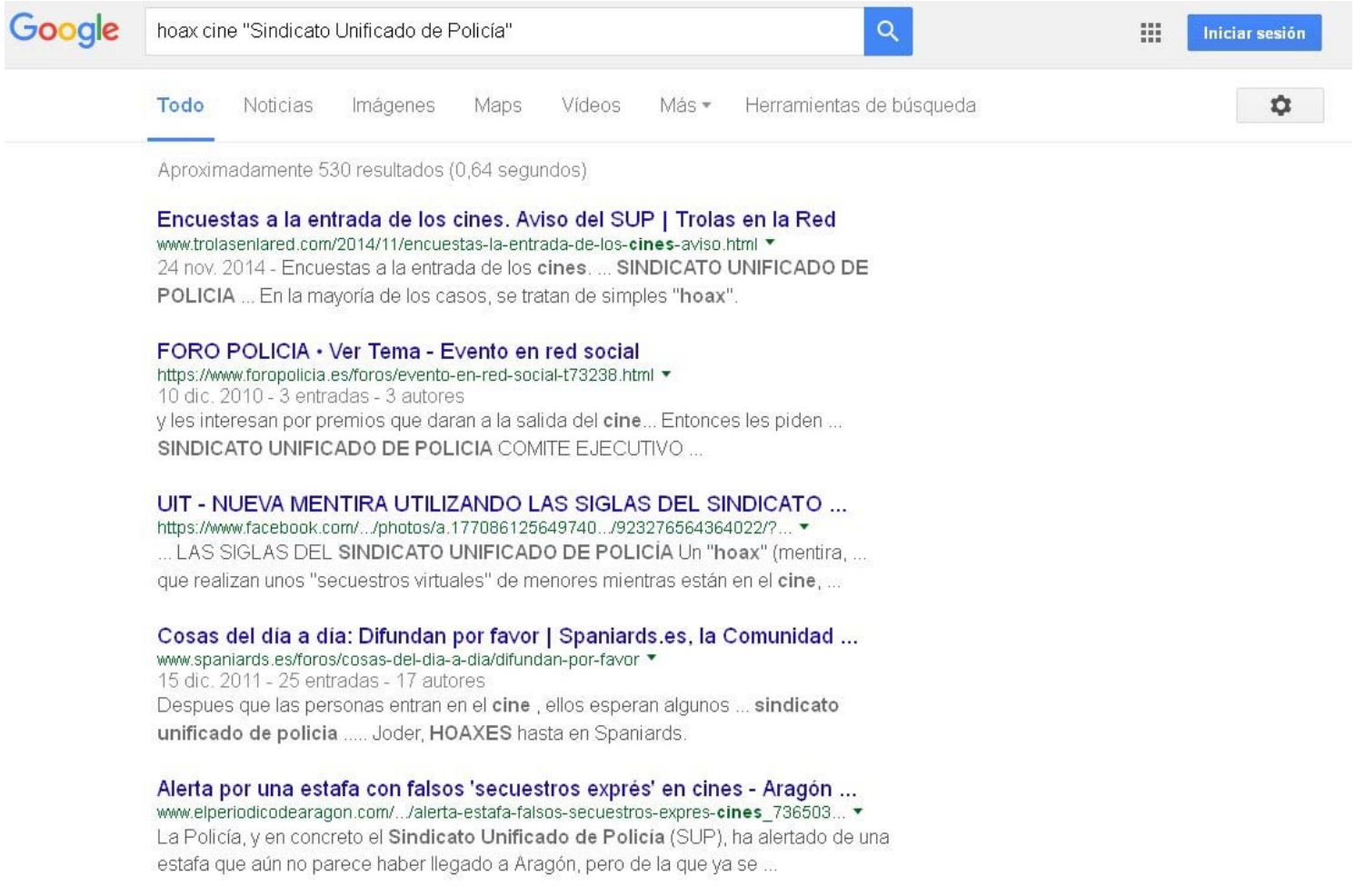
SUP

SINDICATO UNIFICADO DE POLICIA
COMITE EJECUTIVO LOCAL
algeciras@sup.es

Pásalo a tus amigos y familiares.

Bulo

- Comprobar buscar en la Web antes de reenviar

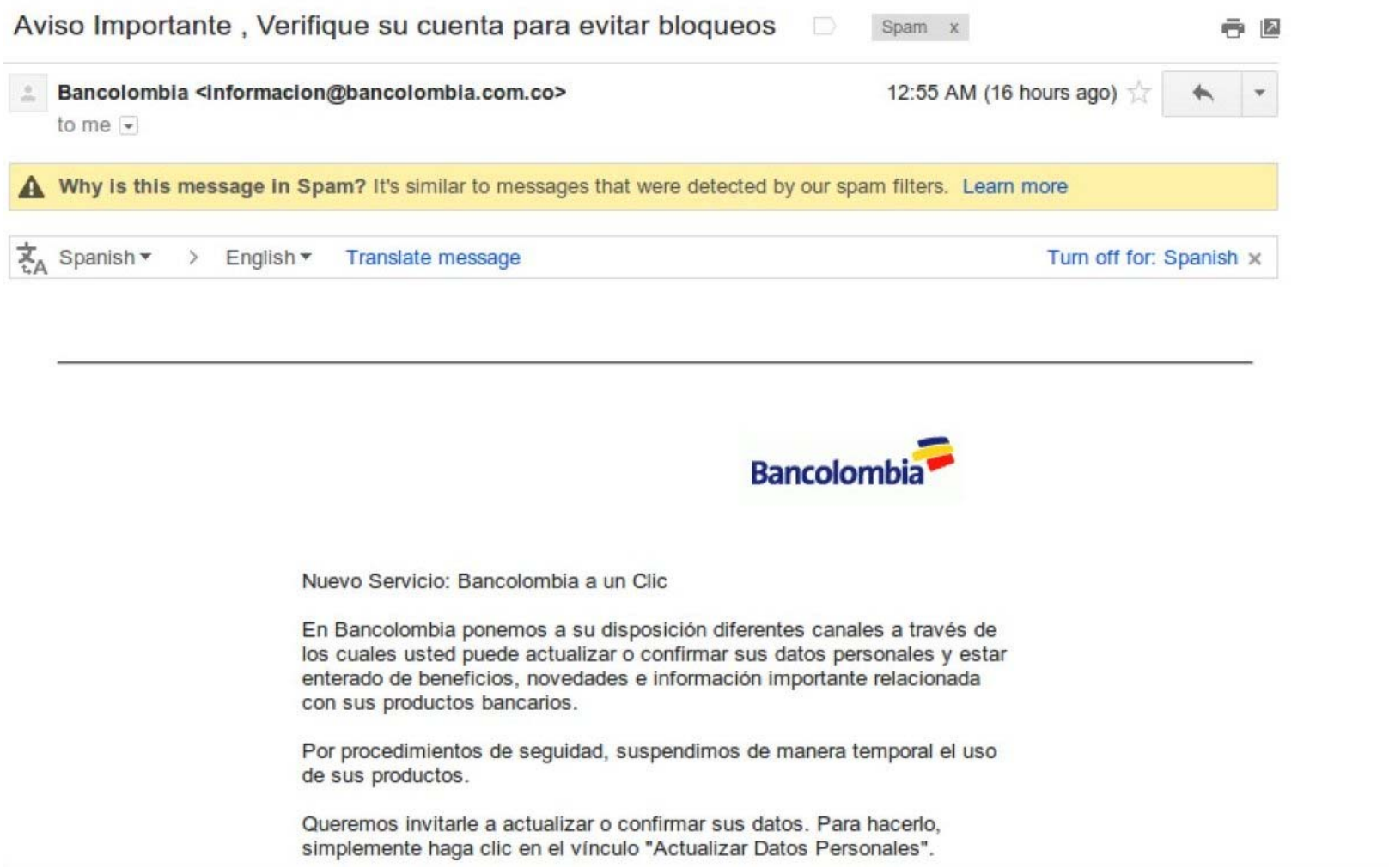


Phishing

- *Phishing*: suplantación de identidad consistente en hacerse pasar por alguien de la confianza del usuario para obtener información privada o conseguir que ejecute algún malware

El enlace redirige a un archivo que secuestra los datos del usuario

Phishing



Aviso Importante , Verifique su cuenta para evitar bloqueos

Spam x

Bancolombia <informacion@bancolombia.com.co>

to me

12:55 AM (16 hours ago)

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

Spanish > English Translate message

Turn off for: Spanish

Bancolombia

Nuevo Servicio: Bancolombia a un Clic

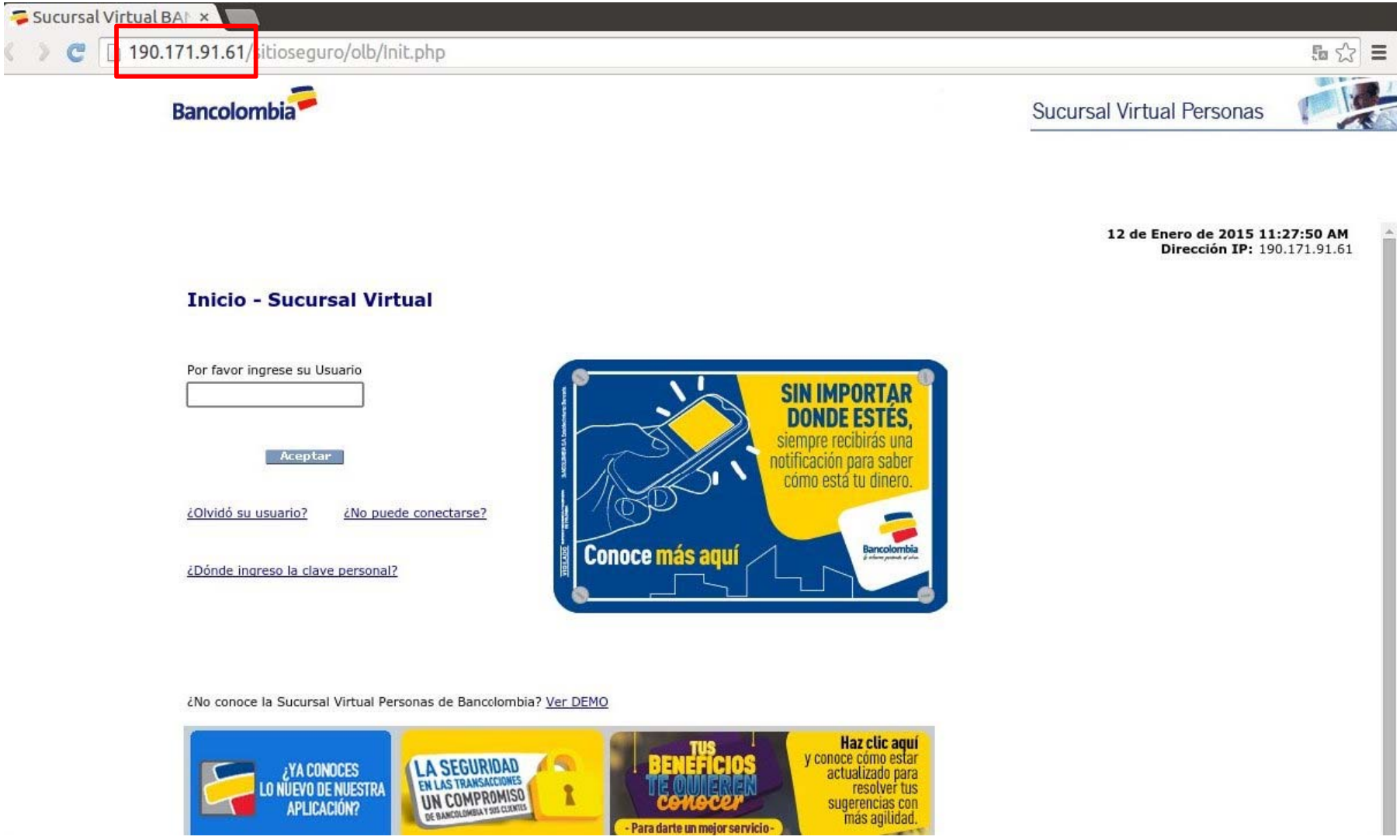
En Bancolombia ponemos a su disposición diferentes canales a través de los cuales usted puede actualizar o confirmar sus datos personales y estar enterado de beneficios, novedades e información importante relacionada con sus productos bancarios.

Por procedimientos de seguidad, suspendimos de manera temporal el uso de sus productos.

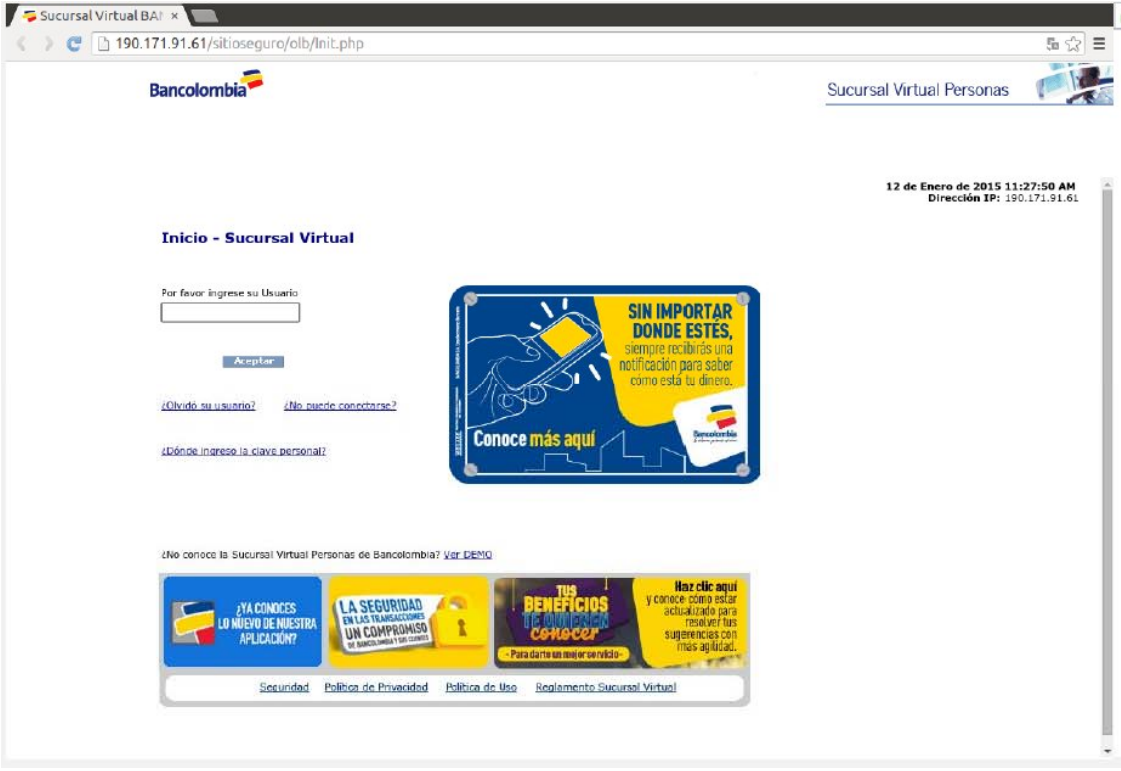
Queremos invitarle a actualizar o confirmar sus datos. Para hacerlo, simplemente haga clic en el vínculo "Actualizar Datos Personales".

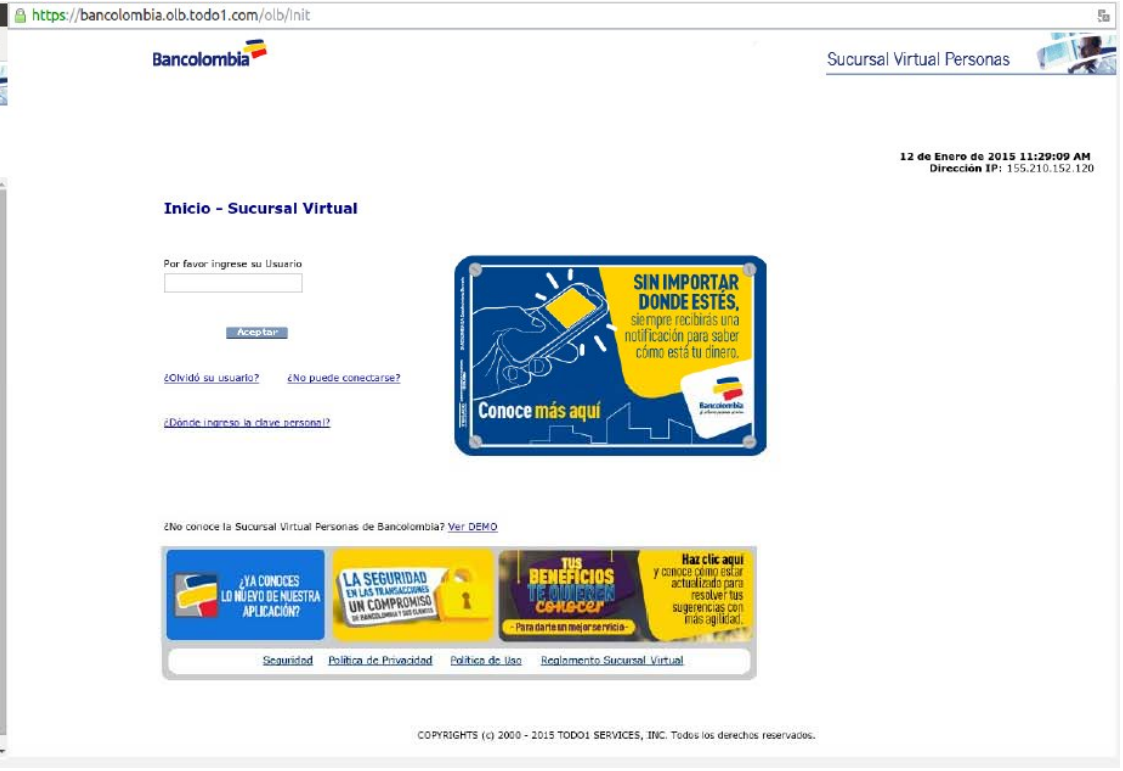
http://www.gremios-unoa.com/css?https=aunclic=http://www.grupbancolombia.com/

Phishing


Sucursal Virtual BA
190.171.91.61/sitioseguro/olb/Init.php
Bancolombia
Sucursal Virtual Personas
12 de Enero de 2015 11:27:50 AM
Dirección IP: 190.171.91.61
Inicio - Sucursal Virtual
Por favor ingrese su Usuario
Aceptar
¿Olvidó su usuario?
¿No puede conectarse?
¿Dónde ingreso la clave personal?
SIN IMPORTAR DONDE ESTÉS,
siempre recibirás una notificación para saber cómo está tu dinero.
Conoce más aquí
Bancolombia
¿No conoce la Sucursal Virtual Personas de Bancolombia? Ver DEMO
¿YA CONOCES LO NUEVO DE NUESTRA APLICACIÓN?
LA SEGURIDAD EN LAS TRANSACCIONES UN COMPROMISO DE BANCOLOMBIA Y SUS CLIENTES
TUS BENEFICIOS TE QUIEREN conocer
- Para darte un mejor servicio -
Haz clic aquí
y conoce cómo estar actualizado para resolver tus sugerencias con más agilidad.

Phishing





http://190.171.91.61/sitioseguro/olb/Init.php https://bancolombia.olb.todo1.com/olb/Init.php

Phishing

- https garantiza que la conexión es segura (cifrada)
  - ¡Pero no garantiza que esa sea la conexión correcta!
- En vez de pinchar el enlace:
  - Acceder desde los marcadores
  - Escribir la URL
- En caso de duda:
  - Buscar en la Web
  - Preguntar
- Plantearnos si es el mecanismo usual de proceder
- Plantearnos si les hemos dado nuestra dirección de e-mail

Phishing

From: Facebook <noreply@face-book.com>
To: [redacted]
Subject: Felicitaciones desde Facebook
Date: Tue, 10 Feb 2015 11:57:16 -0600
Reply-To:

Felicitaciones!

Estamos muy contentos de informarle que su nombre aparece en la promoción d
de facebook para el año 2015 y le estamos dando a la suma total de
$550.000 USD (cinco cientos y cincuenta mil dólares estadounidenses) a nues
ganadores, que es la suma que has ganado. Su nombre fue seleccionado en un
realizó para este año, así que necesitamos su respuesta rápida así podemos
la entrega de su fondo.

Sólo seleccionamos 20 veinte candidatos por-anualmente como nuestros ganado
de sistema de votación electrónico (EBS) sin aplicar el candidato, le felic
uno de nuestros afortunados ganadores. Nuestros ganadores incluyen tanto lo
no abonados de FACEBOOK.

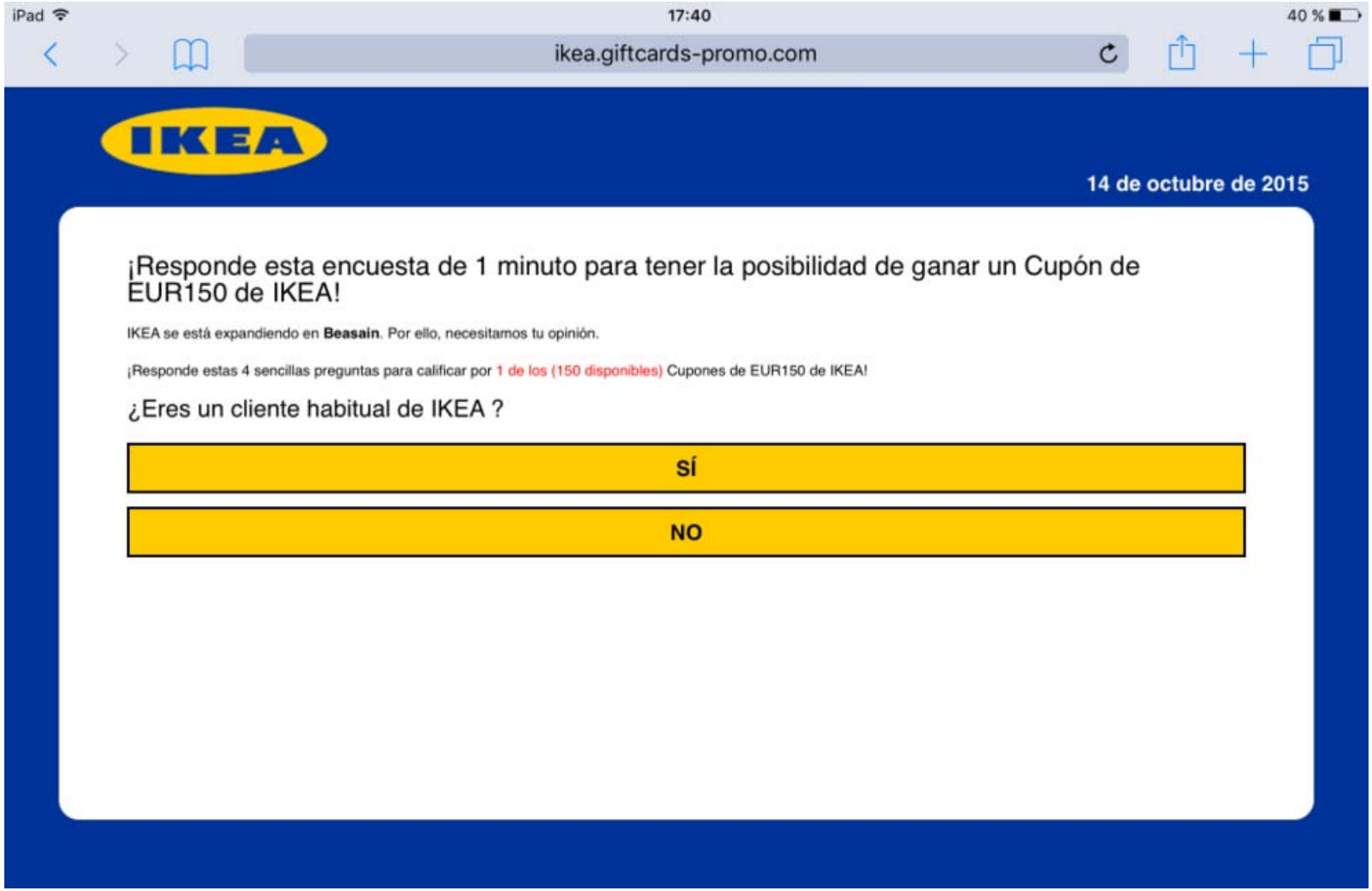
Su nombre fue seleccionado por el Sr. Mark Zuckerberg el CEO de Facebook (f

Parecido no
es lo mismo

Phishing

Ejecutamos un fichero infectado

Phishing



Obtienen nuestros datos personales

Redes sociales y mensajería instantánea

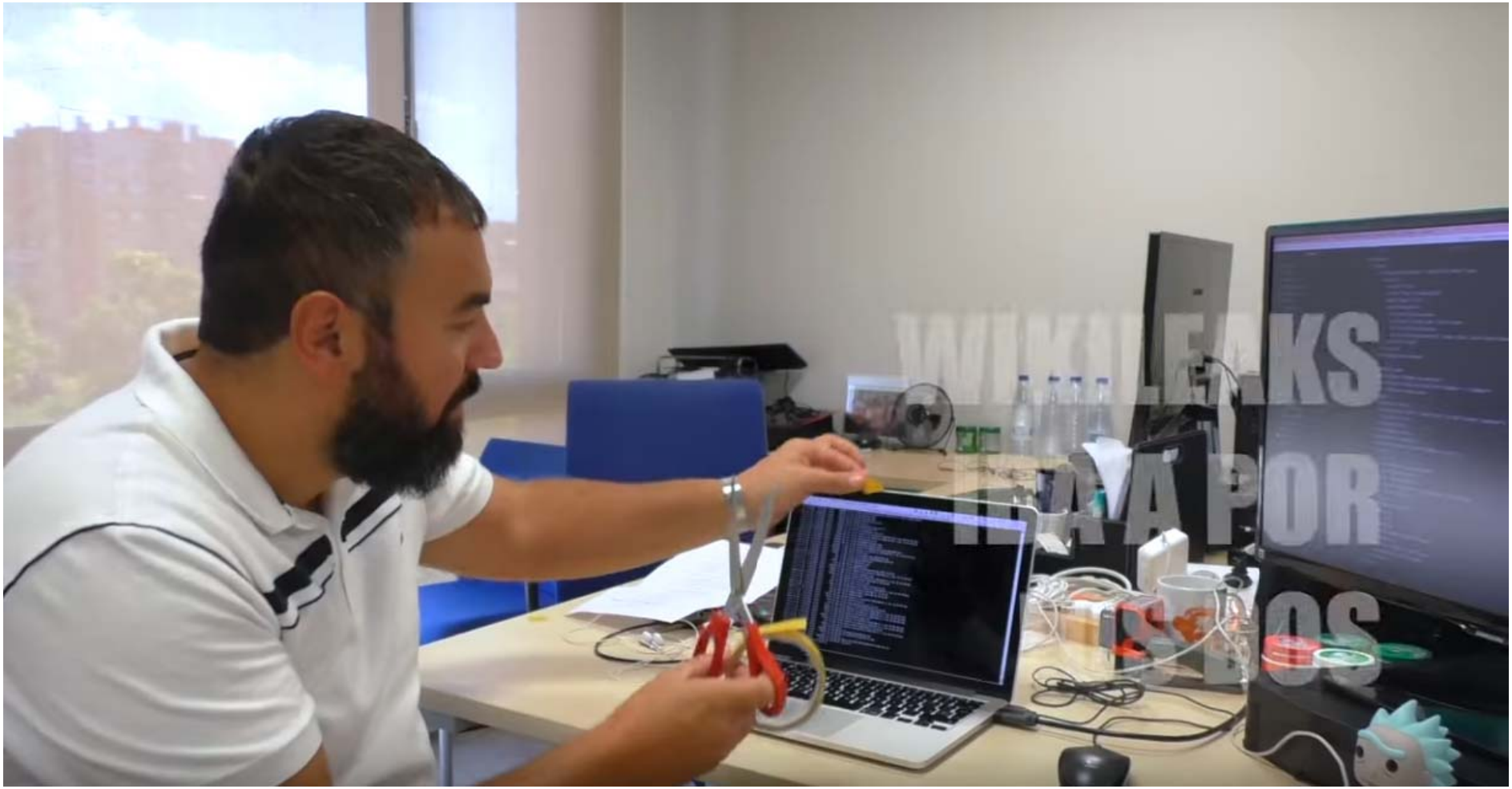
Consejos en redes sociales y mensajería instantánea

- Aprender y comprender las opciones de privacidad
  - ¿Quién puede ver las fotos? ¿Y si etiquetamos a otro?
- Escoger cuidadosamente los contactos
  - Diferentes contactos en cada red social, e.g., Facebook para amigos, LinkedIn para trabajo, Twitter para todos…
- Escoger qué compartimos con quién
  - Grupos de usuarios: no compartir todo con todos
  - Nunca información delicada (dónde vivo, dónde estoy) y mucho menos con desconocidos
- No publicar/difundir rumores ni imágenes/vídeos sin permiso
  - Rectificar y reconocer los errores
  - Retirar la información o material que nos soliciten

Conclusiones

- La red fue diseñada para fiabilidad y robustez, no seguridad
- Mejor prudente y cuidadoso que excesivamente rápido
- En algunos casos, la comodidad es enemiga de la seguridad
- La seguridad es un proceso
- Seguridad como gestión del riesgo
- No hay sustitutos para la sensatez y la prudencia

Conclusiones



http://www.youtube.com/watch?v=UIbBMmWjBnc