Fundación Germán Sánchez Ruipérez

Navegación segura: una apuesta de trabajo y de futuro

Jornada Regional de Participación – 5 de febrero de 2011

Valladolid

Índice

Ciberespacio, Internet o Planeta Web

Extensión: La Tierra y la EEI

Población (2010):
- Humanos: 1.967 millones
- Servidores: 274 millones

Población (2000):
- Humanos: 361 millones
- Servidores: 25 millones

El gran despegue: Web 2.0

Tras la crisis de las puntocom (2000 -2003)

Web de Lectura / Escritura

Inteligencia colectiva

Colaboración

Ingente cantidad de información

¿Por qué navegamos por la Web?

Información

- 1,2 *zettabytes*
- Múltiples formatos

Contactos y relaciones entre personas

- Correos electrónicos
- Amigos de redes sociales

Servicios

- De todo tipo: bancarios, tiendas, formación, etc.
- Nos evitan desplazamientos y ahorramos tiempo

¿Cuál es nuestro vehículo?

Un dispositivo con un navegador de Internet instalado

Es nuestro vehículo de unión entre el mundo real y el virtual

¿Por qué hay amenazas en Internet?

Traslado al mundo virtual de los defectos del mundo real:

- Conseguir dinero fácil
- Acumular y controlar información
- Ganar poder

En Internet no han surgido nuevos comportamientos dañinos sino que se han adaptado del mundo real al virtual

En ocasiones los ha facilitado por el “supuesto” anonimato.

¿Qué tipos de amenazas existen?

Amenazas de Internet o informáticas

- Software con malas intenciones: malware
- Riegos en la comunicación (webs, email, redes sociales)

Amenazas por Internet

- Acciones y conductas dañinas que también se ejercer por Internet: acoso (*ciberbullying*, *grooming*), injurias, apropiación de propiedad intelectual, adicción…

Amenazas informáticas – Malware (I)

Malware: Pequeños programas que se instalan sin nuestro permiso

Objetivos:
- Dañar el equipo
- Recopilar información privada
- Controlar el ordenador
- Enviar publicidad

Varios tipos de ataques que pueden estar combinados

Amenazas informáticas – Malware (II)

Virus

- Se copian a sí mismos y se multiplican rápidamente en el ordenador
- Dañan el equipo, destruyen archivos, formatean los discos u ocupan disco y memoria
- Fueron los primeros en surgir

Gusanos

-Son capaces de replicarse en distintos ordenadores a través de redes

Troyanos

-No se replican pero abren puertas traseras por las que envían información privada o reciben otro malware

Amenazas informáticas – Malware (III)

Spyware

- Monitoriza nuestro comportamiento en el ordenador
- Pueden registrar las pulsaciones del teclado, las páginas web que visitamos e incluso hacer capturas de pantalla
- Estos se envían al autor del *spyware*

Adware

- Envía publicidad mediante ventanas emergentes o enlaces automáticos

Ransonware

- Secuestra documentos encriptándolos o protegiéndolos con contraseña
- Sólo se recibe la contraseña si se envía dinero o se realiza una compra.

Amenazas informáticas – Redes zombies

Bot

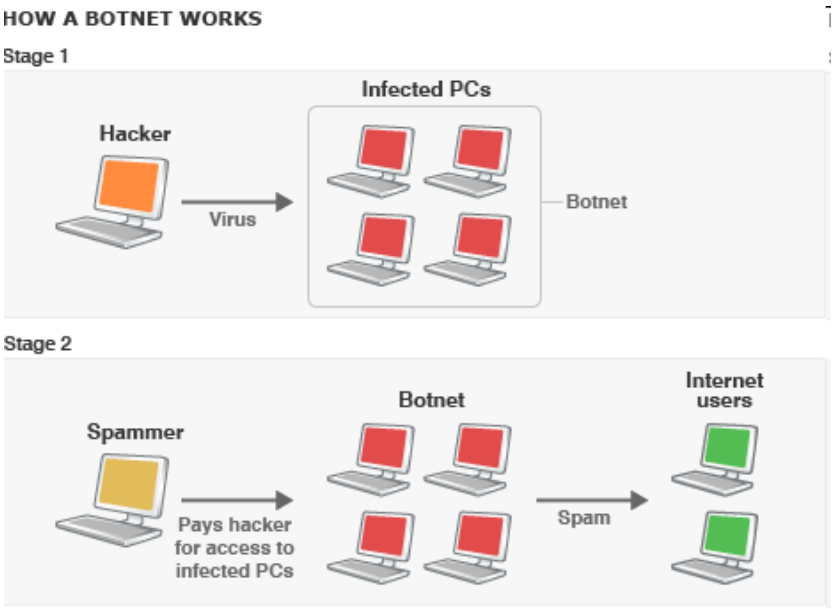
- Pequeño programa que permite el control externo de un ordenador

Botnets o redes zombies

- Conjunto de ordenadores controlados por un único servidor central a través de bots

¿Para qué se usan?

- Envío de correo electrónico basura
- Ataques de denegación de servicio a servidores
- Se venden o alquilan
- Ciberguerra (Stuxnet, Wikileaks)



Stage 1: A hacker sends out a virus or worm over the internet to infect vulnerable home computers. This creates a network of slave machines known as a botnet. Stage 2: The hacker sells or hires out the botnet to other criminals who use it for fraud, spamming, DDoS attacks and other cyber crimes.

Síntomas de infección por malware

- Lentitud general en el equipo o en la conexión.

- Los programas tardan mucho en ejecutarse o dan muchos errores.

- Falta de espacio en el disco duro.

- Falta de memoria.

- El disco duro “rasca” constantemente.

- Aparecen nuevos ficheros con nombres extraños.

- Aparecen gráficos, mensajes o sonidos extraños.

- Comportamiento general “errático”: reinicios, cortes en acceso Internet, etc.

Otras amenazas en Internet – Navegando por la web

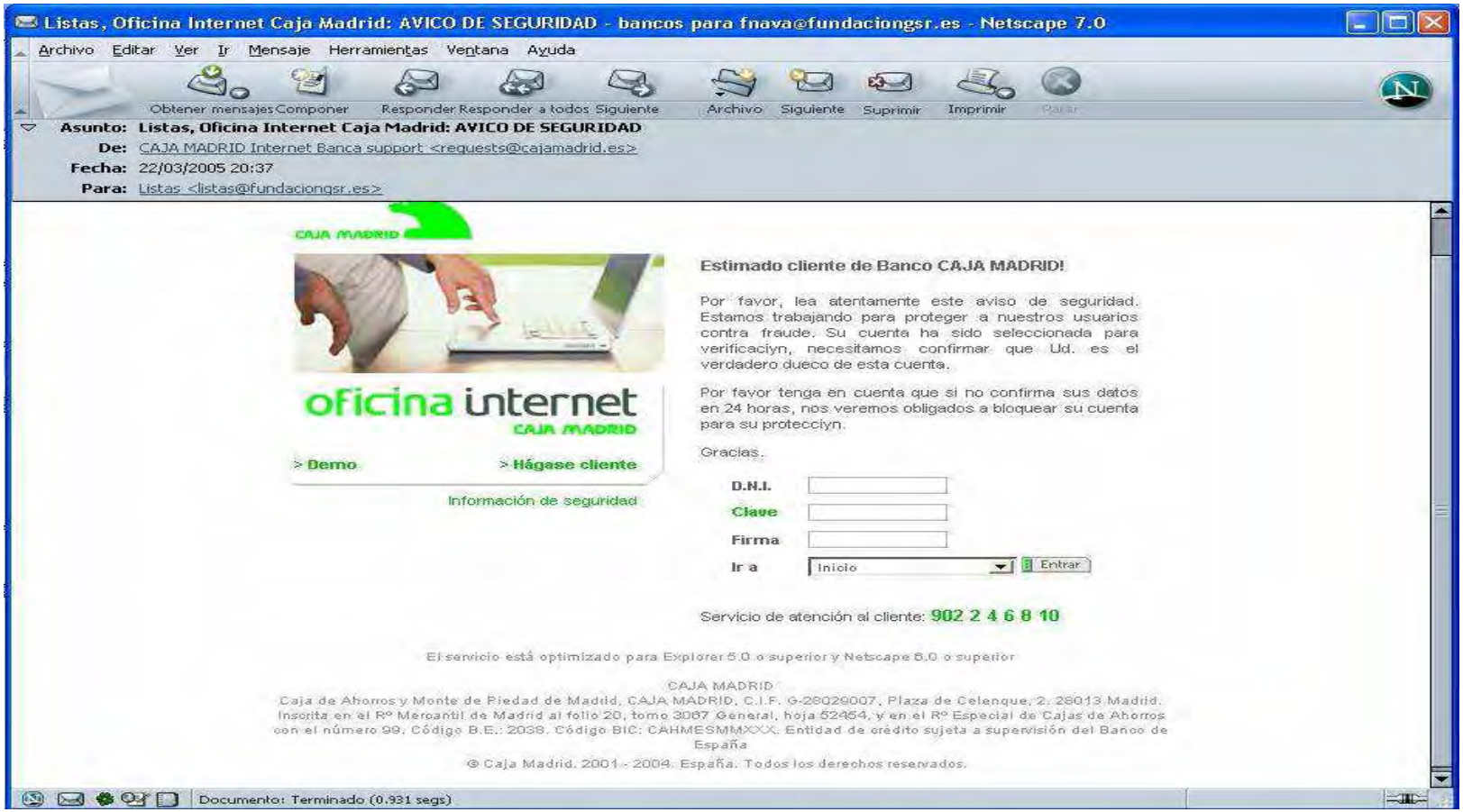
Phishing

Cualquier intento vía teléfono, correo electrónico, fax, web... destinado a obtener información personal para suplantar nuestra identidad: contraseñas, número secreto de la tarjeta de crédito

Pharming

El acto de secuestrar un página web legítima para redireccionarla a un sitio web falso que se parece al original. La web falsa recolecta la información una vez que se ha introducido.

Otras amenazas en Internet – Navegando por la web



¿Cómo nos llegan?

El principal problema está en el factor humano:

- Descuidos, desconocimiento o malintención
- Ingeniería social: tratar de establecer confianza para luego obtener información

"Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es una llamada a un empleado desprevenido para entrar sin más."

Jefe de Seguridad Informática de cualquier empresa

¿Cómo nos llegan?

- Bulos (hoax) por correo electrónico o en redes sociales
- Por el correo electrónico no deseado
- Descargando e intercambiando archivos (P2P)
- Por memorias USB, discos duros u otros soportes de almacenamiento

Vídeo

Hoax o Bulo

Mensajes falsos: alertas sobre virus incurables; falacias sobre personas, instituciones o empresas, mensajes de temática religiosa; cadenas de solidaridad; cadenas de la suerte; métodos para hacerse millonario; regalos de grandes compañías; leyendas urbanas…

Pautas para reconocer un bulo en Internet

1. Los bulos son anónimos, no citan fuentes (ya que carecen de las mismas) y no están firmados para evitar repercusiones legales
2. Los bulos carecen de fecha de publicación y están redactados de la manera más atemporal posible para que pervivan el máximo tiempo circulando en la red
3. Los bulos contienen un gancho para captar la atención del internauta.
4. Los bulos están por general escritos en castellano neutro (en el caso de que este sea el idioma utilizado), para facilitar la difusión a nivel internacional.
5. Los bulos normalmente contienen una petición de reenvío: Se solicita el reenvío para alertar a otras personas, para evitar mala suerte, para evitar la muerte, o con cualquier otro motivo.

El objetivo de esta petición de reenvío reside en captar direcciones IP, crear bases de datos, realizar posteriores campañas de correo masivo o simplemente difundir la información falsa el máximo posible.

Spam

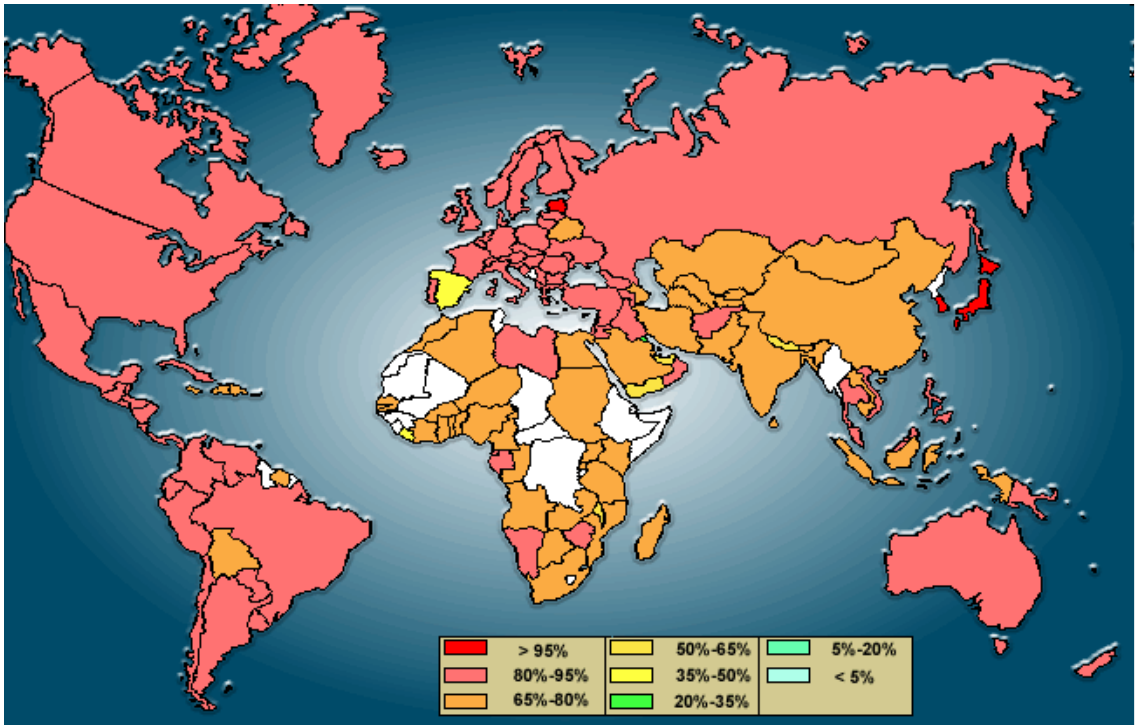
Correo basura

- Más que una amenaza es una molestia por su volumen

- Pueden ser una puerta de entrada de malware

- Son también parte de compras fraudulentas, estafas bancarias, incitación al *phishing*.

- 81 % de spam



¿Cómo nos protegemos?

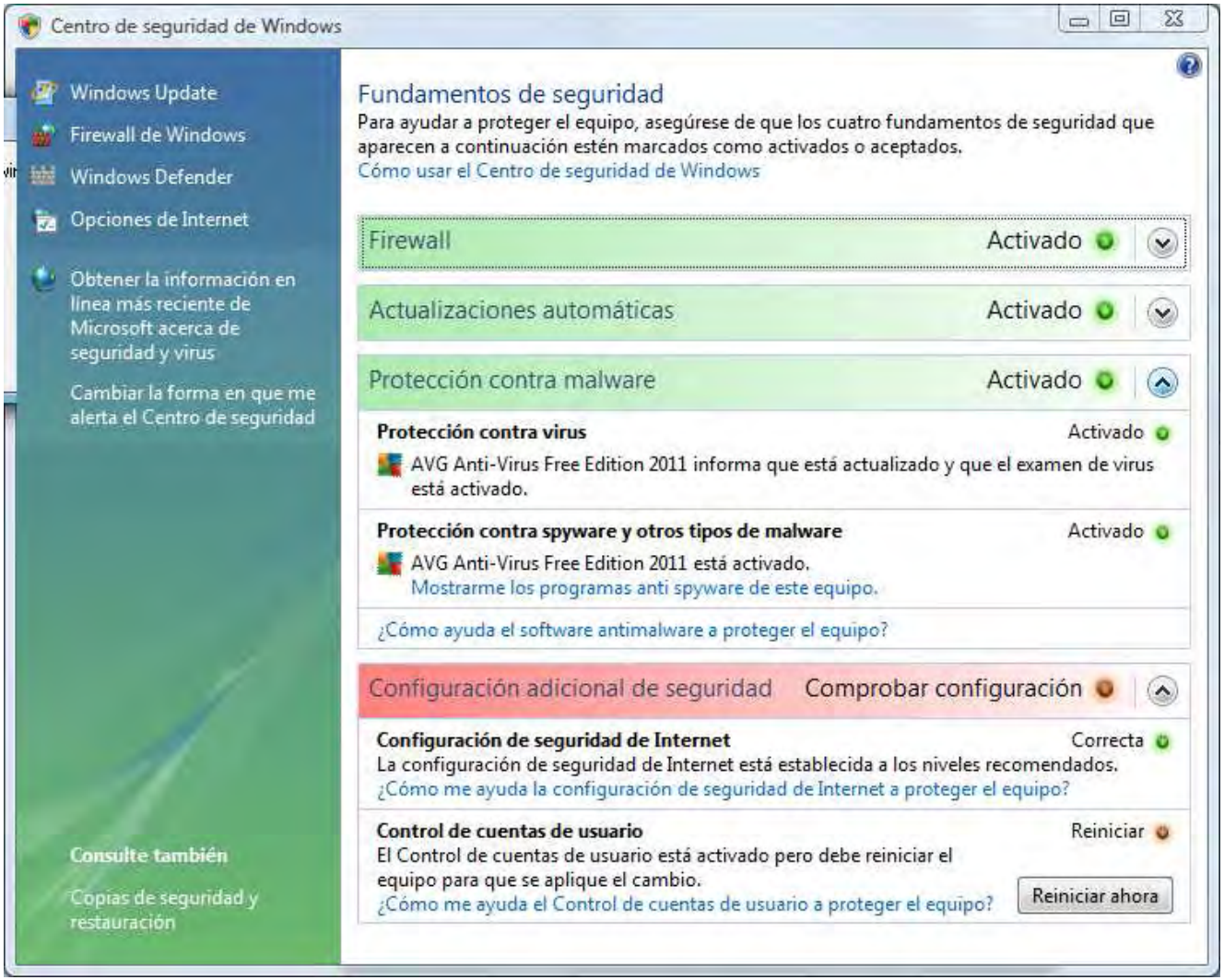
PREVENCIÓN

- Correcto mantenimiento de nuestro vehículo de navegación

- Prudencia en la navegación: Observación y sentido común

- Aprendizaje continuo: Información y formación

Mantenimiento



Mantenimiento – Kit básico

1. **Proteger el ordenador con contraseña y crear varias cuentas**

2. **Actualizaciones automáticas del sistema operativo**

3. **Cortafuegos (Firewall) activado**

4. **Instalar y TENER ACTUALIZADO un antivirus**

- Existen muchas opciones gratuitas que funcionan muy bien
- Actualización diaria (se puede automatizar)

Mantenimiento – Kit básico

5. Mantener actualizado el navegador

6. Instalar y tener actualizado un programa antiespías

- Existen muchas opciones gratuitas que funcionan muy bien
- Actualización semanal

7. Haz copias de seguridad de la información importante

Observación y sentido común – Consejos básicos

Buena gestión de las contraseñas

- Crear contraseñas seguras
- No guardarlas en un fichero en el propio ordenador
- NUNCA compartirlas con otras personas

Detente un momento: lee y observa donde estás a punto de hacer clic

- ¿Te da confianza lo que estás viendo?

Observación y sentido común – Consejos básicos

de PayPal <Services@Support.com>
asunto ***SPAM*** Tu cuenta ha sido temporalmente limitada
para undisclosed-recipients:;

Correo basura

Estimado Usuario,

Tu cuenta ha sido temporalmente limitada

Haga click aqui para resolver el problema

Gracias.
* Porfavor, no responda a este e-mail, ya que tu replica no será recivida. Esto es una notificación automática de nuestro nuevo sistema de seguridad.

Atentamente,
El equipo de seguridad de PayPal.

http://alamcta.org/includes/js/management/financial/login.html?cmd=_login-run

Consejos básicos – Páginas web

1. Ten cuidado con aquellas páginas que te piden instalar un software.

2. Escanea con el antivirus todo aquellos que te bajes antes de instalarlos

3. En las tiendas en línea, estate atento a los símbolos de confidencialidad y a su seguridad.

4. En servicios bancarios y con administraciones usar el certificado digital o el DNI electrónico

Consejos básicos – Correo electrónico

1. Asegúrate de que tu gestor de correo o tu correo web tiene un antispam
2. Comprueba que tu antivirus escanea los adjuntos de los correos electrónicos
3. Observa esos correos no deseados o con apariencia extraña, independientemente de quién te los envíe.
4. No pinches en los enlaces sospechosos de spam ni en los que te piden datos personales, sobre todo si son bancarios
5. Cuando se envía un correo a mucha gente HAY QUE ocultar a los demás la lista de destinatarios
6. No sigas las cadenas

Consejos básicos – Intercambio de archivos (P2P)

1. Descárgate el programa de intercambio del sitio oficial. No uses modificaciones.

2. Mira los comentarios que hay sobre cada archivo y su información

- Te avisan sobre si el archivo es falso, tiene virus, etc.
- Puedes comprobar si efectivamente es lo que buscas o se trata de algo completamente distinto (pornografía)

3. No compartas directorios o discos duros completos. Sólo una carpeta

- ¿Dejarías toda tu casa a disposición pública?

Consejos básicos – Redes sociales

1. Piensa lo que vas a escribir o el contenido que vas a subir
   - ¿Lo harías en el mundo real?
   - ¿Es delito?

2. Investiga y configura la configuración de privacidad de tu red social

3. Sé respetuoso con los demás

4. ¿De verdad tienes que aceptar cómo amigo a todo el mundo?

Vídeo

Consejos básicos – Los menores de edad

Ten el ordenador en un zona común de la casa

Crea una cuenta exclusiva para él con pocos permisos

Acuerda con el niño los períodos de tiempo en que puede conectarse

Busca con él páginas adecuadas, divertidas e interesantes para él.

Usar un filtro de contenidos

Habla con los niños sobre los riesgos de dar información personal a desconocidos o de publicarla (¿no les decimos que no hablen con extraños en la calle?)

Enséñales las reglas de educación en Internet

Información sobre seguridad en Internet

Instituto Nacional de Tecnologías de la Comunicación (INTECO)

- Observatorio de la Seguridad de la Información
- Centro de respuesta a Incidentes
- Juego navegación segura

Oficina de Seguridad del Internauta (OSI)

Internet Segura

E-legales.net

Información sobre seguridad para menores

Chaval.es

Pantallas Amigas

Protégeles

Plan de Prevención del Ciberacoso y Promoción de la Navegación Segura en Centros Escolares de la Junta de Castilla y León

Internet Sin Riesgos

Secukid

Formación para padres

Guía de formación TIC para padres y madres de menores de 3 a 11 años

Escuela de Padres TIC – Padres analógicos, hijos digitales

escuela de padres TIC

PRÓXIMAMENTE...

Fundación Germán Sánchez Ruipérez

GRACIAS