aula MENTOR

GOBIERNO DE ESPAÑA

MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

SEGURIDAD EN INTERNET

AULA MENTOR

educacion.es

Nipo: 660-08-332-X

Autoría:
Pedro García Guillén

Edición:
Inmaculada Sánchez Peñas

Revisión y actualización:
Pedro Martín Echeverría

Coordinación pedagógica:
Cristina Prada Díez

Diseño de portada:
Denica Veselinova Sabeva

INTRODUCCIÓN

Internet, por su propia filosofía de construcción, es una red abierta. Tanto su popularidad como su éxito están fuera de toda duda y en perfecta consonancia con el concepto de globalización. Nunca antes en la historia de la humanidad, el ser humano ha tenido al alcance de la mano la capacidad de acceso a la información y comunicación que brinda Internet.

Internet es de por sí una cultura que se retroalimenta constantemente y que, con el paso del tiempo, no deja de sorprender a propios y extraños.

Sus orígenes, descartando su utilización como medio de protección de las comunicaciones en caso de guerra nuclear (Arpanet), no han podido ser más altruistas:

- El protocolo TCP/IP utilizado por los ordenadores que se conectan a Internet es gratuito.
- Cualquier red y cualquier ordenador puede conectarse sin más costes que los de la conexión.
- No hay ningún propietario de Internet ni ninguna autoridad que pueda imponer un precio o unas condiciones diferentes de las estrictamente técnicas.
- Existen infinidad de documentos, archivos, aplicaciones, etc. disponibles de forma gratuita.

El cálculo estadístico del número de personas que tienen acceso a Internet ya no tiene sentido. Existen redes, particulares e institucionales, bibliotecas, cibercafés, etc. y toda una serie de lugares distribuidos por las ciudades de cualquier parte del mundo, incluyendo los países menos desarrollados, que ofrecen conexión a Internet a cualquier hora y en cualquier momento del día.

Esta extraordinaria facilidad de acceso y popularidad es el principal atractivo de Internet y, a la vez, su talón de Aquiles: también las personas que pretenden emplearla con un fin malicioso gozan de dicha facilidad de acceso.

Partiendo de esta premisa y teniendo en cuenta el efecto que producen las noticias de estafas, sabotajes y espionajes que los medios de comunicación difunden con una cierta regularidad, se ha instalado un clima de inseguridad en muchos internautas que, a medida que dichos actos se magnifican y sofistican, va aumentando.

No resulta difícil vislumbrar que Internet no es más que un fiel reflejo de lo que ocurre en el mundo real. De hecho, una calle comercial de cualquier ciudad del mundo es también accesible a quien quiera aprovechar para delinquir en la confusión de la muchedumbre, y una transacción económica realizada por medios tradicionales es susceptible de ser aprovechada, en cualquier momento, por los amantes de lo ajeno. No obstante, las comunicaciones realizadas por medios tradicionales, cartas o teléfono, son , en ocasiones, mucho más fáciles de interceptar que las comunicaciones a través de Internet. Realizar actividades delictivas a través de Internet requiere unos conocimientos técnicos que no están al alcance de cualquiera pero que, por desgracia, cada vez resultan más fáciles de conseguir.

Por otra parte, las posibilidades de protección de las comunicaciones electrónicas son mucho mayores que las que permiten los medios tradicionales. Hay programas de ordenador gratuitos y muy fáciles de usar que permiten a cualquier usuario el cifrado de sus mensajes de forma que queda plenamente garantizado que sólo el destinatario podrá descifrarlos. También ha surgido toda una tecnología (antivirus, antitroyanos, antispam…) dedicada a la protección y respuesta a un buen número de códigos maliciosos susceptibles de ser transmitidos a través de Internet.

Los certificados digitales y firmas electrónicas aseguran la identidad de las personas con mucha mayor garantía que cualquier firma tradicional. Los sistemas de almacenamiento de datos y su protección frente a accidentes fortuitos o ataques intencionados son más fáciles, baratos y seguros que las cajas fuertes o cámaras de seguridad.

No obstante, el clima de inseguridad persiste y no se aleja de la mente del internauta. El problema es que no hay una cultura de “buenas prácticas” en cuanto a la seguridad en Internet. La sociedad en que vivimos nos ha enseñado desde que éramos niños unas reglas básicas de protección de nuestras propiedades. El gesto de cerrar la puerta de casa, los límites que nos imponemos a la cantidad de efectivo que llevamos en el bolsillo, la forma en que reaccionamos cuando nos aborda un extraño por la calle, son comportamientos que hemos aprendido a lo largo de nuestra vida. En cambio nuestra experiencia con Internet es muy breve y ni nuestros padres, ni nuestros profesores nos dijeron nunca cómo debíamos comportarnos en el ciberespacio.

La protección legal del comercio electrónico ha requerido también la elaboración de nuevas normas. La protección frente a la publicidad indeseada cuyo coste de transmisión recae sobre el consumidor requiere ahora un tratamiento diferente que cuando el coste recaía exclusivamente

sobre el anunciante. El reconocimiento jurídico de las firmas electrónicas y del arbitraje electrónico en los países de la Unión Europea ha establecido un marco legal que garantiza la calidad de los certificados y agiliza los trámites judiciales. Los gobiernos de todo el mundo están interesados en promover el desarrollo del comercio electrónico por lo que están impulsando reformas legales y fiscales que permiten y agilicen las transacciones a través de Internet.

La seguridad en Internet y las leyes que la protegen, están basadas principalmente en los sistemas de encriptación. Esos sistemas son los que permiten que las informaciones que circulan por Internet sean indescifrables, ininteligibles, para cualquier persona que no sea aquella a la que va destinada.

La finalidad de este curso no es otra que la de intentar exponer las técnicas empleadas por los atacantes del ciberespacio, las protecciones que el internauta puede adoptar, los distintos tipos de amenazas que circulan por la Red de redes y que puede llegar a infectar y poner fuera de servicio nuestros sistemas, y, por último, los sistemas de cifrado y su utilización en los medios de pago a través de Internet.

No se pretende que el alumno se convierta en un experto en seguridad, pero si que adquiera una visión realista de la situación, y pueda tomar las medidas que estime oportunas para mejorar su seguridad y experiencia de usuario de este inabarcable recurso que es la World Wide Web.

MÓDULO A

UNIDAD 1

NECESIDAD DE SEGURIDAD EN INTERNET

1 Objetivos.
2 Materiales y recursos.
3 Contenidos.
- **3.1** Panorama actual.
  - **3.1.1** Cuestión de mentalización.
  - **3.1.2** Posibles soluciones.
- **3.2** Criterios generales de seguridad.
  - **3.2.1** Criterios respecto al PC.
  - **3.2.2** Criterios respecto al sistema operativo.
  - **3.2.3** Criterios respecto al software.
- **3.3** Código malicioso.
  - **3.3.1** Algunos aspectos importantes sobre el malware
  - **3.3.2** Tipología de malware.
  - **3.3.3** Software específico
- **3.4** Servicios de seguridad.
  - **3.4.1** Confidencialidad.
  - **3.4.2** Integridad.
  - **3.4.3** Disponibilidad.
  - **3.4.4** Autenticidad.
- 3.5 Ataques.
  - **3.5.1** Ataques contra la confidencialidad del sistema.
  - **3.5.2** Ataques contra la integridad del sistema.
  - **3.5.3** Ataques contra la disponibilidad del sistema.
  - **3.5.4** Ataques contra la autenticidad del sistema.
- **3.6** Ingeniería social.
  - **3.6.1** Medios para evitar los engaños de ingeniería social.

4 Resumen.

1. OBJETIVOS

- Tomar conciencia del peligro real que supone tener ordenadores sin protección alguna conectados a Internet.
- Conocer y saber diferenciar los criterios generales de seguridad que hay que respetar para conectarse con las máximas garantías de seguridad.
- Saber distinguir los diferentes tipos de código malicioso.
- Identificar los posibles ataques que puede sufrir un ordenador conectado a Internet y el código malicioso que los propicia.
- Aprender en qué consiste la Ingeniería Social.

2. MATERIALES

Para el estudio de los contenidos de esta unidad y la realización de sus actividades es necesario:

- Saber realizar búsquedas con Google.
- Instalar y manejar las aplicaciones detectoras de malware Ad-aware y Spy Bot.

3. CONTENIDOS

3.1. PANORAMA ACTUAL

En la actualidad la penetración de Internet ha sido tal, tanto a nivel empresarial como a nivel individual, que la seguridad en el manejo de datos y transacciones se ha hecho imprescindible. En el caso de las grandes corporaciones y empresas la preocupación por la seguridad en Internet es fácil de entender: dichas organizaciones necesitan proteger con la suficiente confidencialidad y privacidad los grandes volúmenes de información reservada que son capaces de generar. Por otra parte, los usuarios de ordenadores personales también deberían vigilar constantemente todo lo referente a la protección de sus datos y a la identidad de las fuentes y destinatarios de los mismos.

En definitiva, la seguridad afecta a todos: a las grandes compañías por ser una tentación y por las consecuencias de una posible filtración, y a los usuarios individuales por su vulnerabilidad.

En España, al igual que en el resto del mundo, la seguridad informática sigue considerándose tanto por parte de la dirección de las empresas como por cada vez más usuarios individuales, como importante o muy importante. Sin embargo, esta importancia que se otorga a la seguridad informática no siempre va unida a la implantación de medidas concretas y

eficaces de seguridad.

La realidad es que cada día podemos encontramos con situaciones tan kafkianas como las siguientes:

- Una empresa concreta, tras haber sido víctima de un ataque de intrusismo que le ha provocado enormes pérdidas, ha invertido tantos miles de euros en seguridad.
- Un usuario confiado ha decidido por fin instalar un antivirus en su ordenador después de haber tenido que formatear su disco duro por la acción de un virus.
- Otro usuario después de tener su ordenador sin ningún tipo de protección conectado permanentemente durante tres meses, se ha encontrado con un incidente de miles de euros en su cuenta bancaria. Ha decidido instalar un cortafuegos.

La moraleja que puede extraerse de estos tres casos, bastante próximos a la realidad cotidiana, es la siguiente: las medidas de seguridad suelen adoptarse a posteriori, cuando el desastre ya ha tenido lugar.

En el panorama actual el acceso a Internet implica la exposición a miles de millones de códigos maliciosos, desarrollados, los menos, para dañar tu ordenador, o, la mayoría, para obtener u beneficio económico.

También es necesario tomar en consideración el llamado “greyware”, que no es software dañino en si mismo, pero que orienta sus esfuerzos a someter al usuario a una publicidad forzada, habitualmente no deseada por el internauta y por la que los autores del código maliciosos obtienen beneficios económicos: spam, adware etc.

Los internautas experimentados han visto evolucionar, a peor, las incidencias y amenazas en la Red y su sofisticación, hasta el punto en que cabe preguntarse ¿A qué se debe este cambio tan dramático en la utilización de uno de los medios de comunicación más universal inventado hasta ahora por el hombre? La respuesta es doblemente contundente:

- La tecnología inicial de Internet es obsoleta.
- La ambición humana no tiene fronteras.

Internet cuando fue creada no contemplaba la mala utilización que podían darse a sus servicios y, por tanto, su tecnología (tipos de protocolos, transmisión de paquetes, etc.) presenta las deficiencias y vulnerabilidades suficientes para que un usuario sin demasiados conocimientos de informática sea capaz de acceder a la información de muchos ordenadores conectados.

Respecto a la segunda afirmación es fácil imaginar que hay gente que, en su afán de ganar dinero de la forma más fácil posible, aprovechan la universalidad de las comunicaciones que brinda Internet para intentar lucrarse sin apenas riesgos ya sea mediante el bombardeo de publicidad (spam y pop up), la apropiación indebida de recursos (troyanos), estafa (phising), etc.

3.1.1. CUESTIÓN DE MENTALIZACIÓN

El problema de la seguridad en Internet no es exclusivamente técnico sino de concienciación de los peligros potenciales que conlleva la transmisión de información confidencial (datos personales, bancarios, códigos de acceso a cuentas y transacciones, etc.) a través del ciberespacio. Es un riesgo nada despreciable el disponer de un gran ancho de banda por donde es posible enviar grandes cantidades de información si ésta puede ser interceptada en cualquier momento.

La seguridad en Internet podría definirse como el conjunto de técnicas destinadas a asegurar la integridad de los contenidos que se transmiten y la confidencialidad del remitente y del receptor.

Las contraseñas y palabras clave no siempre son garantía de seguridad suficiente ya que pueden ser blanco de intrusiones tanto a nivel interno si se trata de una empresa como a nivel externo si se trata de un individuo y de nada sirve esgrimir convicciones del tipo “¿Quién tiene interés en introducirse en mi ordenador si ni siquiera contiene datos de cuentas bancarias?” Es habitual el uso de ordenadores “sin interés” para atacar a un tercero, figurando el ordenador intermedio como autor del ataque.

La realidad es que la situación actual es más grave de lo que parece a simple vista. Por un lado hay que atender a los problemas de seguridad causados por los virus informáticos, cuyo crecimiento y grado de malignidad crece a la par del interés económico, además resulta cada día más preocupante, la inevitable tendencia a utilizar contenidos dinámicos en las páginas web (applets Java, Active-X...), que brindan al usuario páginas web personalizadas y atractivas, pero suponen una vía habitual de introducción de código no deseado, los programas espía que abundan entre los usuarios de los clientes de programas P2P, el correo no deseado molesta en nuestros buzones, los troyanos intentan obtener datos confidenciales y, en definitiva, la abundancia actual de código malicioso ha convertido en insegura la navegación y hasta incluso la simple visualización de páginas de Internet, en ocasiones. La protección que a estos efectos proporcionan los navegadores es siempre insuficiente, como nos demuestra la continua aparición de vulnerabilidades en estos, que van

siendo remediadas, a posteriori, con constantes actualizaciones.

3.1.2. POSIBLES SOLUCIONES

La solución a este problema de seguridad en Internet comprende tres aspectos:

- Mentalización de que la protección es absolutamente necesaria.
- Conocimiento de los tipos de ataques de los que podemos ser víctimas y de los tipos de código malicioso que intervienen en dichos ataques.
- Prevención: utilización de las técnicas necesarias para impedir una gran variedad de ataques, actualización periódica y sistemática de nuestros ordenadores, instalación de software de seguridad y control de nuestras comunicaciones.

En este curso se tratan estos tres aspectos desde el punto de vista del usuario personal con la profundidad suficiente para poder ser abordados sin necesidad de poseer un grado elevado de conocimientos previos en materia de seguridad.

Actividad 1.1 (OPCIONAL)

Utiliza Google para buscar artículos relacionados con la seguridad en Internet. Para ello introduce como criterio de búsqueda “seguridad internet”. Selecciona los tres o cuatro que te parezcan más interesantes y elabora un documento de dos páginas como máximo, titulado: “Opiniones sobre la seguridad en Internet”.

3.2. CRITERIOS GENERALES DE SEGURIDAD

La conexión a Internet por parte de cualquier usuario individual tiene lugar gracias a la concurrencia de los siguientes elementos:

Un dispositivo hardware (el ordenador personal) cuyo funcionamiento permite la conexión.

El software que permite la puesta en marcha del hardware y a la vez sirve de soporte para la instalación y ejecución de las aplicaciones específicas necesarias para la conexión (el sistema operativo).

Las aplicaciones que permiten utilizar los servicios de Internet: el navegador (para páginas web), los diferentes tipos de clientes (e-mail, ftp, P2P...) y aplicaciones específicas (buscadores, gestores de descarga, etc).

Teniendo en cuenta estos tres elementos es posible establecer una serie de criterios de carácter general, a tener en cuenta para incrementar el nivel de seguridad de que se disfruta, como los indicados a continuación.

3.2.1. CRITERIOS RESPECTO A LA SEGURIDAD DEL PC

- Actualizar el equipo. Esta es una medida esencial, las actualizaciones solucionan agujeros de seguridad conocidos.
- Hacer copias de seguridad periódicas de los datos importantes en un soporte distinto: CD, DVD, PenDrives, disco duro externo etc.
- Apagar el ordenador y el router siempre que no se estén utilizando.
- No instalar software de fuentes desconocidas. Estudiar la fiabilidad de una fuente antes de proceder a instalar un software.
- Instalar un antivirus y actualizarlo periódicamente.
- Instalar un cortafuegos, preferentemente con sistema de detección de intrusos.
- Instalar un antispyware y asegurarse de que todo este software de seguridad no presenta incompatibilidades.
- Extremar el cuidado con sistemas de conexión permanente (ADSL o cable), que son la inmensa mayoría del mercado doméstico.
- Eliminar archivos antiguos e inservibles.
- No compartir discos o impresoras a través de Internet.
- No escribir contraseñas en papel ni en documentos del ordenador.
- Cambiar de contraseña periódicamente.
- Elegir contraseñas que respeten unos mínimos criterios de complejidad: más de seis caracteres con letras números y símbolos.
- No utilizar las mismas claves para sitios web peligrosos o desconocidos que para entidades con un alto nivel de seguridad.
- Gestionar los discos duros correctamente: particiones adecuadas, almacenamientos en RAID etc.
- Chequear periódicamente el estado de nuestro ordenador con alguna herramienta de análisis y auditoría de seguridad.

3.2.2. CRITERIOS RESPECTO AL SISTEMA OPERATIVO

- Es conveniente disponer de un disco de arranque del sistema.
- Disponer del CD de instalación para solventar los casos en que haya que reinstalar el sistema total o parcialmente.
- Disponer de versiones originales que permitan las actualizaciones oportunas (paquetes de servicio de Windows). Eliminar los agujeros de seguridad conocidos descargando las actualizaciones del sistema.
- Disponer de un disco de seguridad que nos permita hacer análisis offline, como el de Kasperski

(https://support.kaspersky.com/viruses/rescuedisk), son CD con un núcleo de linux que arrancan desde el lector de DVD y permiten, por ejemplo analizar y (a veces) arreglar un ordenador cuyo sistema no arranca.

- Disponer de un CD de utilidades que nos permita manipular el ordenador en caso de desastre, como por ejemplo el conjunto de utilidades freeware de Hirens Boot (http://www.hirensbootcd.org).

3.2.3. CRITERIOS RESPECTO AL SOFTWARE

- Utilizar versiones actualizadas del navegador instalado. Configurar el navegador apropiadamente, para que no recopile información, como se verá en la unidad siguiente, y, en el caso de que decidamos guardar en él alguna contraseña, que estas estén cifradas por una contraseña maestra de gran complejidad.
- En la medida de lo posible, no dejar desatendidos los ordenadores mientras estén conectados.
- No efectuar nunca la instalación básica de un software descargado. Siempre la avanzada o experta, que nos permite un mayor control sobre la instalación.
- Mantener el anonimato en cuanto a datos personales y profesionales.
- Introducir datos financieros sólo en sitios web seguros, y, por tanto asegurarse de que el sitio web de la entidad cifra sus comunicaciones y presenta su correspondiente certificado de autenticidad. Nunca acceder a un sitio web comercial o financiero a través de un enlace que ha llegado por el correo electrónico.
- No utilizar las mismas contraseñas en los sistemas de alta seguridad que en los de baja seguridad.
- No proporcionar datos personales en sitios web que no garanticen el cumplimiento de la legislación vigente (LOPD) y/o que no tengan un sitio web seguro (SSL).
- Usar cuentas de correo alias (en lugar de la original) para acceder a determinados servicios que exigen la introducción de una dirección de correo electrónico que exista. En determinados casos se puede considerar el uso de direcciones de correo temporales como la que proporciona 10minutemail, por ejemplo (http://10minutemail.com).
- Si no queda más remedio y hay que usar ordenadores públicos o compartidos con terceras personas, cuidar las medidas de protección básicas: desconexión de sesiones, borrado de la memoria caché… en estos casos la seguridad suele ser muy precaria.

Actividad 1.2 (Opcional)

Completa los criterios generales de seguridad expuestos con algunos (al menos uno de cada uno de los tres tipos) que se te ocurran.

3.3. CÓDIGO MALICIOSO

El código malicioso o malware (abreviatura de Malicious software) es la denominación normalmente utilizada para designar a cualquier tipo de programa o código de ordenador cuya función es dañar una o varias partes del sistema informático o causar un mal funcionamiento del mismo, ya sea de un ordenador personal, un servidor o una red de ordenadores.

Aunque el malware más conocido siempre han sido los virus y troyanos en sus distintas variantes, en los últimos años ha ido adquiriendo cada vez más importancia la propagación de nuevos tipos de código malicioso como el spyware que es un software capaz de espiar los movimientos del usuario cuando está conectado a Internet con el objetivo de remitir información valiosa a sus creadores.

3.3.1. ALGUNOS ASPECTOS IMPORTANTES SOBRE EL MALWARE

Su objetivo es extenderse a cuantos más usuarios mejor, ya sea simplemente alarmándolos mediante inofensivos hoax o provocando la destrucción de datos de sus discos duros.

La tecnología actual que permite conectar el mayor número de sistemas informáticos en el menor tiempo posible es Internet y, por consiguiente, es el medio de propagación por excelencia del malware.

La tendencia actual y el futuro a corto plazo del malware se dirige claramente a obtener beneficios económicos (spoofing , phising , troyanos y spyware) en lugar de la destrucción de datos o la ralentización del sistema (virus y gusanos).

Un ordenador sin ningún tipo de protección conectado a Internet a través de una línea ADSL puede convertirse en una máquina comprometida en cinco minutos.

3.3.2. TIPOS DE MALWARE

La siguiente tabla es una primera toma de contacto con las tipologías habituales (virus, gusanos, conejos, troyanos, web-bugs etc.) de malware existente en la actualidad y su objetivo es mostrar la variedad de código