SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

PROTEGE TU INFORMACIÓN

SEGURIDAD EN LA ERA DE LOS MEDIOS DIGITALES

¿Por qué preocuparnos?

- Uso de internet para tareas tradicionalmente “offline”
- Mayor cantidad de riesgos, más sofisticados, más silenciosos
- Redes sociales para fines laborales
- Límite difuso entre el ambiente personal, social y laboral
- Mayor interconexión de los servicios
- Muchos puntos de entrada para atacantes

¿Por qué preocuparnos? (1)

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Control de Acceso Credenciales

Autenticación

¿Qué es la autenticación?

Sistemas basado en usuario y contraseña

Ataques de contraseña:

350 mil millones de contraseñas por segundo

	Números	Minúsculas	Minúsculas + números	Minúsculas + Mayúsculas + números
6 caracteres	<0,003 milisegundos	< 1 milisegundos	6 milisegundos	0,16 segundos
8 caracteres	0,3 milisegundos	0,6 segundos	8 segundos	10 minutos
10 caracteres	0,3 segundos	6,7 minutos	3 horas	1 mes
12 caracteres	3 segundos	3 días	5 meses	296 años

¿Qué es una contraseña robusta?

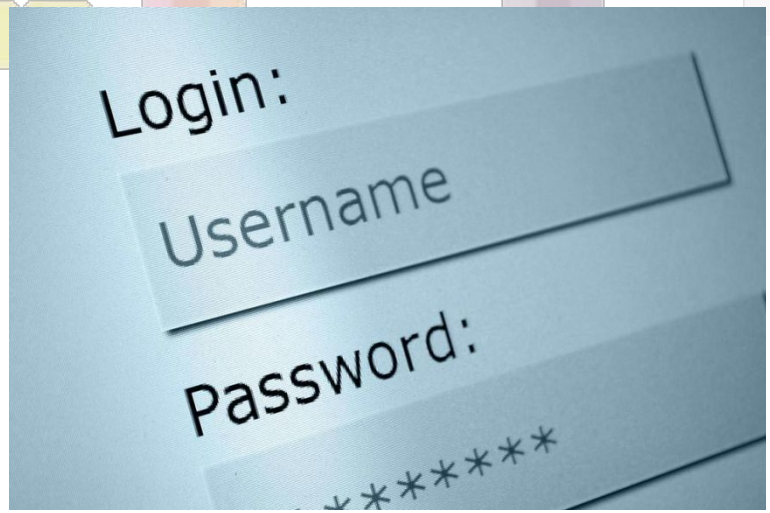
Longitud

¿Son suficiente 8 caracteres?

NO!

Mínimo 12 caracteres!

En una contraseña compuesta solo por minúsculas, 1 carácter adicional significa una contraseña 16 veces más difícil de crackear



SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

¿Qué es una contraseña robusta? (1)

Combinación de tipo de caracteres

No limitarse a usar minúsculas!

- Minúsculas
- Mayúsculas
- Números
- Caracteres: $ # % & ! . , * -

DATO: En una contraseña de 8 minúsculas, 1 carácter adicional significa una contraseña 35% más difícil de crackear

¿Qué es una contraseña robusta? (2)

Frases

- ¿Por qué usar palabras si podemos usar frases?

EJEMPLO:

“Esta frase es solo un ejemplo” → “Est4.fr4s3-3s.s0l0-un.Ej3mpl0”

¿Qué es una contraseña robusta? (3)

NO usar palabras de diccionario

- Palabras o nombres conocidos, propios del lenguaje
- Contraseñas comunes y conocidas: admin, root, qwerty, etc..

DATO:
Contraseñas más comunes:

1) **123456**
2) **password**
3) **12345678**
4) **qwerty**
5) **12345**
6) **123456789**

Buenas prácticas

- No uses la misma contraseña para todo
- Cambia tu contraseña regularmente
- Cambia las contraseñas por defecto
- No la escribas en papeles o documentos accesibles

Tv5Monde revealed his own passwords in an interview

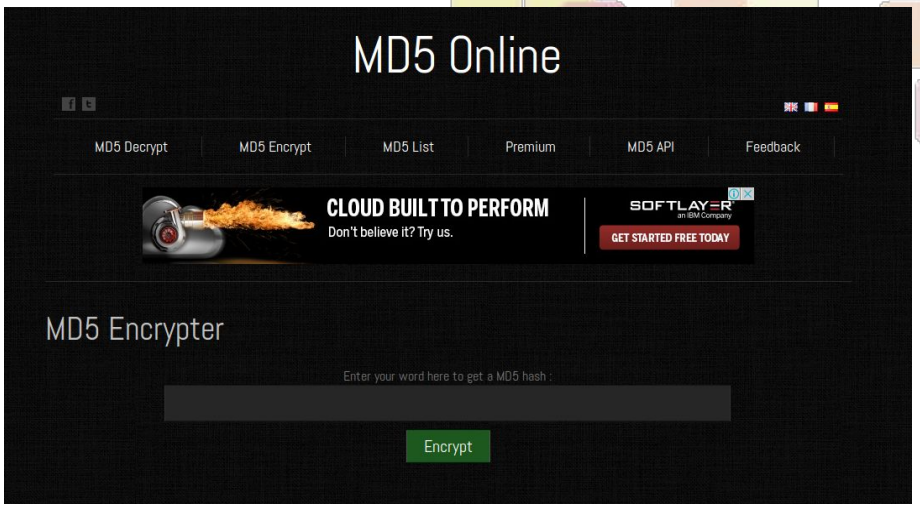
April 10, 2015 By Pierluigi Paganini

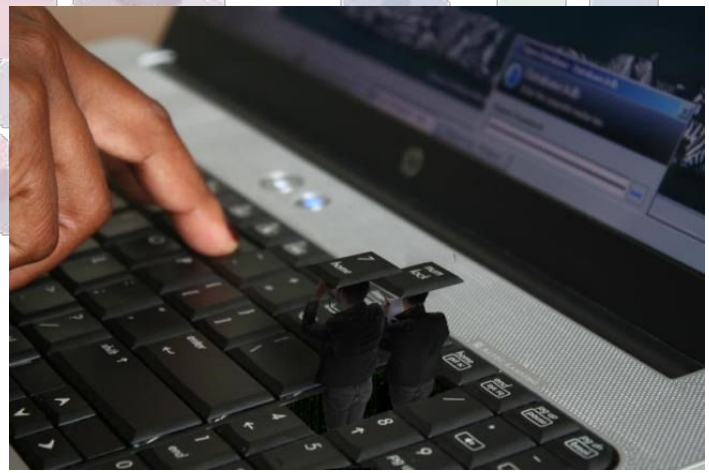
A TV5Monde staffer accidentally revealed a password used to access the social media account of the broadcaster in an interview.

Following the successful attack against the network of the TV French Channel TV5Monde, law enforcement and French Intelligence started to investigate the attach chain.

Buenas prácticas (1)

- No la introduzcas en sitios o programas desconocidos – cuidado con el **PHISHING**!
- No la introduzcas en equipos poco seguros – cuidado con los **KEYLOGGERS**!
- No uses herramientas online para crear contraseñas





¿Es suficiente? ...

Autenticación de doble factor

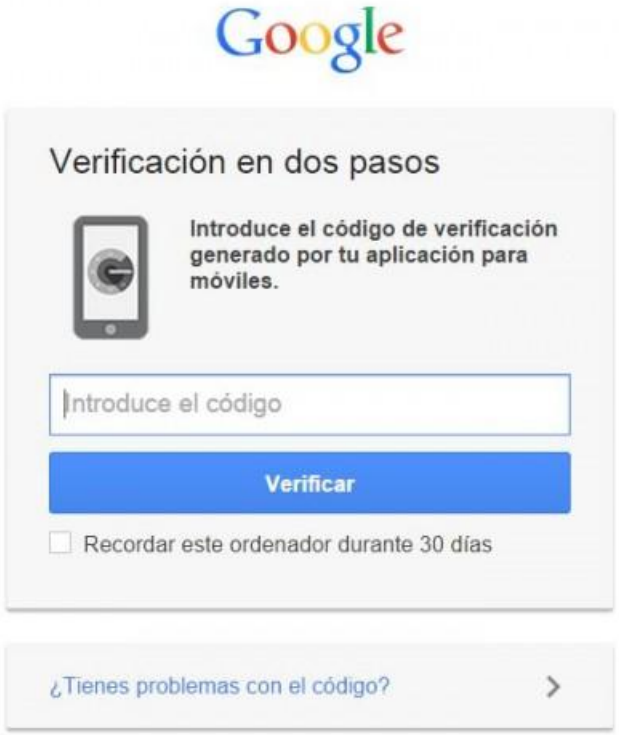
- Medida de seguridad adicional al usuario y contraseña

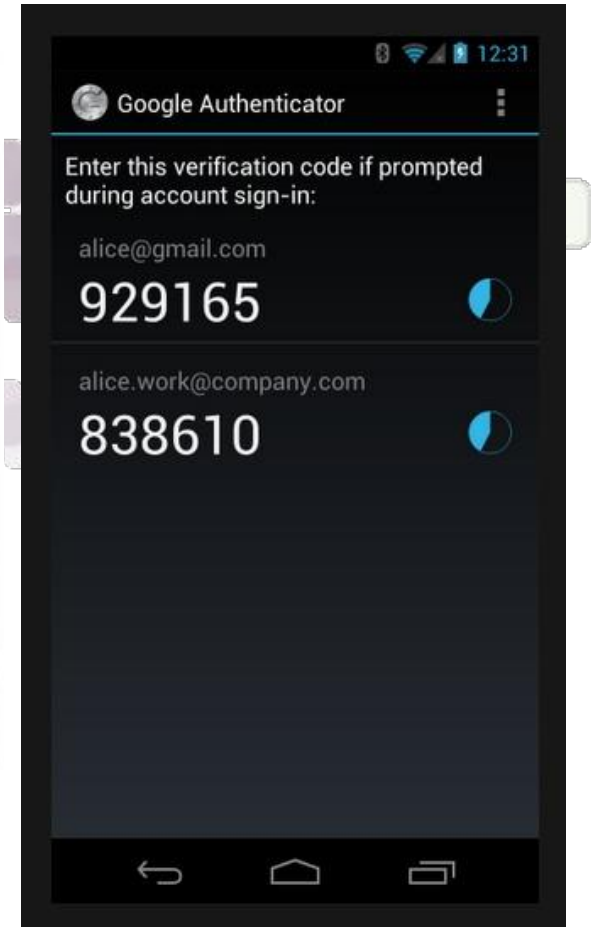
Usuario + Contraseña + CÓDIGO DE SEGURIDAD

1) Algo que el usuario sabe → contraseña
2) Algo que el usuario tiene → teléfono
3) Algo que el usuario es → huella dactilar

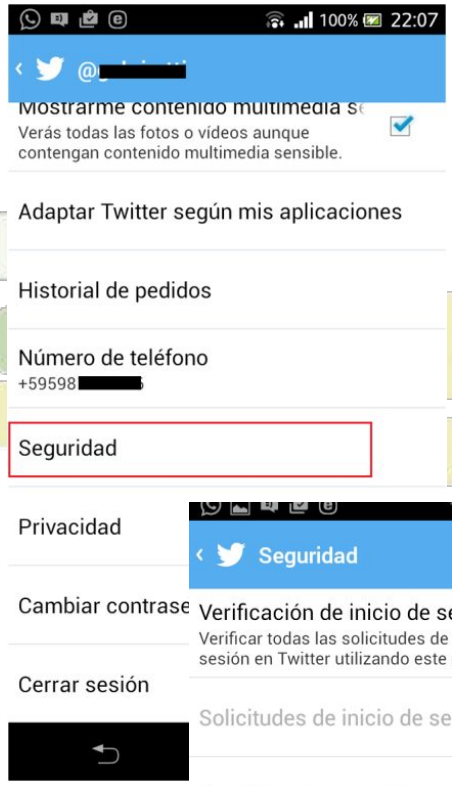
Autenticación de doble factor (1)

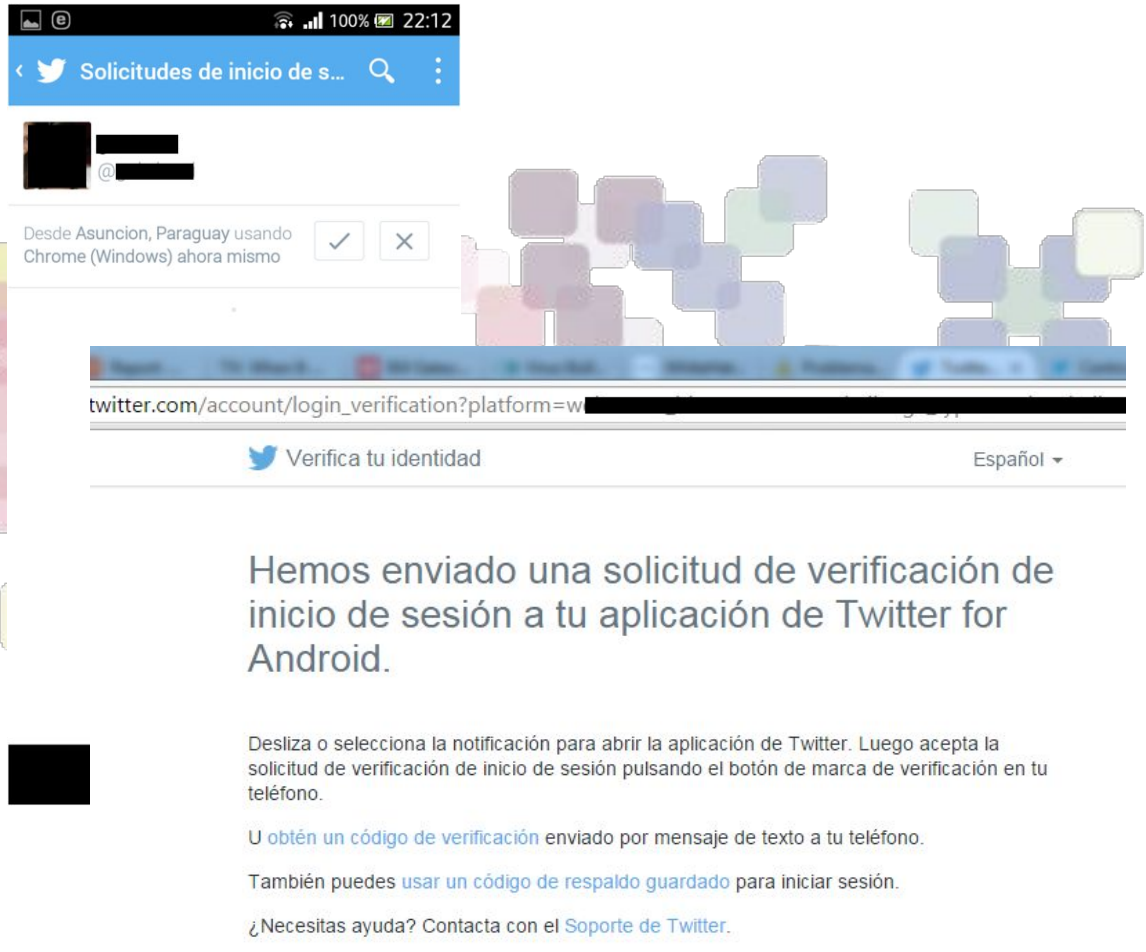
- Google
- Outlook
- Facebook
- Twitter
- Dropbox
- Wordpress





Autenticación de doble factor (2)





Gestores de contraseña

.. ¿Cómo acordarnos de tantas contraseñas? ..

Gestores de contraseña (1)

Offline:

KeePassX

KeePass

1Password

Norton Identity Safe

Kaspersky Password Manager

Online:

LastPass

Dashlane

Zoho Vault

Avast Easy Pass

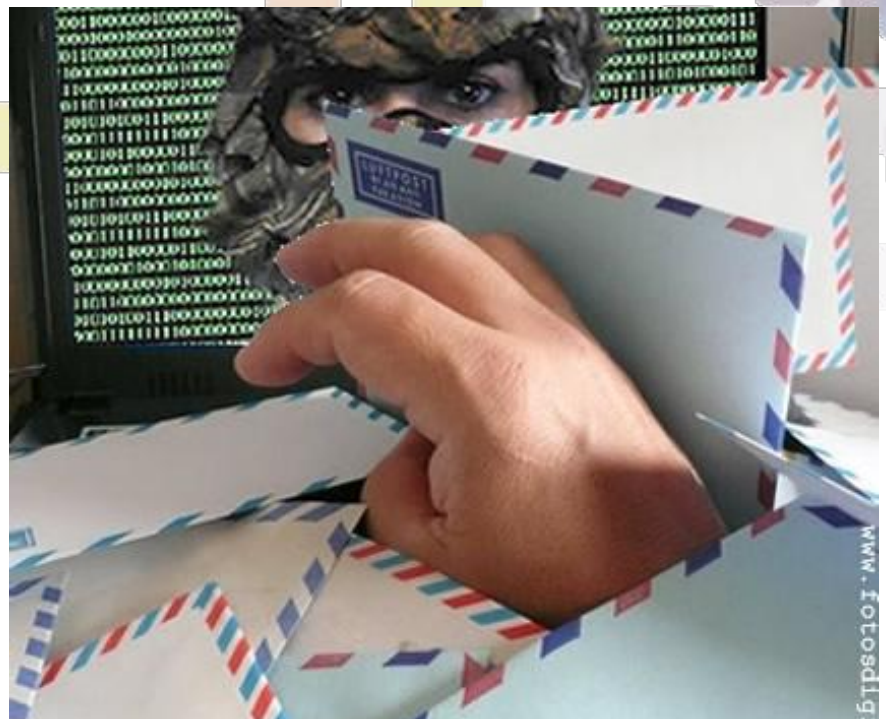
McAfee LiveSafe

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

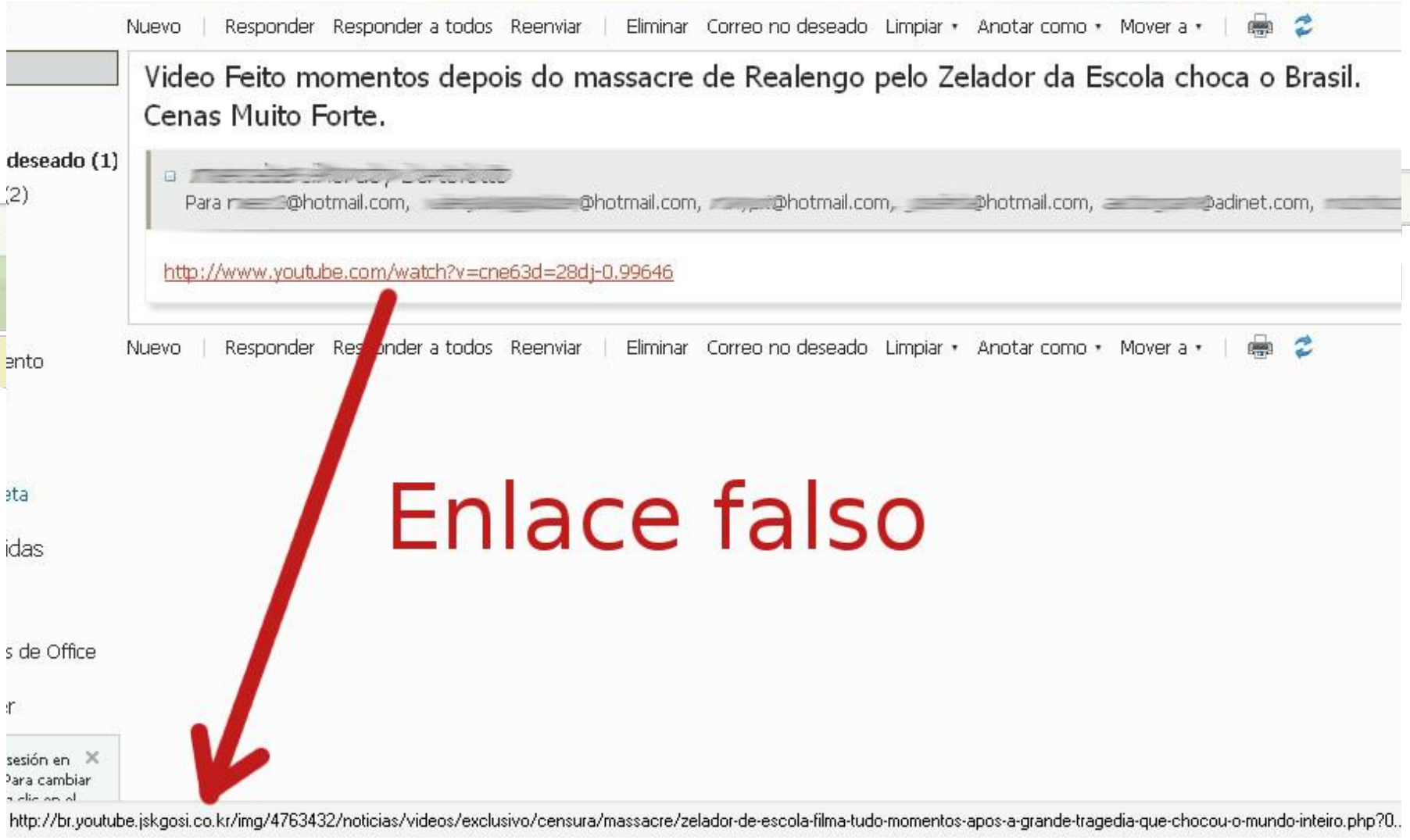
CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Correo Electrónico



Spam


Nuevo | Responder | Responder a todos | Reenviar | Eliminar | Correo no deseado | Limpiar | Anotar como | Mover a
Video Feito momentos depois do massacre de Realengo pelo Zelador da Escola choca o Brasil. Cenas Muito Forte.
Para r@hotmail.com, @hotmail.com, @hotmail.com, @hotmail.com, @adinet.com,
http://www.youtube.com/watch?v=cne63d=28dj-0.99646
Nuevo | Responder | Responder a todos | Reenviar | Eliminar | Correo no deseado | Limpiar | Anotar como | Mover a
Enlace falso
http://br.youtube.jskgosi.co.kr/img/4763432/noticias/videos/exclusivo/censura/massacre/zelador-de-escola-filma-tudo-momentos-apos-a-grande-tragedia-que-chocou-o-mundo-inteiro.php?0..

Spam (2)

Mar Jun 16 05:42:14 2015 **abuse@cert.gov.py - Caso creado**

Asunto: Cheque Devolvido Seu Nr. 00124-46556 Evite Protesto! (27588)

Date: Tue, 16 Jun 2015 01:30:27 -0500 (CDT)

From: abuse@cert.gov.py

?

Segue a cópia dos cheques devolvidos anexada abaixo

Segue a cópia dos cheques devolvidos anexada abaixo.
tenha um bom dia !

Copia cheque 1.pdf [lookup host] (151,8 KB)
Copia cheque 2.pdf [lookup host] (146,5 KB)

ANEXO: Cheque001_PDF.ZIP (342k)

>Att: Fernanda Martins - fernanda@pdg.com.br
PDG Realty S/A Empreendimentos.

//googledrive.com/host/0Bw2m28L2vF-4QzNyWUJJUE1lTmM/

Spam (3)

Mar Jun 16 05:42:14 2015 **abuse@cert.gov.py - Caso creado**

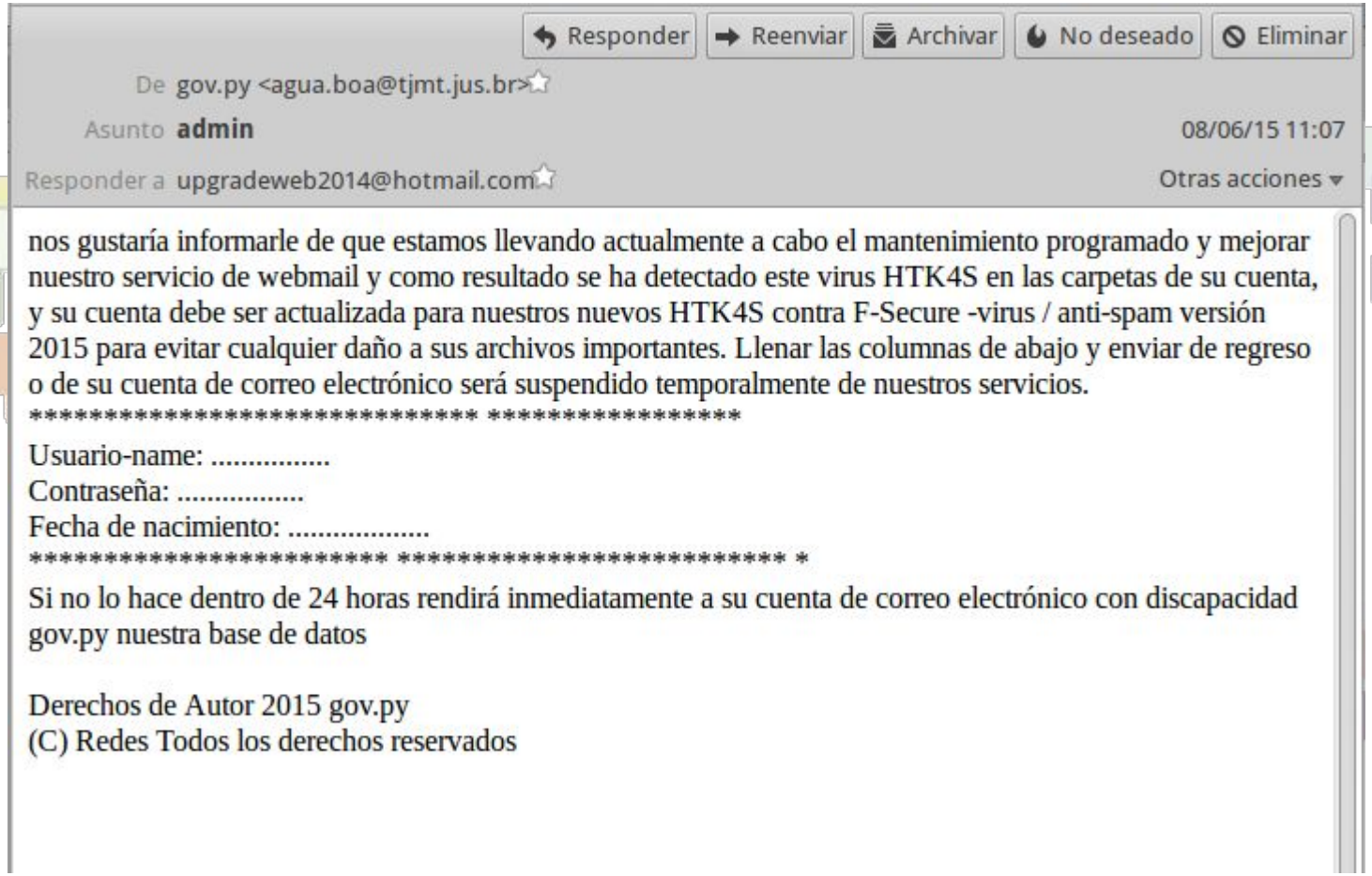
From www-data@group5.stats.gru 42:13 2015
Tue Jun 16 05:

MIME-Version: 1.0
X-Sender: abuse@cert.gov.py [lookup email] [lookup "cert.gov.py"]
X-Spam-Status: Yes, score=8.845 tagged_above=-10 required=6.6 tests=[BAYES_20=-0.001, DATE_IN_PAST_03_06=1.592, FORGED_OUTLOOK_HTML=0.021, HEADER_FROM_DIFFERENT MIME_HTML_ONLY=0.723, RCVD_IN_PSBL=2.7, RCVD_IN_RP_RNBL=1.31, TO_NO_BRKTS_MSFT=2.497] autolearn=no autolearn_force=no
X-Mailer: Microsoft Office Outlook, Build 17.551210
X-Mailer: iGMail [www.ig.com.br [lookup host]]
X-Spam-Flag: YES
Message-ID: <20150616092800.80A8717945F@group5.stats.gru> [lookup email] [lookup "group5.stats.gru"]
Reply-To: abuse@cert.gov.py [lookup email] [lookup "cert.gov.py"]
content-type: text/html; charset="utf-8"
X-Spam-Score: 8.845
Received: from correo.cert.gov.py [lookup host] (correo.cert.gov.py [lookup host] [192.168.202.27 [lookup IP][Add IP]]) by rtir.cert.gov.py [lookup host] (8.14.4/8.14.4) with ESMTP id t5G9gDIX
<abuse@rtir.cert.gov.py> [lookup email] [lookup "rtir.cert.gov.py"]; Tue, 16 Jun 2015 05:42:13 -0400
Received: from localhost (localhost.localdomain [127.0.0.1 [lookup IP][Add IP]]) by correo.cert.gov.py [lookup host] (Postfix) with ESMTP id C1EB64D52752; Tue, 16 Jun 2015 05:42:12 -0400
Received: from correo.cert.gov.py [lookup host] ([127.0.0.1 [lookup IP][Add IP]]) by localhost (correo.cert.gov.py [lookup host] [127.0.0.1 [lookup IP][Add IP]]) (amavisd-new, port 10024) with E
Received: from group5.stats.gru [lookup host] (119.81.243.24 [lookup IP][Add IP]-static.reverse.softlayer.com [lookup host] [119.81.243.24 [lookup IP][Add IP]]) by correo.cert.gov.py [lookup h
Tue, 16 Jun 2015 05:42:03 -0400 (PYT)
Received: by group5.stats.gru [lookup host] (Postfix, from userid 33) id 80A8717945F; Tue, 16 Jun 2015 01:30:27 -0500 (CDT)
Asunto: Cheque Devolvido Sed Nr. 00124-46556 Evite Protesto! (27586)
X-Originating-Email: abuse@cert.gov.py [lookup email] [lookup "cert.gov.py"]
Date: Tue, 16 Jun 2015 01:30:27 -0500 (CDT)
X-Spam-Level: ********
X-Igspam-Global: Unsure, spamicity=0.570081 - pe=5.74e-01 - pf=0.574081 - pg=0.574081
X-PHP-Originating-Script: 0:5.php [lookup host]
Para: abuse@cert.gov.py [lookup email] [lookup "cert.gov.py"]
Content-Transfer-Encoding: 8bit
From: abuse@cert.gov.py [lookup email] [lookup "cert.gov.py"]
X-RT-Original-Encoding: iso-8859-1
X-RT-Interface: Email
Content-Length: 10433

Segue a cópia dos cheques devolvidos anexada abaixo

Segue a cópia dos cheques devolvidos anexada abaixo.
tenha um bom dia !

Phishing



Responder | Reenviar | Archivar | No deseado | Eliminar

De gov.py <agua.boa@tjmt.jus.br>

Asunto **admin** 08/06/15 11:07

Responder a upgradeweb2014@hotmail.com Otras acciones

nos gustaría informarle de que estamos llevando actualmente a cabo el mantenimiento programado y mejorar nuestro servicio de webmail y como resultado se ha detectado este virus HTK4S en las carpetas de su cuenta, y su cuenta debe ser actualizada para nuestros nuevos HTK4S contra F-Secure -virus / anti-spam versión 2015 para evitar cualquier daño a sus archivos importantes. Llenar las columnas de abajo y enviar de regreso o de su cuenta de correo electrónico será suspendido temporalmente de nuestros servicios.

********** **********

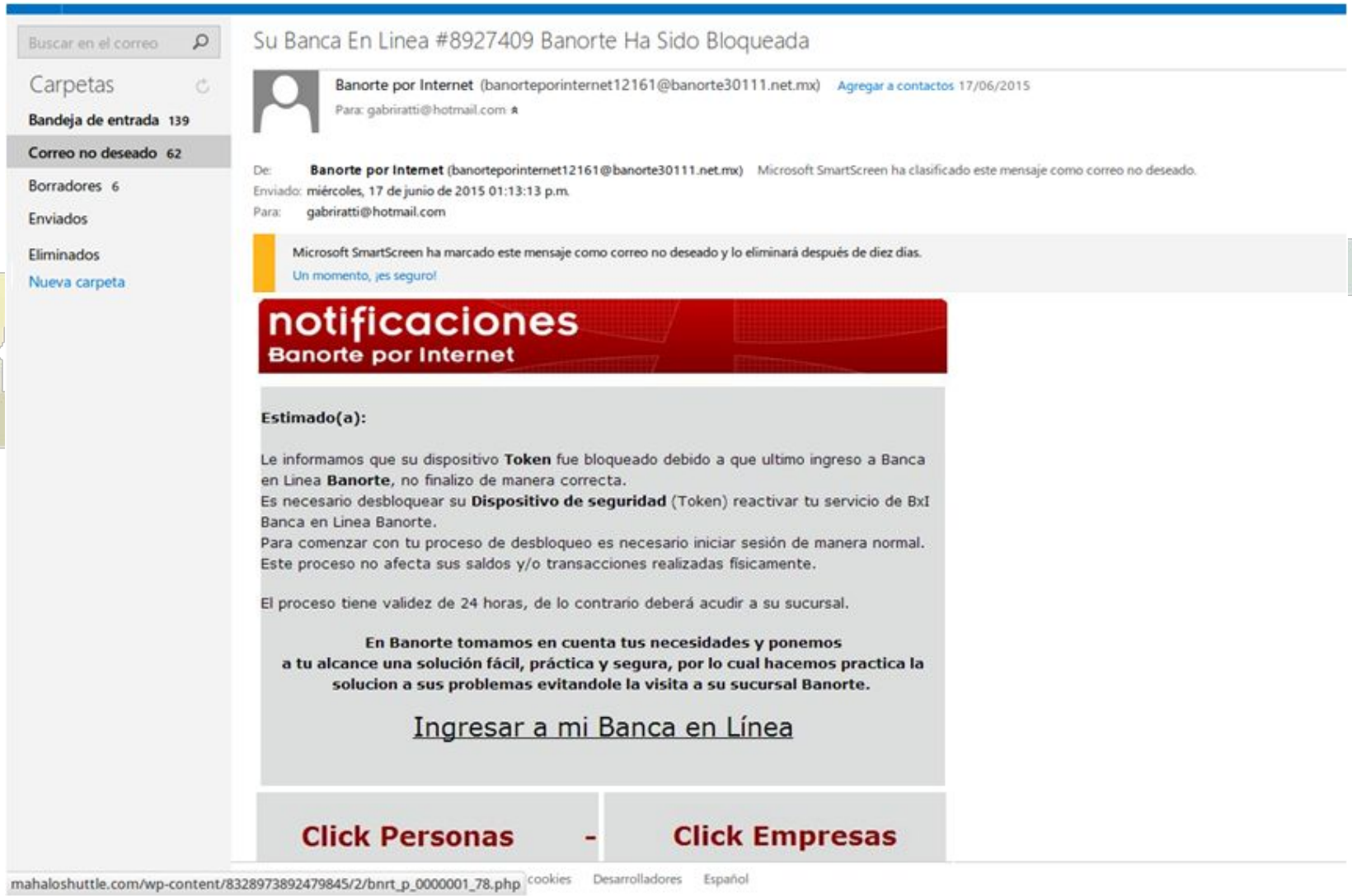
Usuario-name: .....
Contraseña: .....
Fecha de nacimiento: .....

********** ********** *

Si no lo hace dentro de 24 horas rendirá inmediatamente a su cuenta de correo electrónico con discapacidad gov.py nuestra base de datos

Derechos de Autor 2015 gov.py
(C) Redes Todos los derechos reservados

Phishing (2)


Buscar en el correo
Carpetas
Bandeja de entrada 139
Correo no deseado 62
Borradores 6
Enviados
Eliminados
Nueva carpeta
Su Banca En Linea #8927409 Banorte Ha Sido Bloqueada
Banorte por Internet (banorteporinternet12161@banorte30111.net.mx) Agregar a contactos 17/06/2015
Para: gabriratti@hotmail.com
De: Banorte por Internet (banorteporinternet12161@banorte30111.net.mx) Microsoft SmartScreen ha clasificado este mensaje como correo no deseado.
Enviado: miércoles, 17 de junio de 2015 01:13:13 p.m.
Para: gabriratti@hotmail.com
Microsoft SmartScreen ha marcado este mensaje como correo no deseado y lo eliminará después de diez días.
Un momento, ¡es seguro!
notificaciones
Banorte por Internet
Estimado(a):
Le informamos que su dispositivo Token fue bloqueado debido a que ultimo ingreso a Banca en Linea Banorte, no finalizo de manera correcta.
Es necesario desbloquear su Dispositivo de seguridad (Token) reactivar tu servicio de BxI Banca en Linea Banorte.
Para comenzar con tu proceso de desbloqueo es necesario iniciar sesión de manera normal.
Este proceso no afecta sus saldos y/o transacciones realizadas físicamente.
El proceso tiene validez de 24 horas, de lo contrario deberá acudir a su sucursal.
En Banorte tomamos en cuenta tus necesidades y ponemos a tu alcance una solución fácil, práctica y segura, por lo cual hacemos practica la solucion a sus problemas evitandole la visita a su sucursal Banorte.
Ingresar a mi Banca en Línea
Click Personas
-
Click Empresas
mahaloshuttle.com/wp-content/8328973892479845/2/bnrt_p_0000001_78.php
cookies
Desarrolladores
Español

SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

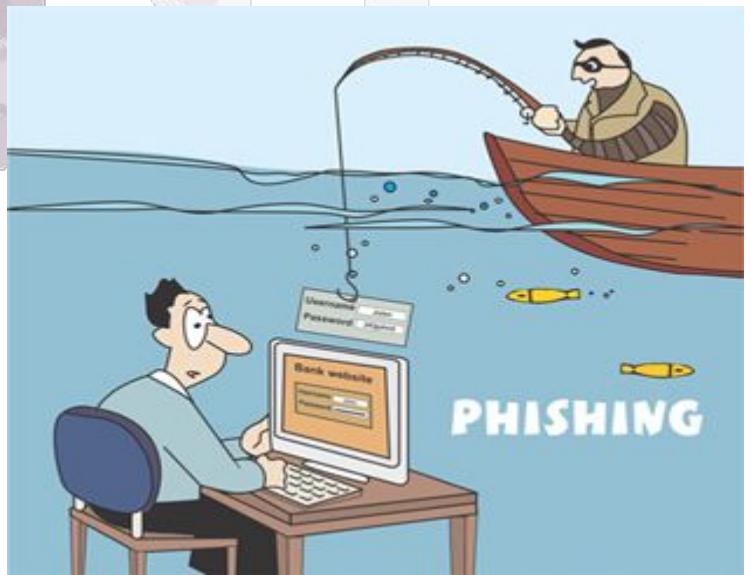
¿Cómo cuidarnos del Spam?

- Cuidado con los archivos adjuntos
- Bloquear imágenes y contenido remoto de los correos
- Proteger la dirección de correo
- Filtros anti-spam
- No responder jamás el spam
- No entrar a enlaces
- Buenas prácticas para las contraseñas
- No reenviar cadenas
- Utilizar la opción “Con Copia Oculta” (CCO)
- No enviar un correo a más de 10 ~ 15 contactos.
- Reportar el spam!

¿Y del phishing? ...

¿Cómo cuidarnos del Phishing?

- No proporcionar nunca información confidencial por correo
- Asegurarse de que la URL comience con HTTPS
- Verificar el remitente del correo, en caso de duda, comunicarse personalmente
- Examinar periódicamente la actividad en las cuentas (bancarias, de correo, de redes sociales, etc.)



SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

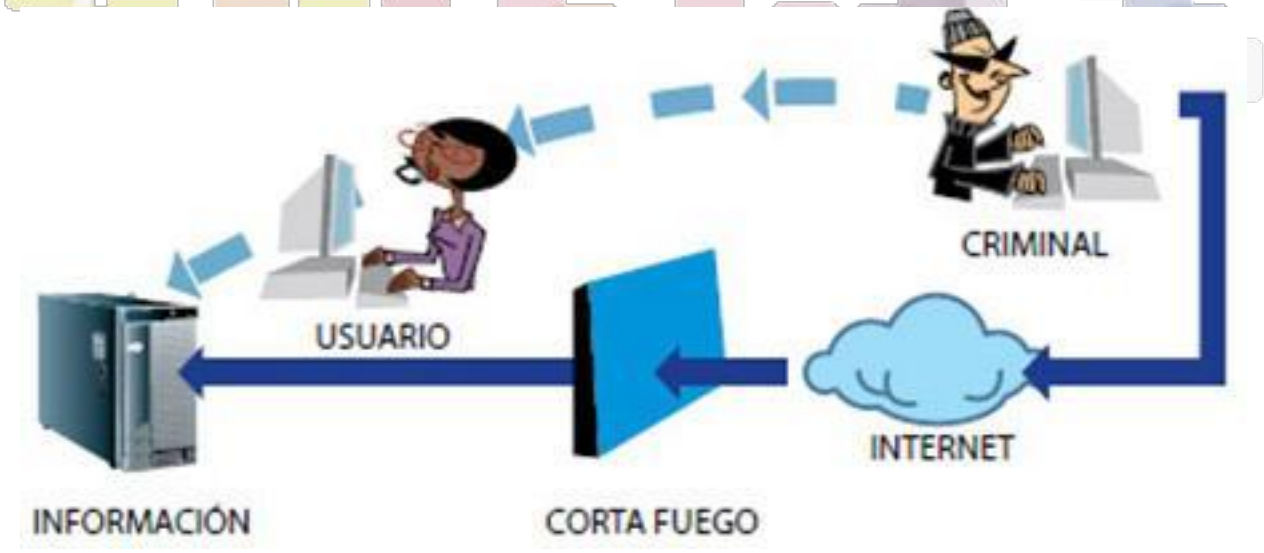
CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Ingeniería Social

¿Qué es la ingeniería social?

Es el **arte del engaño** que busca que la víctima revele información confidencial o realice acciones que brinden al atacante un **punto de entrada** a sus sistemas informáticos.



Ingeniería social

Ingeniería social (1)

Ingeniería social (2)

¿Qué hay de las redes sociales? ...

Ingeniería social - Otros medios

¿Y si el engaño no es a través de internet? ...

- **Curiosidad**
- **Empatía**
- **Miedo**
- **Vanidad**
- **Vergüenza**

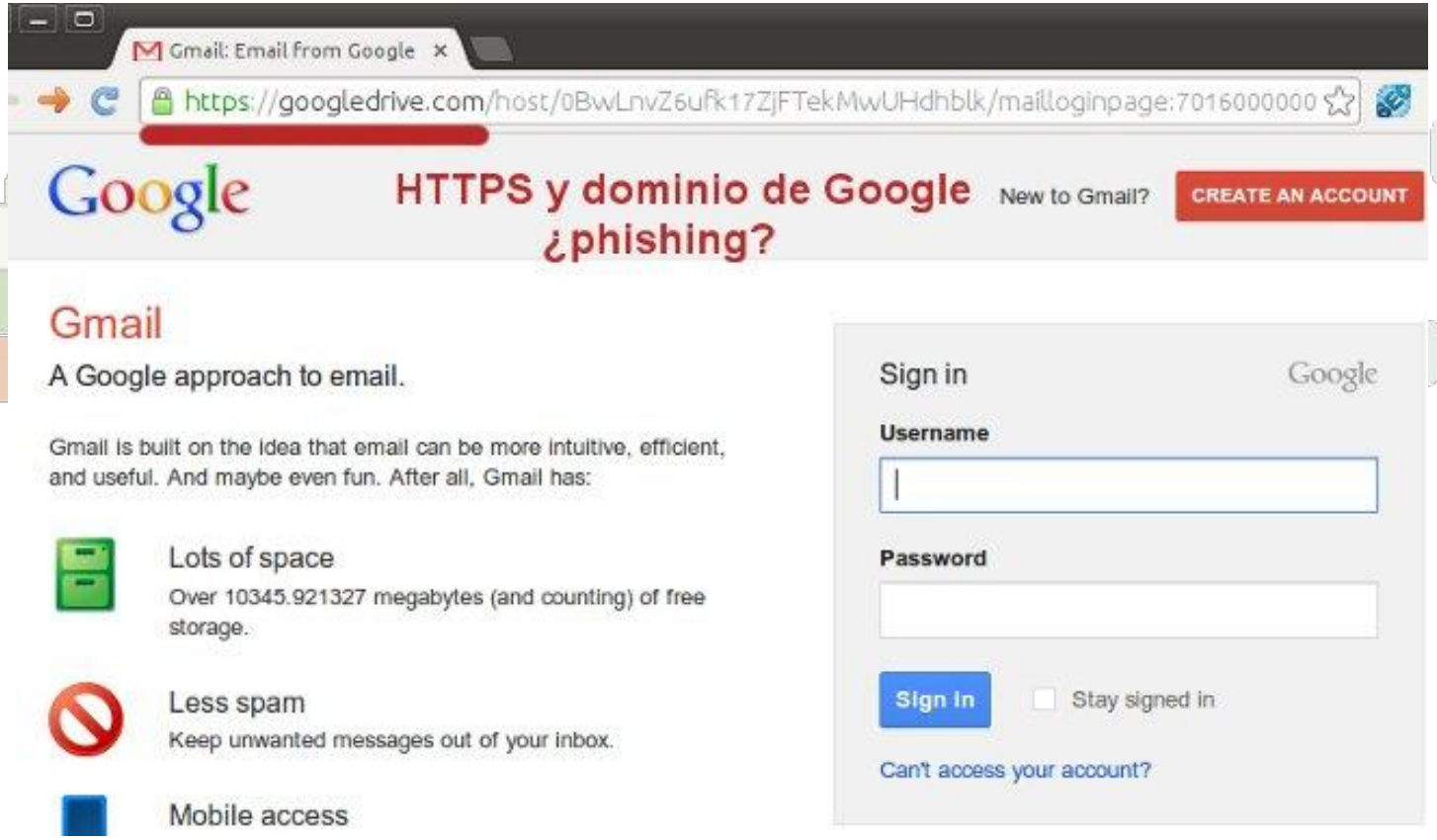
SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

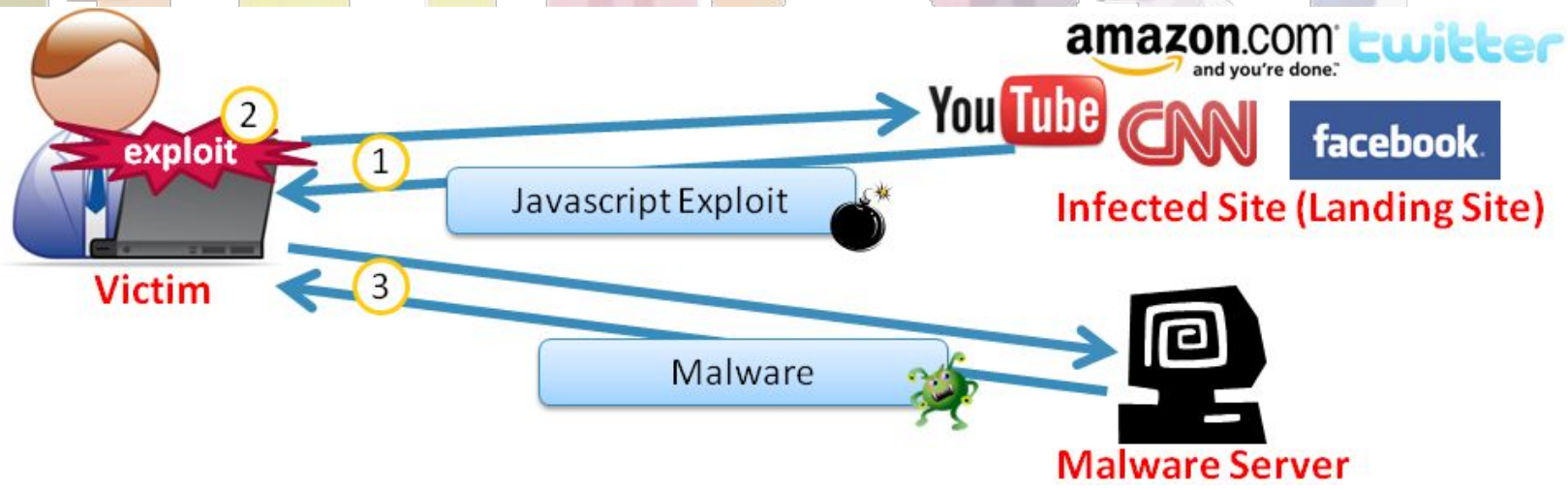
Navegación Segura

Cuando las buenas prácticas no bastan..



Cuando las buenas prácticas no bastan.. (1)

Existen técnicas a través de las cuales sólo se requiere que un usuario abra una página web en el navegador para infectarlo.



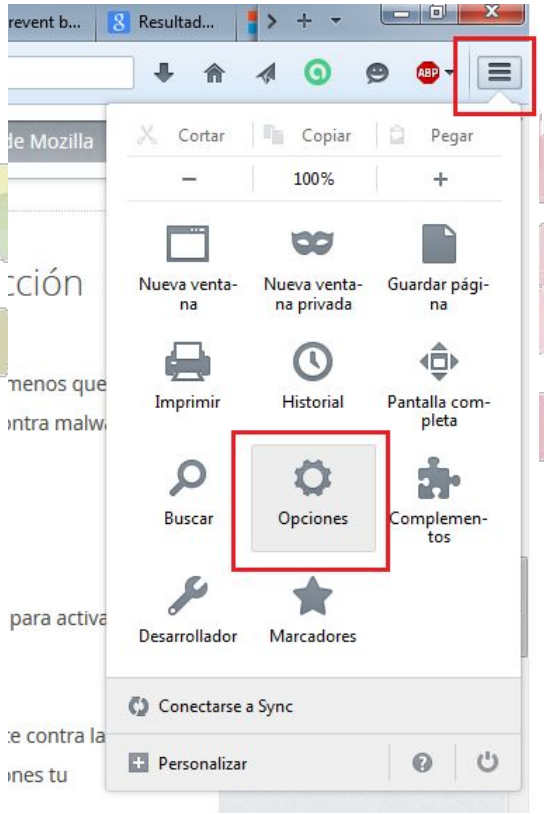
Securizando el Navegador

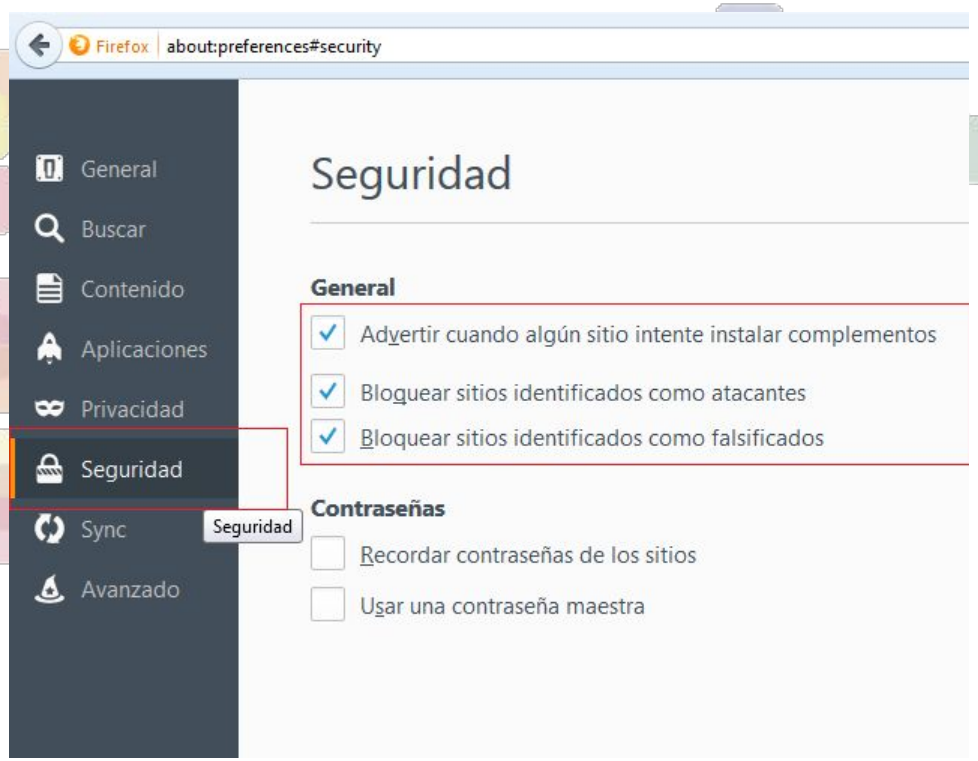
Protección anti-phishing y anti-malware

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Safari

Securizando el Navegador (1)

- Protección anti-phishing y anti-malware - Configuración



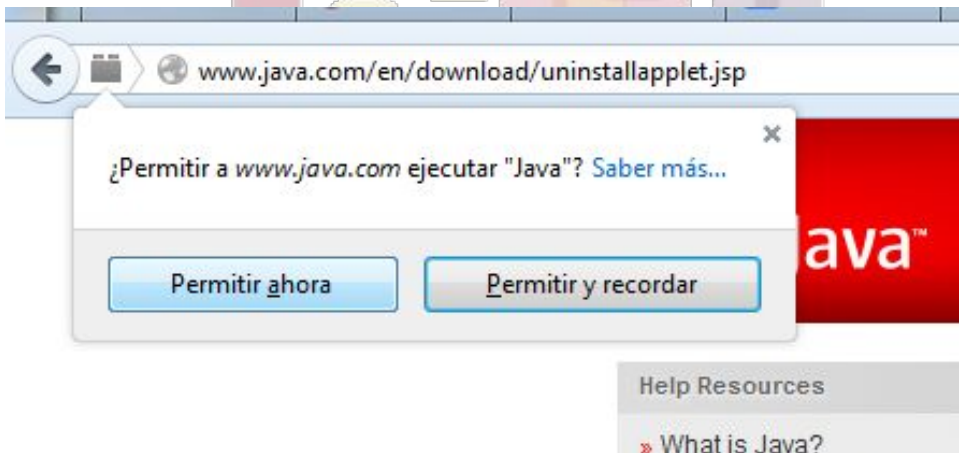


Securizando el Navegador (2)

Plugins

- Adobe Flash Player
- Visor de PDF
- Java
- Decodificadores de audio
- Silverlight

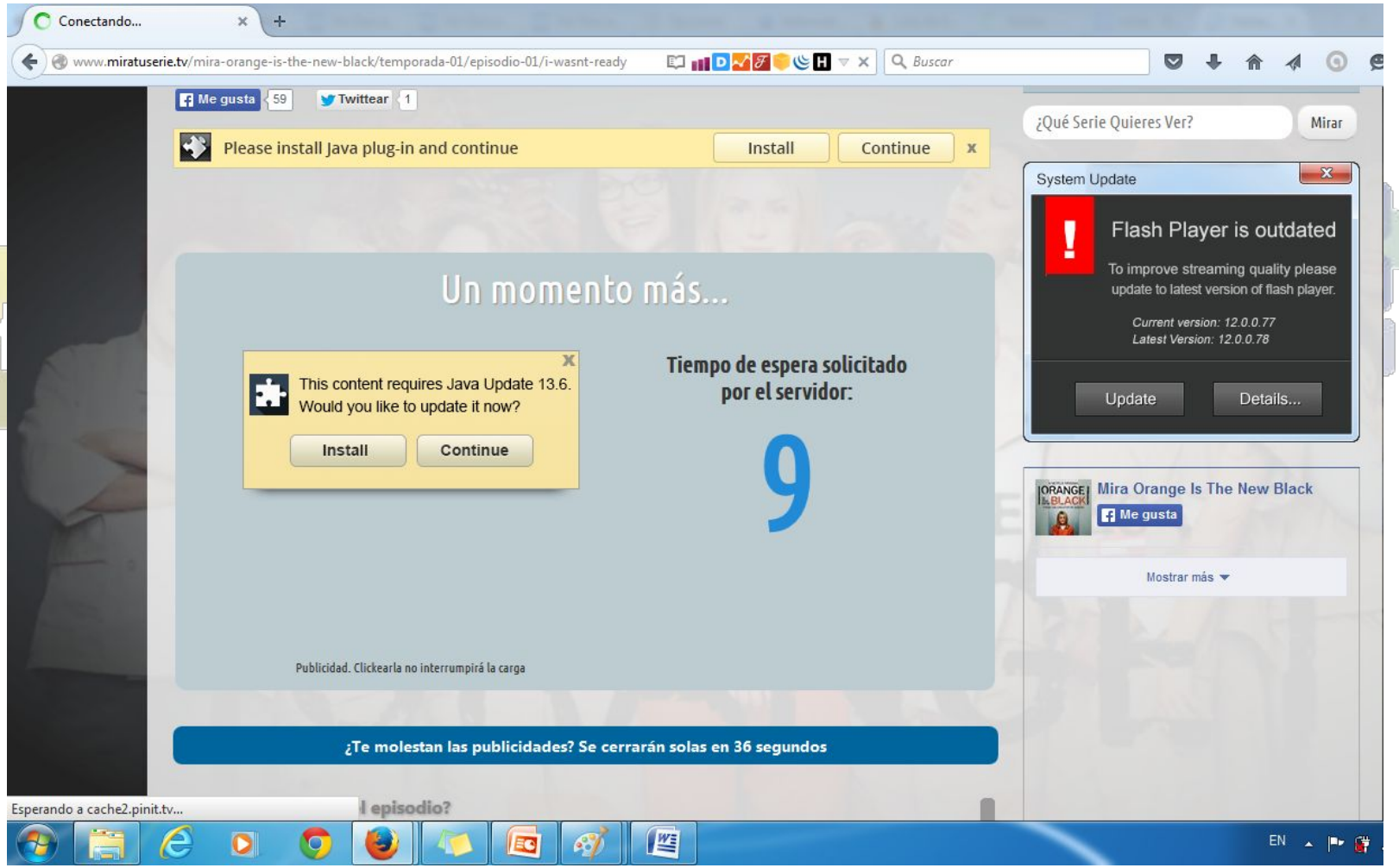
- Decidir cuándo otorgar permiso de ejecutar
- Mantenerlos actualizados
- No instalar ni autorizar plugins de sitios dudoso – **cuidado con los plugins maliciosos!**



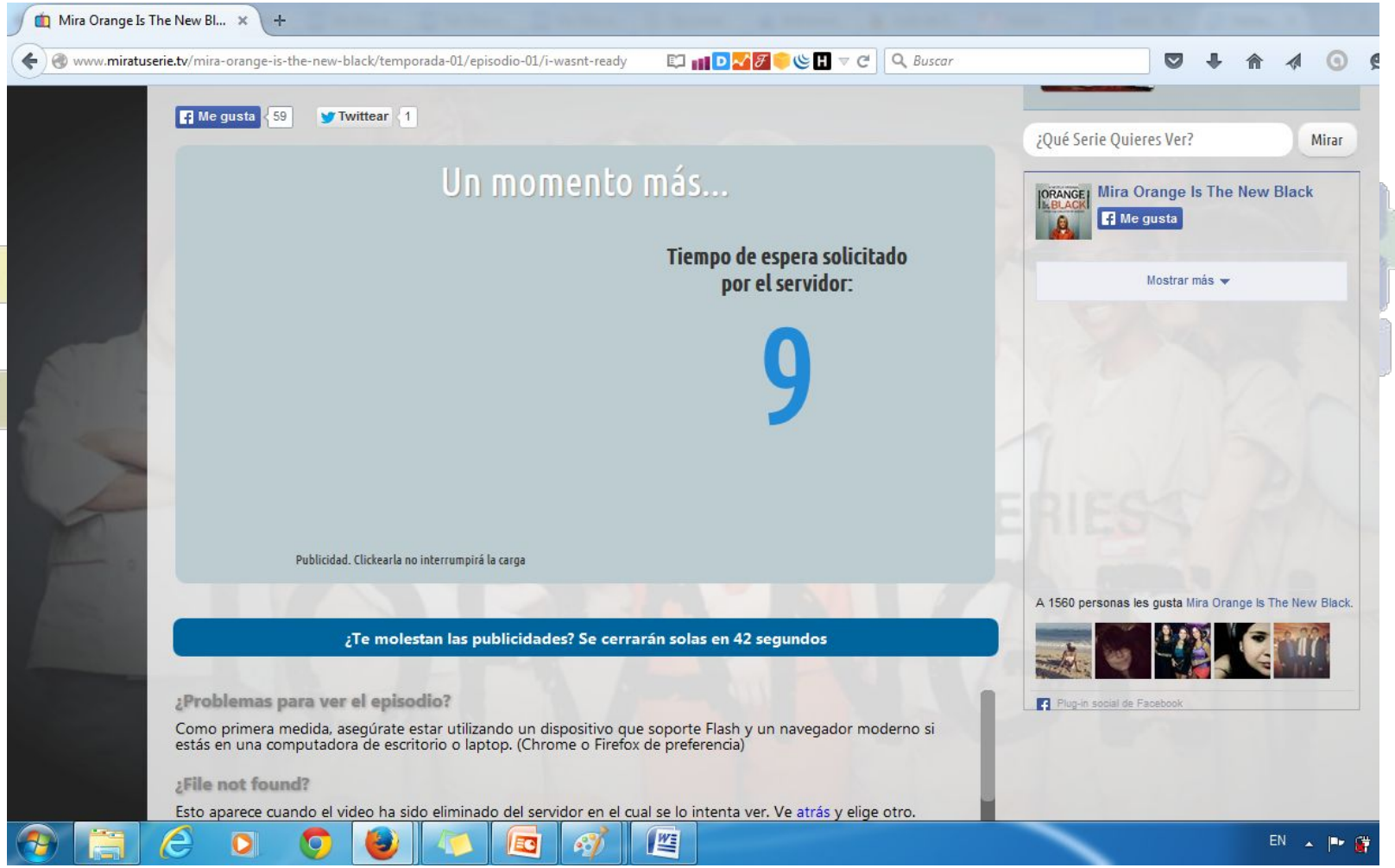
Securizando el Navegador (3)

- Complementos de seguridad
  - AdBlock-Plus
  - No-Script
  - ScriptSafe
  - HTTPS Everywhere
  - Ghostery

¿Qué tan efectivo es?



¿Qué tan efectivo es? (1)



¿Qué tan efectivo es? (2)

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Seguridad en Equipos

Los riesgos

- Virus
- Gusanos
- Spyware
- Troyanos
- Ransomware

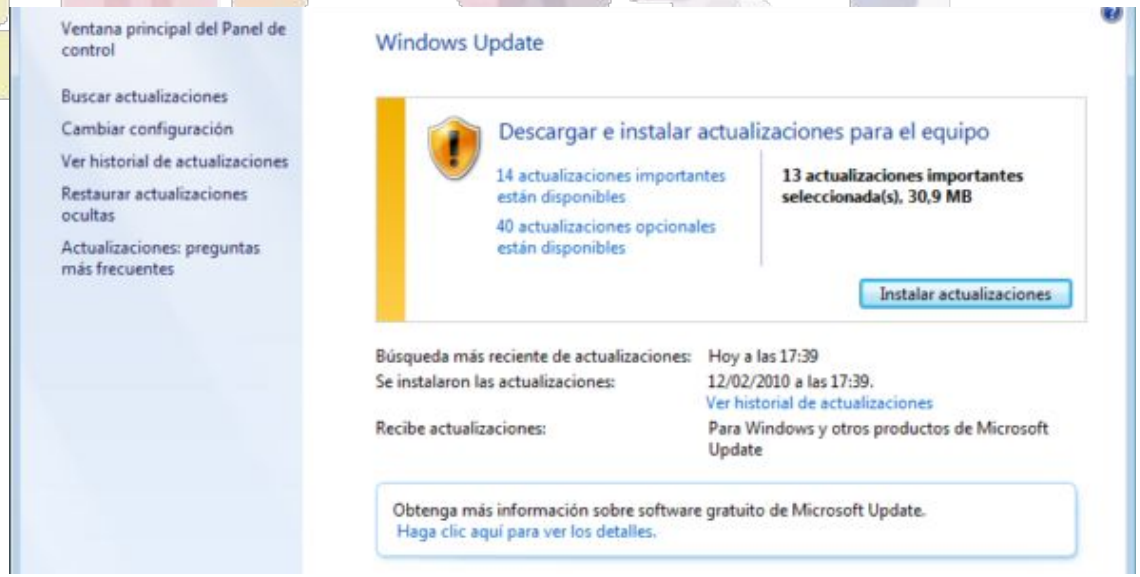
¿Cómo entran? ...

Vulnerabilidades

- Sistema operativo:
  - Windows
  - Linux
  - OS X
  - Android
- Programas o aplicaciones:
  - Office
  - Java
  - Navegadores

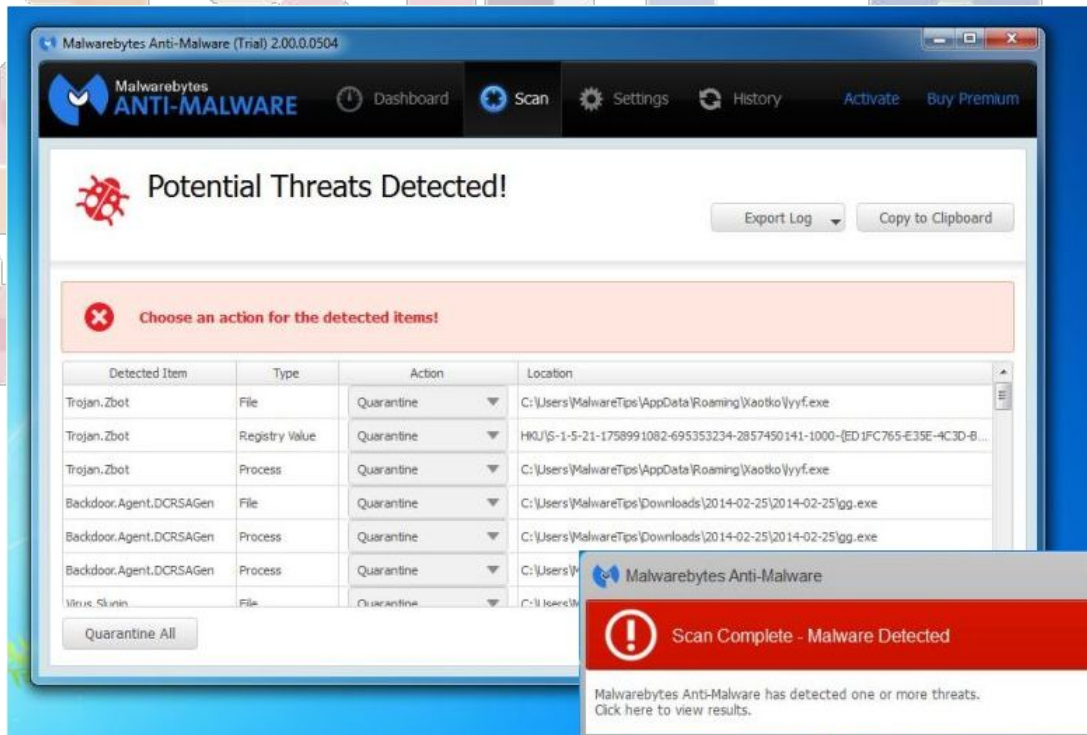
¿Cómo protegernos del malware?

- Actualización permanente del sistema operativo y aplicaciones
- Usar software legal
- No descargar programas de dudosa reputación
- Deshabilitar la ejecución automática de dispositivos USB
- Contar con software de seguridad



Software de seguridad

- Antivirus
- Antimalware
- Firewall



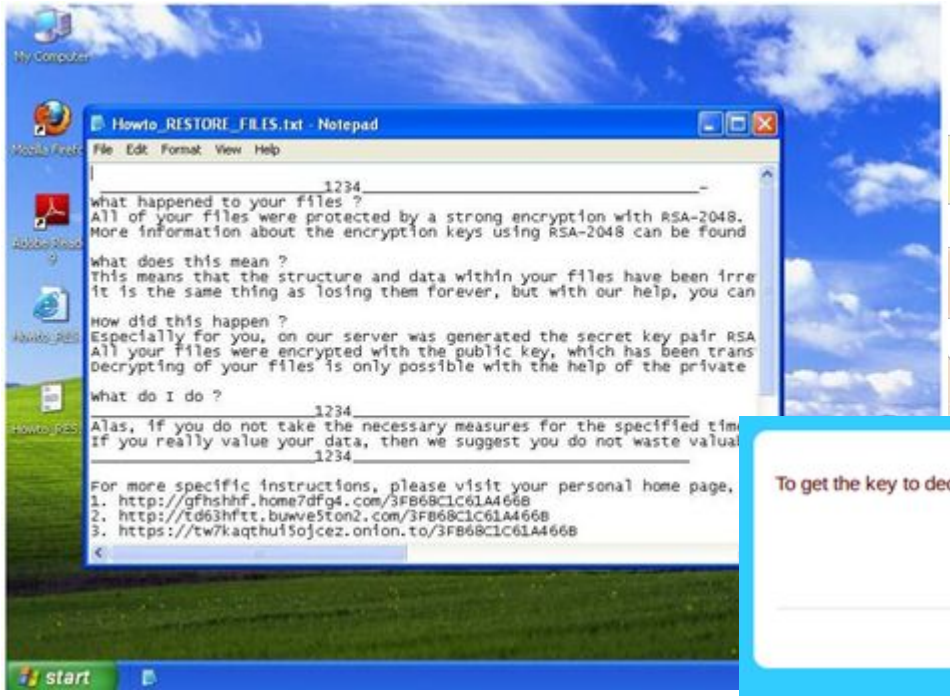
Free vs. Premium

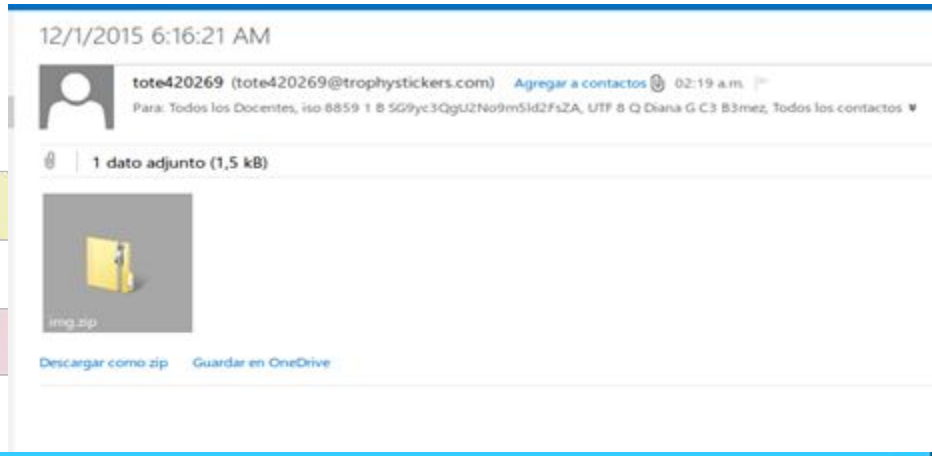
Malwarebytes Anti-Malware Key Features	Free	Premium
REAL-TIME PROTECTION	✗	✓
MALICIOUS WEBSITE BLOCKING	✗	✓
AUTOMATIC UPDATES	✗	✓
FAST HYPER SCANS	✗	✓
SCHEDULED SCANS	✗	✓
ADVANCED MALWARE DETECTION	✓	✓
ADVANCED MALWARE REMOVAL	✓	✓

Ransomware


Your personal files are encrypted.
Your personal files are encrypted.
Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.
You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.
Press 'View' to view the list of files that have been encrypted.
Press 'Next' to connect to the secret server and follow instructions.
WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
View
71:59:07
Next >>
can open it and use copy-paste for address and key.

Ransomware (1)





SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

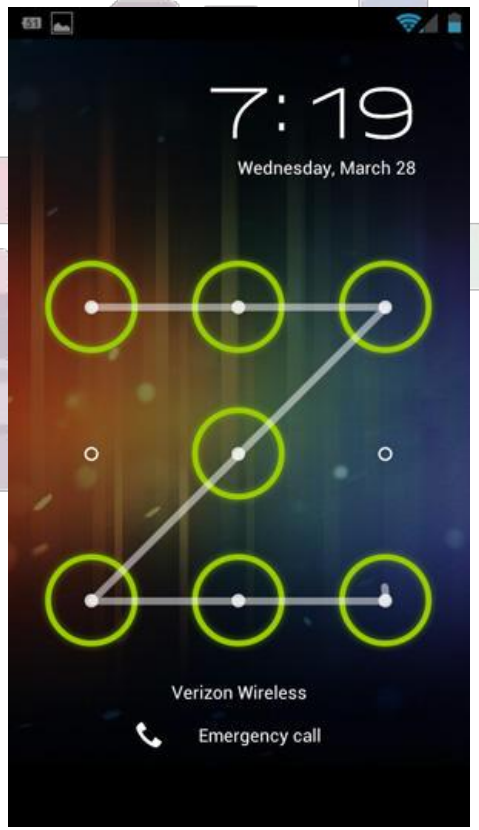
Protección de Datos

Los riesgos

- Robo de equipos
- Daños
- Pérdida de equipos
- Malware (Ransomware)
- Intrusiones

¿Cómo proteger nuestros datos?

- **Contraseña de inicio de sesión**
- **Pantalla de bloqueo**



Encriptación

Cada vez que se quiera acceder a los mismos, se deban descifrar mediante una **clave**.

- ✓Encriptación de disco
- ✓Encriptación de archivos

Herramientas nativas del SO:

- Windows: EFS, Bitlocker
- Mac OS X: FileVault
- Linux

Encriptación (1)

Herramientas de terceros:

Windows:

- AxCrypt
- AES Crypt
- Challenger
- Conceal

Mac OS X:

- Scrambler
- Espionage
- DocWallet

Multiplataforma:

- KeyParc

Backup

Más importante que nunca ..

Ransomware

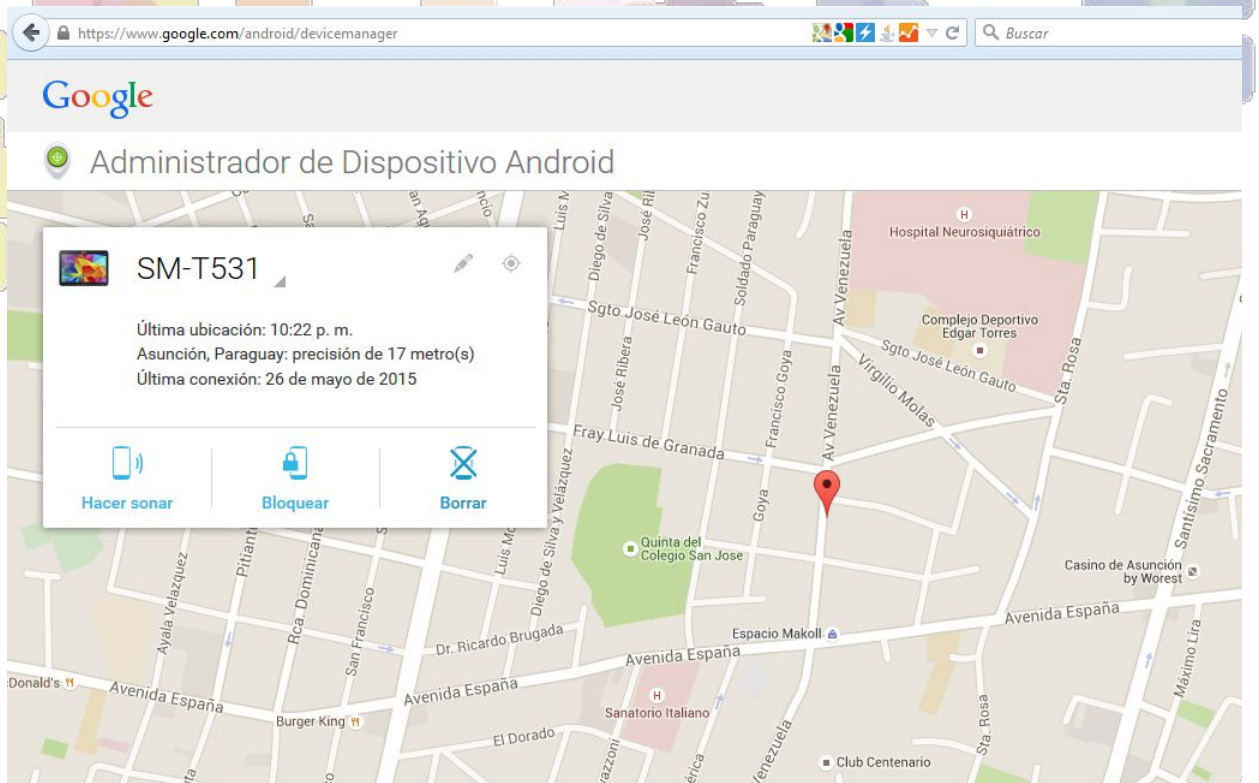
Borrado remoto

Soluciones anti-theft

- Captura de pantalla o foto
- Bloqueo remoto
- Borrado remoto
- Localización

✓ **Android Device Manager**

✓ **iOS: iCloud**

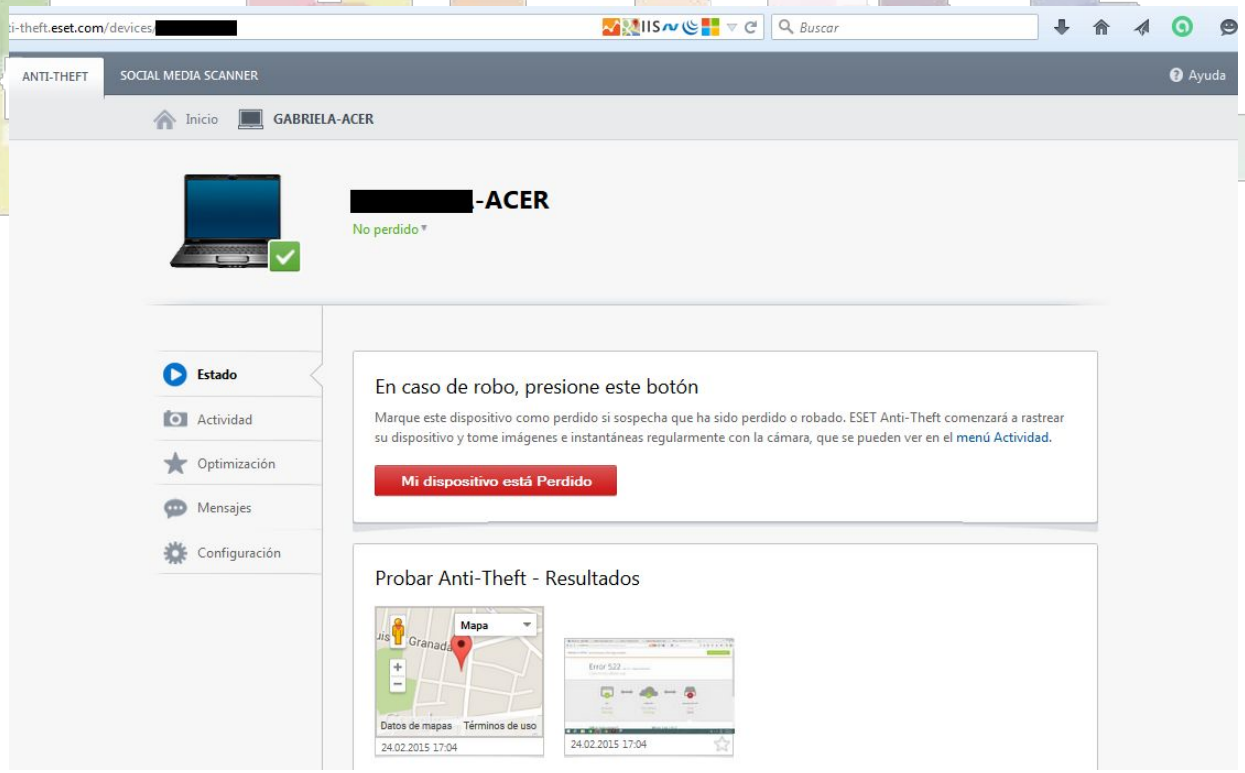


Borrado remoto (1)

Soluciones anti-theft:

- ESET Anti-Theft
- Norton
- Prey

DATO: Generalmente se requiere que el equipo se conecte a Internet.



SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Muchas gracias!

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS

CERT-PY

@CERTpy

/CERT-Py

www.cert.gov.py

denuncias: abuse@cert.gov.py
contactos: cert@cert.gov.py