SEGURIDAD Y RIESGOS EN INTERNET: DELITOS INFORMÁTICOS

D. Francisco Javier Marzo

Ingeniero Superior Industrial, experto en delitos tecnológicos

TROYANOS

Control total del ordenador o móvil por terceras personas

- Capturan pulsaciones de teclas (numeración tarjetas, claves cuentas bancarias, correos…)
- Graba vídeos del movimiento del ratón
- Control de la webcam
- Acceden a archivos (fotos, vídeos, documentos…)

TROYANOS

Formas de infectarse:

- Sistema operativo o programas (aplicaciones) desactualizado
- Adjuntos (falsean remitente en correos y SMS)
- Enlaces a webs maliciosas
- Descargas
- «Amigos» con acceso físico al ordenador

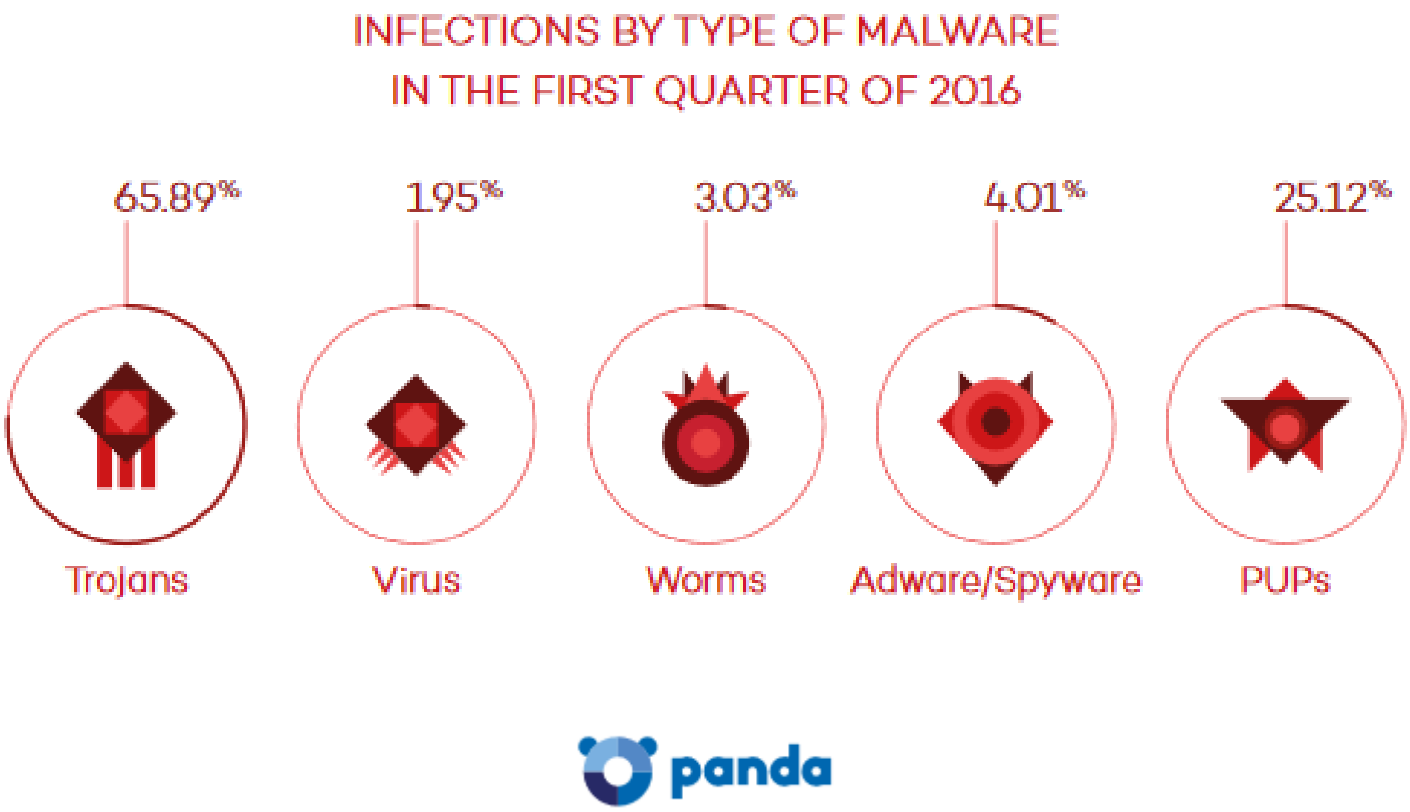
Windows y Mac: Los antivirus los detectan tarde y mal

TROYANOS

Utilidades:

- Dinero: claves bancarias, tarjetas, claves de correos, PayPal…
- Espiar y robar información
- Pornografía infantil robando cuentas de menores
- Usar la conexión de Internet para cometer delitos
- Botnets: Spam, ataques DNS…

INFECCIONES POR TIPO DE MALWARE



RANSOMWARE.- DEFINICIÓN

Malware (normalmente troyano)

Encripta archivos (documentos, imágenes, vídeos…)

Pide un rescate para recuperarlos

Pagar no garantiza recuperarlos

Muchos tipos de ransomware no tienen todavía solución a corto plazo

RANSOMWARE.- INFECCIÓN

Correo: adjunto o enlace

Visitar web infectada: scripts maliciosos

Ataca sobretodo a Windows y algo a Android

Infecta también carpetas compartidas de la Red, Dropbox…

RANSOMWARE.- CONSEJOS

COPIA DE SEGURIDAD:

- ✓ De archivos importantes
- ✓ Física: No conectada al PC
- ✓ Online: no las que se basan en carpeta compartida (Dropbox)
- ✓ Única opción contra ransomware (encripta archivos y pide rescate)
- ✓ *Solo hay dos tipos de personas: los que han perdido alguna vez todos sus datos y los que están a punto de perderlos*

RANSOMWARE RESPONSE KIT:

https://bitbucket.org/jadacyrus/ransomwareremovalkit/overview

RANSOMWARE.- CONSEJOS

No abrir adjuntos o enlaces sospechosos

NoScrip y uBlock Origin de Firefox navegando

Copia de seguridad online no vinculada a una carpeta: Google Drive, Mega…

Usar Linux

Sistema Operativo, programas, antivirus, antiespía y cortafuegos actualizados

RANSOMWARE.- CONSEJOS

Mostrar extensiones de nombres de archivos:

http://windows.microsoft.com/es-es/windows/show-hide-file-name-extensions#show-hide-file-name-extensions=windows-7

Android, si no encripta se puede **desbloquear**:

- Buscando en Google el texto que aparece en el terminal
- Reseteando a valores fábrica el terminal (podemos perder información)

RANSOMWARE.- EJEMPLO 1

lun 16/03/2015 11:20

Legalización de Documentos

Para

Mensaje | Legalización Exportación-Correo Expres 2015.pdf.zip (209 KB)

Buenos días,
Continuando conversación telefónica, le remitimos nuestra propuesta que esperamos sea de su interés.

lun 16/03/2015 11:52

factura electrónica

Para

Mensaje | factura electrónica NOMBRE 6781743.xls.zip (45 KB)

Os envío los códigos. Si tenéis algún problema me comentáis.

--- AVISO SOBRE CONFIDENCIALIDAD. La legislación española ampar= el secreto de las comunicaciones. Este correo electrónico y sus an=xos son
estrictamente confidenciales. Si Vd. no es el destinatario d=l mismo, por favor, notifíquenoslo inmediatamente y destruya el ori=inal. No deberá copiar
este mensaje ni sus anexos o usarlo para=propósito alguno, ni divulgar su contenido a ninguna persona.

RANSOMWARE.- EJEMPLO 2

Movistar

Factura sin Papel: Sus últimas facturas ya están disponibles

Para

Mensaje factura electronica (sin papel).zip (44 KB)

movistar

Estimado Cliente,

Ya puede **consultar sus facturas** telefónicas de fecha 14/jul/2015 o descargarse los archivos pdf que le adjuntamos en esta comunicación y que contienen una hoja resumen de cada una de ellas.

ATENCIÓN: Por favor, no responda a este mensaje, este buzón no es atendido. Si tiene alguna duda, estamos a su servicio en el apartado de Ayuda en movistar.es y en el 1489. Si desea actualizar la dirección de e-mail en la que recibe el aviso de disponibilidad de factura, acceda con sus claves de usuario al apartado Ayuda, gestión de e-Factura.

TELEFONÍA.- CONSEJOS

No fiarse de llamadas recibidas

- Mienten
- No dar datos personales o bancarios a nadie

No fiarse de mensajes recibidos

- Se puede falsear el remitente
- No instalar APP recibidas por mensaje

TELEFONÍA.- CONSEJOS

Llamando al operador:

- Eliminar llamadas a números de tarificación adicional (905, 806, 803, 807)
- Eliminar mensajería Premium
- Eliminar llamadas al extranjero

Nueva ley SMS Premium impide:

- Suscripciones a través de Internet, o de la instalación de *apps*,
- Que el número de tarificación adicional figure como identificador

TELEFONÍA.- CONSEJOS

Configurar el bloqueo de pantalla

Delitos:

- Amenazas, insultos, estafas…
- Instalar APP para grabar las conversaciones

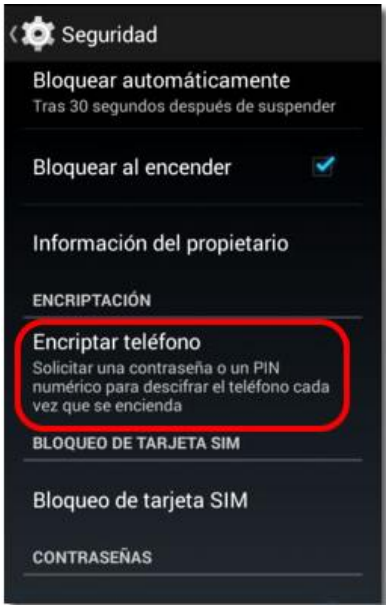
No contactar con mensajes al contestador ni de regalos.

Alargar enlaces cortos: http://longurl.org/

TELEFONÍA.- CONSEJOS

No almacenes información bancaria:

- ❑Claves
- ❑Nº tarjeta



Encriptar el teléfono

Poner clave a ciertas APPs

Verificación en 2 pasos en la nube que uses de backup

Desactiva pre-visualización de mensajes con pantalla bloqueada

ANDROID

No hacer root

Actualizar Android:

- ✓Sólo usuarios expertos
- ✓Antes hacer un backup

Si se puede, mejor usar CyanogenMod:
http://www.cyanogenmod.org/

Actualizar las APPs

ANDROID

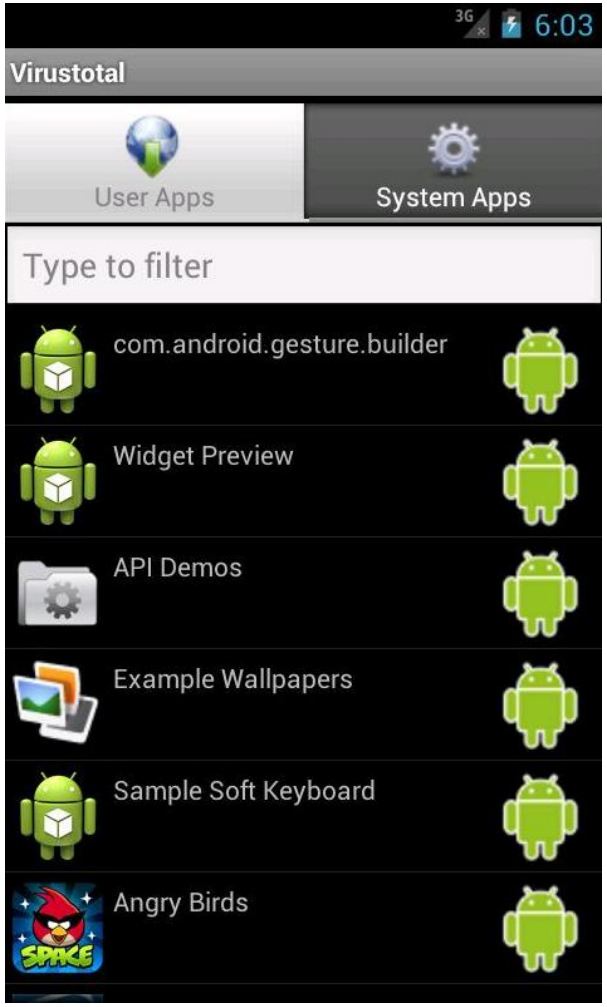
ANTIVIRUS:

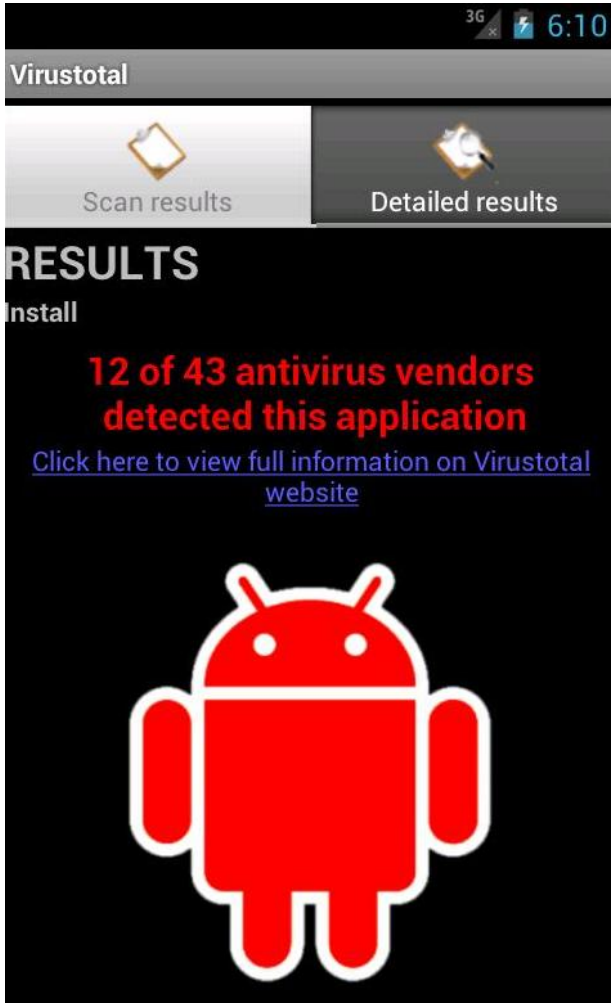
- CM Security, Lookout, TrustGo, avast!
- VirusTotal: 56 antivirus

Conan Mobile: comprueba seguridad

Hacer copia de seguridad de datos personales

ANDROID.- VIRUSTOTAL





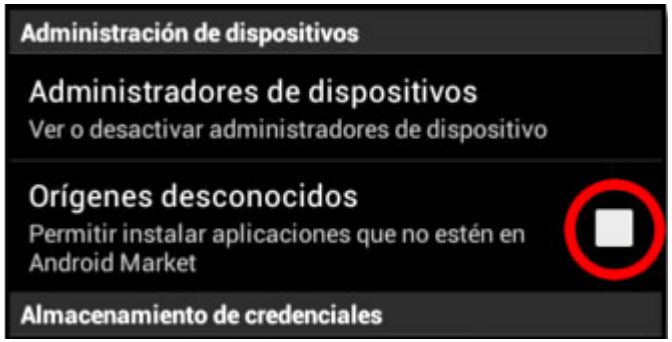
Hacer root SOLO para eliminar troyanos

ANDROID.- APPs

Descargar SOLO de Play Store

Revisar comentarios negativos de otros usuarios

Observar los permisos



Sólo descargar si hay cientos de miles de descargas de otros

Desactivar MMS

ANDROID.- MENSAJES, SMS

SE FALSEA EL REMITENTE

No instalar APPs que nos manden por correo o SMS

No acceder a enlaces económicos (bancos, PayPal…) recibidos por correo o SMS

ANDROID.- ROOT

SuperSU:

https://play.google.com/store/apps/details?id=eu.chainfire.supersu&hl=en

PARA ELIMINAR APPs CON TROYANOS, usar System App Remover:

https://play.google.com/store/apps/details?id=com.jumobile.manager.systemapp&hl=en

Titanium Backup:

https://play.google.com/store/apps/details?id=com.keramidas.TitaniumBackup&hl=en

Greenify:

https://play.google.com/store/apps/details?id=com.oasisfeng.greenify&hl=en

ANDROID.- ENLACES

VirusTotal: https://play.google.com/store/apps/details?id=com.virustotal&hl=en

CM Security: https://play.google.com/store/apps/details?id=com.cleanmaster.security&hl=en

Lookout: https://play.google.com/store/apps/details?id=com.lookout&hl=en

TrustGo Antivirus & Mobile Security:
http://play.google.com/store/apps/details?id=com.trustgo.mobile.security

avast! Mobile Security & Antivirus:
https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity

CONAN Mobile:
https://play.google.com/store/apps/details?id=es.inteco.conanmobile&hl=en

AppLock: https://play.google.com/store/apps/details?id=com.domobile.applock

No hacer jailbreak

Actualizar iOS y APPs.

ANTIVIRUS: Lookout, avast!

Hacer copia de seguridad de datos personales

https://www.osi.es/es/actualidad/blog/2012/06/07/consejos-para-proteger-un-iphone

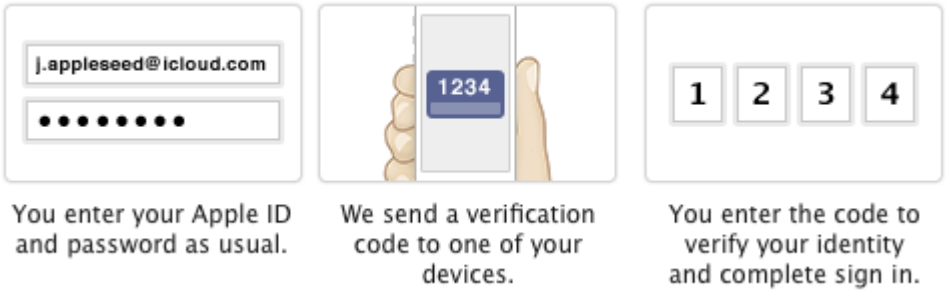
Hace copia en la nube de TODO

Activar opción Busca mi iPhone:

Menú>Ajustes>iCloud

Verificación en dos pasos:

http://support.apple.com/es-es/HT5570



iOS.- APPs

Descargar SOLO de Apple Store

Revisar comentarios negativos de otros usuarios

Observar los permisos

Sólo descargar si hay cientos de miles de descargas de otros

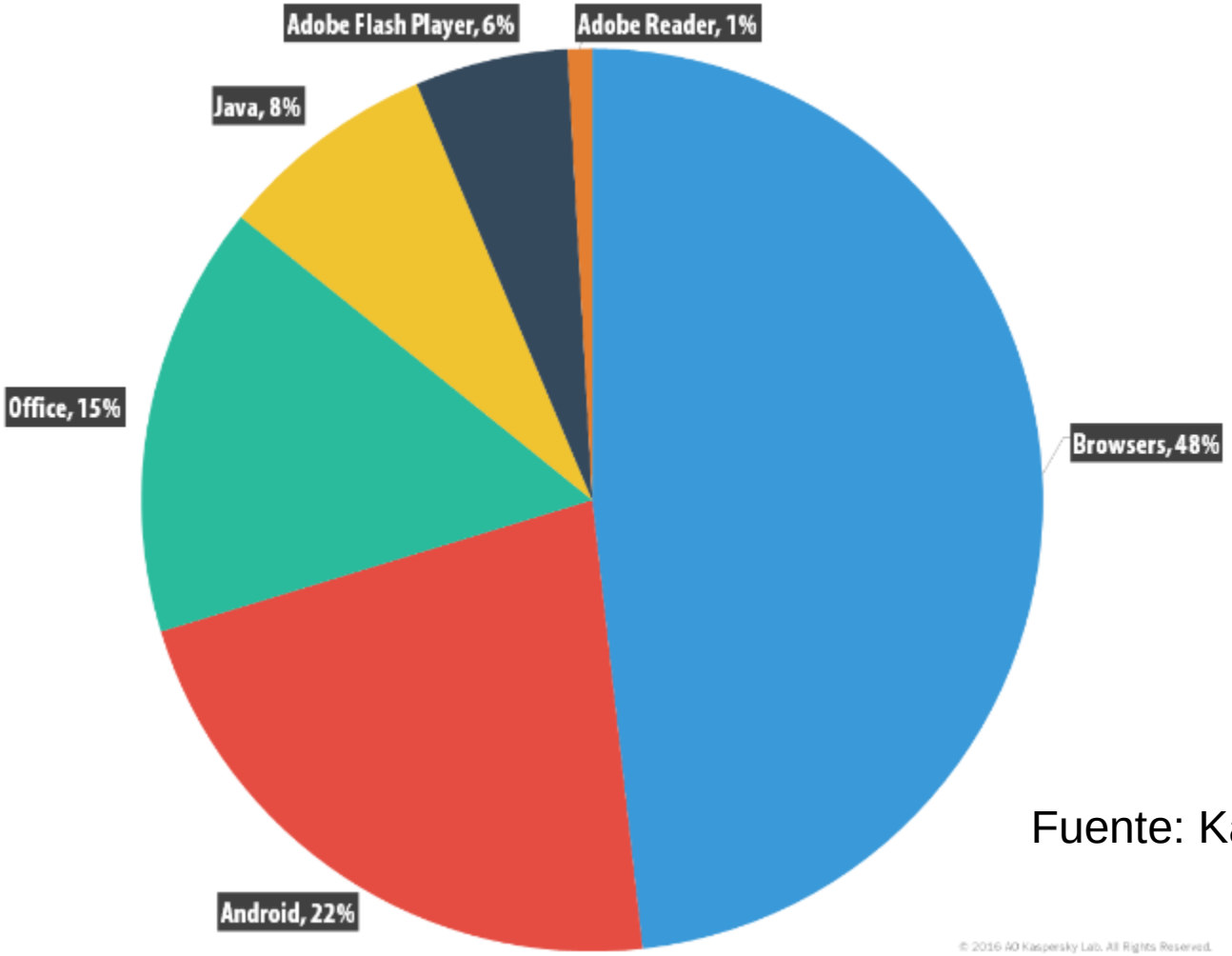
LINUX.- VENTAJAS

Mucho más seguro:

- Apenas tiene malware
- Los programas funcionan por defecto con bajos privilegios
- Código abierto
- Programas y sistema se actualizan con frecuencia
- Programas se instalan desde repositorios de confianza
- No necesitan antivirus ni cortafuegos ni antiespía

Gratis

APLICACIONES VULNERABLES EXPLOTADAS POR CIBERCRIMINALES



Distribution of exploits used in attacks by the type of application attacked, Q1 2016

Fuente: Kaspersky

ACTUALIZAR WINDOWS Y PROGRAMAS:

- Navegadores
- Programas de descarga
- Java
- Otros programas
- Corrige vulnerabilidades críticas
- Actualizar programas con Glary Utilities Free:

http://www.glarysoft.com/glary-utilities/download/

Glary Utilities

WINDOWS

ANTIVIRUS ACTUALIZADO:

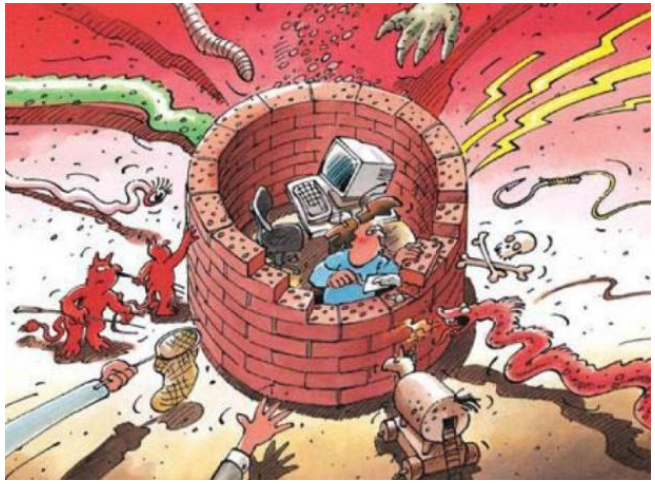
- Sólo UNO
- Comodo Antivirus, Panda Cloud Antivirus, Avira Free, Microsoft Security Essentials, Avast
- Evitar piratear antivirus de pago: troyanos

ANTI-ESPÍAS:

- Superantispyware, MalwareBytes' Anti-Malware, …
- Elimina mejor virus, troyanos y espías
- Elimina programas espía

CORTAFUEGOS O FIREWALL:

- PrivateFirewall, Comodo Firewall, Outpost Firewall Free, Zone Alarm Free, Windows 7 Firewall Control …
- Evita ataques externos o que troyanos o virus que tenemos se conecten sin nuestro permiso a Internet.



privacyware

WINDOWS

DESINFECTA PC:

http://www.osi.es/es/te-ayudamos/desinfecta-tu-ordenador

OSI Oficina de Seguridad del Internauta

ANTIVIRUS ONLINE:

- ✓ Trend, Kaspersky, Eset (Nod32)…
- ✓ No me exime de tener antivirus
- ✓ Hace análisis puntuales

CONTROL DE PROCESOS: CrowdInspect:

http://www.crowdstrike.com/community-tools/

NAVEGADOR

EVITAR EL INTERNET EXPLORER: MUY INSEGURO, especialmente versiones viejas

FIREFOX + COMPLEMENTOS:

- NoScript: bloquea TODOS los scripts
- WOT: advierte de webs maliciosas
- Adblock Plus: bloquea publicidad
- Ghostery: bloquea rastreadores
- El más seguro: tiene NoScript

NAVEGADOR

CHROME + EXTENSIONES:

- ScriptSafe: inferior al NoScript
- WOT: advierte de webs maliciosas
- Adblock: bloquea publicidad
- Ghostery: bloquea rastreadores

CORREO

Roban contraseña y acceden al correo:

- ✓ Si tenemos gestor online: ordenan transferencia a su cuenta
- ✓ Si hacemos transacciones comerciales con otra empresa: cambian la cuenta bancaria destino

DOBLE FACTOR DE AUTENTICACIÓN:

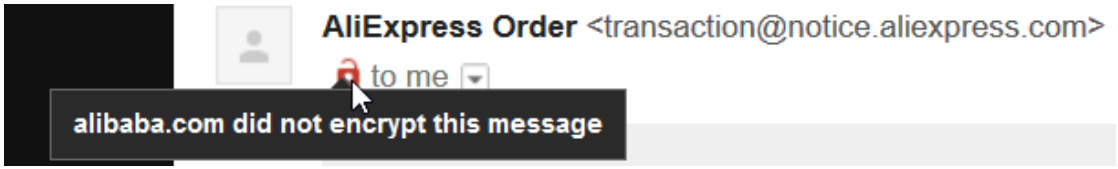
- ✓ Contraseña + Código aleatorio en móvil
- ✓ Imprescindible para evitar el robo o acceso ilícito a cuentas online
- ✓ https://www.turnon2fa.com/
- ✓ https://www.authy.com/

AUTHY By twilio

CORREO

Comprobar seguridad:

- ✓ Últimos accesos y dispositivos
- ✓ Encriptación



No hacer click sobre enlaces económicos:

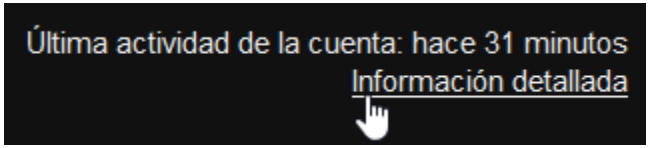
Tecleamos la URL

Phising:

- ✓ Formar a los trabajadores
- ✓ https://getgophish.com/

CORREO.- GMAIL

Información detallada: abajo a la derecha



Actividad reciente:

Tipo de acceso [?] (Navegador, móvil, POP3, etc.)	**Ubicación (dirección IP) [?]**	**Fecha/Hora** (Se muestra en tu zona horaria)
Navegador (Firefox) Mostrar detalles	* España (87.222.43.18)	22:18 (hace 1 minuto)
Móvil	España (87.222.43.18)	21:47 (hace 32 minutos)
Navegador (Firefox) Mostrar detalles	* España (87.222.43.18)	20:03 (hace 2 horas)
Navegador (Firefox) Mostrar detalles	* España (87.222.43.18)	19:03 (hace 3 horas)
Navegador (Firefox) Mostrar detalles	España (87.222.43.18)	15:38 (hace 6 horas)
Navegador (Firefox) Mostrar detalles	España (87.222.43.18)	13:47 (hace 8 horas)
Navegador (Firefox) Mostrar detalles	España (87.222.43.18)	13:04 (hace 9 horas)
Móvil	España (87.222.43.18)	10:09 (hace 12 horas)
Navegador (Firefox) Mostrar detalles	España (87.222.43.18)	23 jul. (hace 1 día)
Navegador (Firefox) Mostrar detalles	España (87.222.43.18)	23 jul. (hace 1 día)

Preferencia de alertas: Mostrar una alerta por actividad inusual. cambiar

* indica que esta actividad corresponde a la sesión abierta ahora.

Este ordenador utiliza la dirección IP 87.222.43.18. (España)

CORREO.- GMAIL

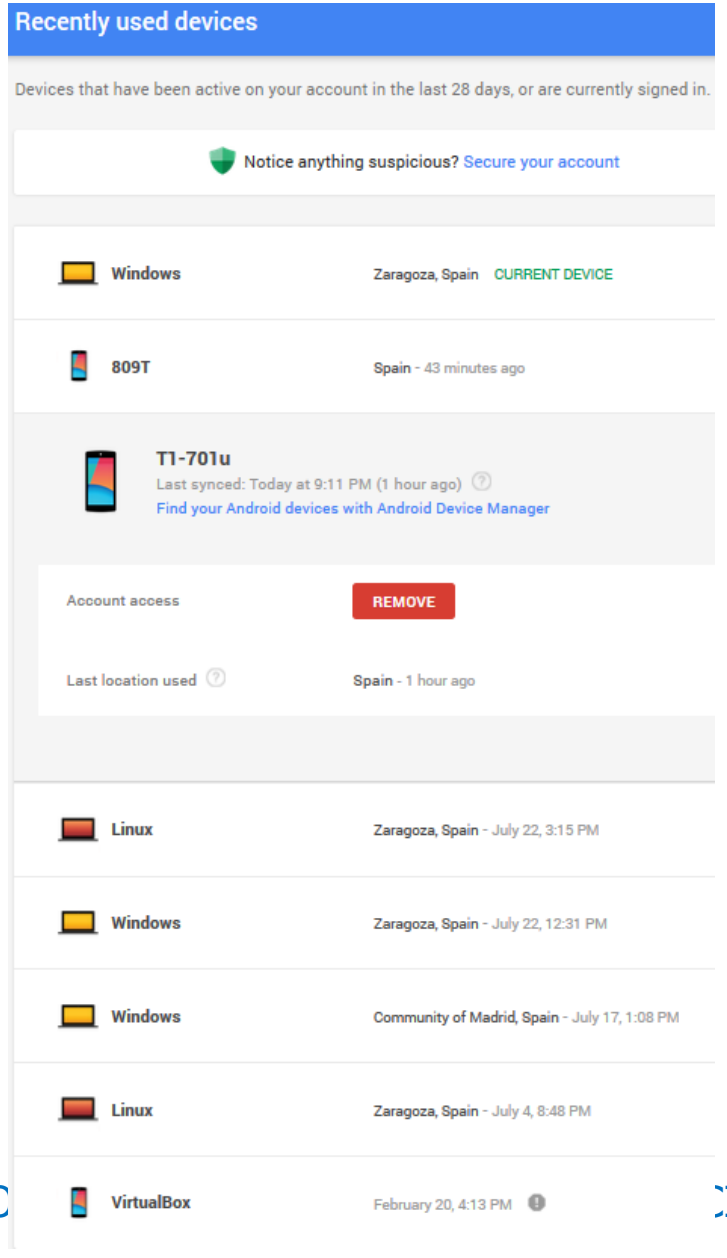
Mi cuenta: arriba a la derecha

Acceder a Device Activity & Notifications (Actividad de Dispositivos y Notificaciones)

Ahí, en Recently Used Devices se ven los dispositivos desde los que se ha accedido a esa cuenta

Se pueden eliminar los ajenos

CORREO.- GMAIL



BANCA ONLINE

Asociamos teléfono a la cuenta

Recibimos SMS con cargos o transferencias

Recibimos SMS con código de validación de transferencias

Aplicación móvil bancaria: CUIDADO!!!

Ojo a devolución de FALSA transferencia recibida (troyano)

COMPRA DE PRODUCTOS

No enviar dinero a desconocidos

Verificar fiabilidad del vendedor (web, historial de ventas, comentarios)

Verificar nº de cuenta por teléfono

Usar tarjetas virtuales o monedero

Uso de pasarelas de pago seguras:

- SSL
- Qué pasa si usan tarjetas ilícitamente??

Ransomware:

- Hacer copia de seguridad
- Estudiar vulnerabilidades
- Actualizar software

Proteger propiedad intelectual e industrial:

- Contenidos de la web (diseño, código fuente, logos, textos, fotografías, nombres comerciales, marcas, productos…) son titularidad de la empresa
- Hacerlo saber en el «Aviso legal»
- Si los ha hecho un tercero: evitar un uso no autorizado si no nos ha cedido los derechos de explotación

SEGURIDAD JURÍDICA

Contratos de confidencialidad con quienes disponen de acceso a datos sensibles:

- ✓Empleados
- ✓Proveedores
- ✓Clientes
- ✓Colaboradores: Asesoría jurídica, gestoría

✓http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2013-0464_Anexo-al-contrato-de-trabajo-sobre-deber-de-confidencialidad.-Uso-de-internet-y-correo-electr-oo-nico..pdf

✓http://plantilla.madrid.slu.edu/uploads/docs/ANEXO_1_Clausulas_contractuales_%28MODELO%29.pdf

Contratos de confidencialidad:

- ✓Lugar y fecha
- ✓Partes que intervienen
- ✓A qué se dedican
- ✓Motivo
- ✓Servicio cubierto por el acuerdo
- ✓Cláusula de confidencialidad

Compromiso de confidencialidad:

- ✓Qué información se considera confidencial (procedimientos, técnicas, diseños, borradores, diagramas…)
- ✓Uso aceptable de la información: para qué fines debe usar la información
- ✓Duración del deber de secreto
- ✓Medidas de seguridad a aplicar según LOPD y el RDLOPD
- ✓A la finalización del servicio, devolver o destruir la información (asesorías…)

Control de uso de herramientas de la empresa

- ✓Aconsejable notificar por escrito
- ✓Por seguridad
- ✓Para medir el rendimiento y la producción
- ✓En caso de ausencia (correos corporativos)
- ✓Por sospechas de actuación irregular

Medida restrictiva de derechos del trabajador:

Idónea: Permite específicamente conocer la conducta laboral de sus empleados.

Necesaria: Si no existe ninguna otra que siendo menos agresiva o limitadora de los derechos del trabajador, pueda aplicarse con la misma eficacia.

Medida restrictiva de derechos del trabajador:

Proporcionada: Deben derivarse de ella más beneficios para el interés general que perjuicios sobre otros valores en conflicto.

Justificada: Debe responder a motivaciones objetivas y no basada exclusivamente en lo que conviene al empresario, o a un comportamiento arbitrario o caprichoso del mismo.

PoS (POINT OF SALE)

Encriptación en transmisión de datos

Whitelist de aplicaciones que puedan funcionar en un PoS

Actualizarlo

Test de vulnerabilidades

Monitorizar los datos

Segmentar redes usadas por PoS

Contraseña segura y 2FA

Antivirus y antimalware

Controlar acceso físico

OTRAS AMENAZAS

Ataques DDoS:

- ✓Bloquear rangos de Ips (extranjeras??)
- ✓Bohatei: https://github.com/ddos-defense/bohatei

DESCARGAS

DESCARGAS DE PROGRAMAS GRATUITOS:

- ✓ Desde la web original del programa
- ✓ No usar softonic: adware
- ✓ Google: evitar anuncios
- ✓ Lo mejor: http://www.techsupportalert.com/

VIRUSTOTAL.COM: https://www.virustotal.com/

- ✓ Comprobar si archivo tiene virus
- ✓ Comprobar si web está infectada

ENLACES.- WINDOWS

Antivirus escritorio, en línea, antiespías, cortafuegos…:
http://www.osi.es/herramientas-gratuitas

Comodo Antivirus: https://antivirus.comodo.com/download-free-antivirus.php

Avira Free: http://www.free-av.com/it/download/index.html

Superantispyware: http://free.agnitum.com/

MalwareBytes Anti-Malware: http://www.majorgeeks.com/Malwarebytes_Anti-Malware_d5756.html

PrivateFirewall: http://www.privacyware.com/personal_firewall.html

Comodo Firewall: https://personalfirewall.comodo.com/

ZoneAlarm: http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm

Outpost Firewall Free: http://free.agnitum.com/

Windows 7 Firewall Control: http://www.sphinx-soft.com/Vista/order.html

Firefox: http://www.mozilla-europe.org/es/products/firefox/

Complementos Firefox (WOT, Adblock Plus, NoScript):
https://addons.mozilla.org/es-es/firefox/extensions/?sort=users

Chrome: http://www.google.com/chrome/eula.html?hl=es

Extensiones Chrome: https://chrome.google.com/extensions/?hl=es

Opera: http://www.opera.com/download/

Fing: http://www.overlooksoft.com/download

ENLACES.- WINDOWS

http://www.osi.es/es/herramientas-gratuitas/

Herramientas gratuítas

Herramientas

Acceso remoto ☐	Antivirus ☐	Cifrado de datos y gestión de contraseñas ☐
Copias de seguridad ☐	Análisis de tráfico de red ☐	Antirrobo ☐
Gestión de Tareas ☐	Privacidad y navegación segura ☐	Análisis online y cleaners ☐
Control parental ☐	Cortafuegos y Filtrado de tráfico ☐	Mantenimiento y Limpieza ☐

Buscar

ENLACES.- WINDOWS

Mejores programas: http://techsupportalert.com/dr/

Equivalentes gratuitos:

- http://www.freealts.com/index.php
- http://es.wikibooks.org/wiki/Introducci%C3%B3n_a_Linux/Equivalencias_Windows_en_Linux

LibreOffice: http://www.documentfoundation.org/download/

CDBurnerXP: http://cdburnerxp.se/download

GIMP: http://gimp.org/downloads/

Avidemux: http://fixounet.free.fr/avidemux/download.html

CCleaner: http://www.piriform.com/ccleaner/download

Sophos: http://www.sophos.com/es-es/products/endpoint-antivirus.aspx

ENLACES

Jugar en LINUX:

- Gmount-ISO + WINE
- http://www.playonlinux.com/en/download.html
- http://www.linuxjuegos.com/
- http://www.juegoslibres.net/juegos/linux/

Cursos gratis: http://www.aulafacil.com/

Traductor: http://www.google.es/language_tools

Oficina de Seguridad del Internauta: http://www.osi.es/

ENLACES

Ubuntu: http://www.ubuntu.com/getubuntu/download

LibreOffice: http://es.libreoffice.org/

Ccleaner (Limpieza PC, reparación registro, desinstalar programas, gestionar programas que se cargan en inicio)

http://www.filehippo.com/download_ccleaner/

AVG Free: http://free.avg.com/us-en/download-free-antivirus

Superantispyware: http://www.superantispyware.com/download.html

CDBurnerXP: http://cdburnerxp.se/download

GIMP: http://gimp.org/downloads/

Teamviewer (Acceso remoto a otros ordenadores)

http://www.teamviewer.com/download/TeamViewer_Setup_es.es

Httrack (Descarga webs enteras)

http://www.httrack.com/page/2/en/index.html

Atube catcher (Descarga vídeos de youtube y otros portales)

http://atube-catcher.softonic.com/

Rainlendar (Calendario-agenda de escritorio)

http://www.rainlendar.net/cms/index.php?option=com_rny_download&Itemid=30

MagicDisc (Montar imágenes de programas, juegos...)

http://www.magiciso.com/tutorials/miso-magicdisc-history.htm

ENLACES.- WINDOWS

Secunia PSI: http://secunia.com/vulnerability_scanning/personal

Advanced SystemCare (Limpieza PC, reparación errores, protección, optimización, actualización de drivers y programas)
http://www.iobit.com/advancedwindowscareper.html?Str=download

VLC (Reproduce vídeo y música, captura de pantalla de vídeos)
http://www.videolan.org/vlc/download-windows.html

Skype: http://www.skype.com/intl/es/download/skype/windows/

7-zip (Comprime y descomprime archivos): http://www.7-zip.org/download.html

Picassa (Ver y tratar imágenes): http://picasa.google.com/intl/es/

VirtualBox (Ejecuta máquinas virtuales, por ejemplo Linux sobre XP o Vista, etc.):
http://www.virtualbox.org/wiki/Downloads

jDownloader (Descarga automática desde rapidshare, megaupload, etc.):
http://jdownloader.org/download/index

Tixati (descarga de torrents): http://www.tixati.com/download/

Deluge (descarga de torrents): http://dev.deluge-torrent.org/wiki/Download

Pidgin (Programa de chateo que soporta messenger, Gtalk...):
http://www.pidgin.im/download/windows/

Process explorer (Finaliza cualquier tarea)
http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

PDF-Xchange Viewer (Lee pdf)
http://www.docu-track.com/download/PDFXVwer.zip

MUCHAS GRACIAS POR SU ATENCIÓN

http://delitostecnologicos.wordpress.com/