Etica y seguridad en la Red

- El mundo de la información y la comunicación esta cambiando.
- Los cambios van mas deprisa que la formación
- Los delincuentes también “se actualizan”

Patológico...

Lo que es anormal, también lo es en la Red

- asaltar ordenadores ajenos,
- mandar virus, troyanos
- difamación,
- robo, etc.
- Y... ¡enorgullecerse de la ignorancia!

Compañerismo

- La red la usamos todos, ... y tenemos que compartir el caudal.
- Aplicaciones del tipo Gnutella, Edonkey, Kazaa, Emule, Bittorrent, Freenet, etc acaparan el ancho de banda en perjuicio de los demás.

y Solidaridad...

Para mandar grandes archivos hay cosas mejores que el mail

- El mail tiene un receptor... O muchos (listas de mail)
- Considerar la capacidad del receptor ...
  - Forma de conexión....
  - Utilidad...
  - Filtros
- Alternativas: dar url, ponerlo en web, sftp, correo postal!

Propiedad intelectual:

- Nada cambia porque se haga en Internet.
- Paginas web con programas “piratas” o con ‘crack’: además de tener “otros” contenidos y banner indeseados, insertan trojanos

Seguridad del sistema

- Dos caras de la misma moneda
  - Anverso: sencillez de manejo
  - Reverso: facilidad para el atacante.
- Su seguridad es la nuestra...
  - Si usted no quiere aprender, ahorrese el ordenador, por favor.

Sensatez..

Las llaves son las contraseñas

- Diferentes para cada cosa
- Complejas
- Sin sentido
- Memorizarlas
- Discrección

Cuidar los recursos

- Acceso físico por terceros indeseables
  - ordenador, discos, CD-ROM...
- Acceso remoto
  - ¿Quién puede estar interesado en mi persona?
    - Recoger datos de terceras personas.
    - Medio para atacar a otros.
    - Fines destructivos

Reglas básica: prudencia

- Configurar adecuadamente los programas (navegadores, lectores de correo, programas de IRC, intercambiadores, etc...) para que no ejecuten automáticamente programas desconocidos, ni reciban archivos, etc
- Nunca ejecutar programas ni abrir ficheros en aplicaciones con capacidades de programación, que provengan de fuentes no confiables (aun amistades)

Ataques a la seguridad: ‘Infecciónes’

- virus (cuyo efecto puede ser desde la destrucción del contenido almacenado, a efectos más o menos molestos en el uso de la máquina)
- bakdoors
- troyanos
  - todos ellos comparten la forma de infección: ejecutar código malicioso en nuestro ordenador;

‘Fisiopatología de la infección’

- Auto-replicación
- Envío de nuestra información a terceros,
- Instalación de programas ‘durmientes’ a la espera de órdenes remotas
- Utilización de nuestros recursos para ser utilizados en ataques contra terceros; (DoS: Distributed Denial of Service-)

Peligro con:

- Todos los ficheros ejecutables: exe, sct vb bat
- Aplicaciones ofimáticas con capacidades programables:
  - Los ficheros con .doc y .xls (entre otros) pueden contener miniprogramas perniciosos
    - No vale renombrarlos
  - Mail con html: pueden contener código malicioso en java, javascript, Visual Basic Script, ...)

‘Puertas de entrada’

- Múltiples vías:
  - A través de otras personas (disquetes, etc.).
  - Como parte del código de otros programas ejecutables normales que conseguimos en la red,
  - Intercambio de ficheros P2P (tipo Napster, videos...),
  - Ficheros adjuntos de mail, recibidos por IRC, etc.

Mas vale prevenir....

- Disponer de un antivirus y actualizar a menudo (a diario).
- Atención a reiniciar (si procede)
- Actualizar el programa el fabricante produzca versiones mas actuales

Prudencia con el mail

- Nadie necesita enviar documentos en formatos peligrosos. (nosotros tampoco)
- Es más seguro y conveniente enviar solamente texto, (y ocupa menos espacio)
- Cuando el aspecto es importante, usar formatos que sean seguros (rtf, pdf (ojo), ps, formatos de imagen, ...).
- El html también puede ser peligroso, pues puede contener código ejecutable.

La confidencialidad ...

- Internet no fue diseñada para ser segura, sino fiable y robusta.
- Para llegar de un ordenador a otro, hay multiples caminos,
- No hay recorridos predeterminados.
  - La información se va transmitiendo por nodos intermedios, sobre los que no tenemos ningún control, ni casi conocimiento.

Confidencialidad ... ?

- Alguien puede ‘escuchar’ nuestras comunicaciones, sin poder detectarlo.
- Alguien generar información y transmitirla, suplantandonos.
- Alguien puede interceptar nuestra comunicación y modificarla.
- Cualquiera puede generar una información, transmitirla, y después negarlo, simulando haber sido suplantado

Secretos a gritos:

- El email no goza de confidencialidad: tarjeta postal
- El remite nunca es seguro

Soluciones:

- Criptografía,
  - Julio César: sustitución de cada letra por su tercera siguiente en el alfabeto.
  - Parece ser que también Mesopotamia, India y China, Grecia y Egipto utilizaban sistemas similares.
  - Desarrollo a partir del final de la I Guerra Mundial.
  - Algoritmos no retornables
- Firma digital

Discreción:

- No dar más información de la habitual
- Cuidado con el acceso al ordenador
- Responsabilidad de la información que manejamos: secreto profesional
- Cuidado con el medio de almacenamiento: discos, CD etc
- Cuidado con las transmisiones
- Ley de Protección de datos.

Spam

- El spam (correo masivo no solicitado) es delito
  - Utilización de servidores de mail desprotegidos
  - Remites falsificados
  - Pueden enviar spam con nuestro remite
- Prevención:

Spam

- El spam (correo masivo no solicitado) es delito
  - Utilización de servidores de mail desprotegidos
  - Remites falsificados
  - Pueden enviar spam con nuestro remite

Prevención del Spam:

- Fuentes: mail en paginas web.
- Suscripciones “inocentes
- Ojo a la navegación...
- (opcional, no configurar el mail en el navegador)

Lucha contra el spam:

- Ignorarlo:
  - No desuscribirse.
  - No adquirir lo ofertado
  - No incentivarlo visitando la web
- Protestar al admin del servidor abierto
  - ¡ Ojo a quien se protesta!

Lucha contra el spam:

- No incrementarlo...
- La Solidaridad mal entendida... HOAX:
  - "Cuidado, virus muy peligroso!.
  - “mande este mail a toda su lista de contactos”
  - “no rompa la cadena...”

Sensatez:

- Datos bancarios por Internet:
  - Robots buscadores de 20 dígitos
  - Solo mediante paginas cifradas https.

Optimismo, pero...

- Estar preparados para lo peor:
  - Copias de seguridad!
  - Guardar las copias se fuera del propio ordenador
    - otro disco duro,
    - disquetes,
    - cintas,
    - CD-ROM.
- Estar al día