UNIVERSIDAD CARLOS III DE MADRID

La Seguridad informática también es cosa tuya

UNIVERSIDAD CARLOS III DE MADRID

Introducción

Cada día surgen nuevos programas que amenazan la seguridad de los datos y aplicaciones instaladas en los ordenadores. Estos programas utilizan las redes de comunicación para propagarse, por lo que tanto el ordenador del despacho y/o aulas informáticas como el de casa (si utilizas la conexión a Internet) están amenazados. Además, estos programas pueden generar problemas en el resto de equipos conectados a la red.

Como consecuencia de una infección por un virus o gusano, nuestro ordenador se ralentiza, la conexión a Internet o con los servidores de la Universidad se degrada, imposibilitando en ocasiones acceder a algunos servicios de red. En muchas ocasiones incluso pueden ser utilizados sin que lo sepamos para realizar acciones ilícitas de las cuales podemos llegar a ser considerados responsables.

El Servicio de Informática ha editado este folleto que pretende servir de guía para mejorar la protección de los equipos informáticos y evitar los problemas mencionados. En todo caso, no olvides que el componente principal de la seguridad es el factor humano, no las herramientas técnicas, y que todo lo que te proponemos en estas páginas que siguen no cumplirá su objetivo de incrementar la seguridad, si no te involucras activamente en ella.

Ya pero ... ¿Para qué quieren infectar mi ordenador?

Actualmente una de las principales amenazas de Internet procede de las denominadas redes botnet. Estas redes son conjuntos de miles o incluso millones de ordenadores (por ejemplo, la botnet Mariposa desarticulada en España por la Guardia Civil estaba formada por más de 12 millones de equipos en todo el mundo) que han sido infectados con algún tipo de programa malicioso, lo que permite al atacante controlarlas sin tener acceso físico a ellas y sin conocimiento del propietario.

Una vez el equipo ha sido infectado e incorporado a la red botnet, se convierte en un zombi, a la espera de

recibir órdenes del hacker. Éstas hacen que el ordenador infectado sea utilizado para cometer crímenes en la red como el envío masivo de spam, la extorsión o el chantaje en la red, sin que el dueño legítimo sea consciente de ello. Esto permite al atacante obtener importantes cantidades de dinero.

¿Qué puedes hacer para mejorar la seguridad de tu ordenador?

1. Utiliza contraseñas que sean difíciles de adivinar, combina letras, números y signos. Actualízalas con cierta frecuencia.
2. Instala y actualiza el programa antivirus en todos los ordenadores que utilices de forma habitual.
3. Instala de forma periódica los parches proporcionados por los fabricantes no sólo del sistema operativo sino también de las aplicaciones que tengas instaladas.
4. Apaga el ordenador cuando no lo vayas a utilizar durante un período de tiempo largo.
5. Haz copias de seguridad de tu información crítica.
6. Utiliza programas legales y no instales programas sospechosos o que no te sean necesarios.
7. Borra sin leer aquellos mensajes de correo de remitentes desconocidos o que te resulten sospechosos.
8. Alerta sobre cualquier comportamiento extraño de tu ordenador.
9. Ante cualquier eventualidad, utiliza el sentido común y sé cauteloso ante cualquier programa o mensaje extraño.
10. Piensa que “Si algo es gratis en Internet, puede ser que tú seas el «producto» que alguien está vendiendo”.

¿Cómo elegir una buena contraseña?

La contraseña de acceso a los servicios de red, es un elemento que da acceso a múltiples servicios y que es utilizada para identificar al usuario de dichos servicios, por lo que es necesario que la contraseña sea segura y sea difícil de adivinar. Para ello:

- ✓ Elige una contraseña de 8 o más caracteres.
- ✓ Combina letras (mayúsculas y minúsculas), números y signos.
- ✓ Evita los caracteres no ingleses (ñ, ç, _, etc), ya que dan problemas con algunos servicios.
- ✓ Cambia la contraseña periódicamente.
- ✓ Puedes utilizar acrósticos (iniciales de las palabras) de una frase, por ejemplo, "Volverán Las Oscuras Golondrinas En Tu Balcón Sus Nidos A Colgar", daría VLOGETBSNAC. Ahora modificaríamos la contraseña para que tenga minúsculas, números y signos. Por ejemplo podemos sustituir las letras LO por los números 10, insertar una coma tras la G y pasar a minúsculas la V inicial, con ello la contraseña elegida sería v10G,ETBSNAC, fácil de recordar, pero difícil de adivinar. Puedes obtener consejos para elegir una buena contraseña en: **https://correong.uc3m.es/usuarios/claveok.html**

¿Cómo puedo instalar el antivirus y el cortafuegos corporativo?

Uno de los programas maliciosos que existen son los virus y los programas antivirus permiten detectar su presencia y neutralizar sus efectos.

Un cortafuegos es un dispositivo físico hardware o software que impide el acceso a nuestro ordenador desde el exterior. También se llama Firewall en Inglés. Mediante este dispositivo se impide el paso a los hackers y a muchos tipos de virus y gusanos. Los cortafuegos son uno de los frentes de defensa más importantes para mantener la seguridad del equipo.

La Universidad ha adquirido licencia para la utilización del antivirus + cortafuegos de Trend-Micro, para los ordenadores de profesores, personal de administración y servicios y aulas informáticas. Además también se cuenta con licencia para instalarlo en los ordenadores de casa.

Toda la información sobre el antivirus corporativo la tienes en **https://antivirus.uc3m.es** (requiere autenticación en CG).

Desde allí podrás acceder a:

Antivirus para la oficina:
http://www.uc3m.es/portal/page/portal/portal_informatica_antivirus/Officescan

Antivirus para casa:
http://www.uc3m.es/portal/page/portal/portal_informatica_antivirus/InternetSecurity

Antivirus para productos Apple:
http://www.uc3m.es/portal/page/portal/portal_informatica_antivirus/Antivirus%20para%20MAC

Recuerda que los programas antivirus sólo protegen (y no siempre) de virus conocidos. Así, el mejor antivirus es tu suspicacia ante correos inesperados, de asunto sospechoso, de remitentes desconocidos, redactados en lengua que no son la materna del remitente, etc.

¿Cómo mantener actualizado el sistema operativo Windows y las aplicaciones Office?

En el ordenador de la Universidad, los equipos homologados que se compran a través del proveedor oficial se instalan con una Configuración Ofimática Mínima y se adscriben al dominio UC3M. Dicha configuración está preparada para descargar de un servidor corporativo (WSUS) todos los parches que Microsoft hace

públicos los segundos martes de cada mes. El servicio de informática y comunicaciones instala dichos parches en un entorno de pruebas y posteriormente se distribuyen al resto de la comunidad Universitaria a través de herramientas internas. No obstante, se puede forzar la descarga en un momento puntal desde **http://update.microsoft.com/**.

En el ordenador de casa, configura la descarga de parches de manera automática a través del icono de Actualizaciones Automáticas que se encuentran en el Panel de Control de tu ordenador. Si lo deseas puedes forzar tú mismo la descarga e instalaciones de parches visitando la web oficial de Microsoft **http://update.microsoft.com/.**

Puedes obtener más información sobre la actualización del sistema operativo y aplicaciones en **https://asyc.uc3m.es/index.php?Id=50**

¿Cómo hacer copias de seguridad de mi información?

Es posible que un programa malicioso deteriore el sistema hasta el punto de que no sea posible acceder a la información contenida en él. Por ello es recomendable realizar periódicamente copias de seguridad, que permitan recuperar aquellos ficheros importantes.

Puedes utilizar compresores de archivos para que ocupen menos y por lo tanto sea más fácil y rápido realizar las copias de seguridad. Puedes encontrar información sobre la realización del Backup en:

http://www.uc3m.es/portal/page/portal/informatica/CAU/Centro_de_Recursos/hacer_backup_mi_pc

En la Universidad, el personal de la Universidad dispone de un espacio de disco en red, del cual se realizan copias de seguridad de forma periódica. Puedes obtener más información sobre el servicio de disco en red en: **http://sdi.uc3m.es/sistemas/servicios/NT/discos.html**

En casa,

Utiliza CD/DVD si tienes grabadora.
Utiliza lápices de memoria o discos duros externos.

¿Por qué es importante utilizar programas legales?

La utilización de programas legales permite tener acceso a las actualizaciones del fabricante y disponer del soporte técnico necesario.

Una copia ilegal de un programa puede haber sido alterada para realizar tareas que comprometan la seguridad del ordenador. Debemos tener en cuenta que la instalación de programas protegidos por derechos de autor de forma ilegal es responsabilidad de cada usuario, siendo la autoridad competente la encargada de determinar la sanción correspondiente.

¿Por qué no instalar programas para compartir ficheros a través de Internet?

Los programas para compartir ficheros a través de Internet, también llamados P2P ("Peer to Peer"), permiten acceder a ficheros que se encuentran en otros ordenadores, pero también permiten que otros ordenadores accedan a los ficheros de nuestro ordenador. Habitualmente estos programas son utilizados para distribuir ficheros o programas protegidos por los derechos de autor. Como consecuencia de ello:

Nuestro ordenador y la conexión a Internet y servicios de red se ralentizarán.

Puede que descargar un determinado fichero suponga vulnerar los derechos de autor y por lo tanto podríamos estar incurriendo en un delito. Además, estos programas suelen ser utilizados para la distribución de virus y otros programas maliciosos, que pueden comprometer la seguridad de nuestro ordenador. Debemos tener en cuenta que descargar y/o disponer de ficheros o programas protegidos por derechos de autor de forma ilegal es responsabilidad de cada usuario, siendo la autoridad competente la encargada de determinar la sanción correspondiente.

Los programas que nos descargamos y en especial los de tipo “keygen”, “cracks” y similares suelen estar infectados con código malicioso de forma que cuando los ejecutamos permiten a los atacantes controlar de forma remota nuestro ordenador, incorporarlo a una red de botnets y en algunas ocasiones también capturar nuestras contraseñas (de correo, bancarias, etc.) y enviárselas al atacante.

¿Por qué no instalar programas innecesarios?

Cualquier programa instalado en un ordenador consume recursos (espacio en disco, memoria, etc.). Además, todos los programas son susceptibles de contener vulnerabilidades, por lo que la instalación de programas innecesarios ralentiza el ordenador e incrementa el nivel de riesgo. Muchos de los programas que hay en Internet incorporan funcionalidades ocultas que no se indican en la página de descarga. A veces, estos programas

ralentizan el funcionamiento de nuestro ordenador,

algunos de ellos envían información sobre nuestros ficheros a otros ordenadores.

incluso algunos permiten que un desconocido pueda utilizar nuestro ordenador para atacar otros ordenadores.

En otros casos, estos programas configuran el acceso a Internet a través un número de tarificación especial (80x generalmente) y en este caso el perjuicio se advierte en el recibo telefónico.

Recomendaciones de uso del correo electrónico

Habitualmente los programas maliciosos utilizan el correo electrónico como medio de transmisión, por ello:

Actualiza tu programa de correo con los parches y/o versiones más modernas.
Nunca instales programas o actualizaciones de programas que recibas a través de correo electrónico.
No reenvíes ni crees cadenas de mensajes.
Deshabilita la vista previa de los mensajes.
¿Qué hacer con los mensajes sospechosos (respuestas a mensajes que no enviaste, enviados por desconocidos, etc)?

Borra los mensajes sospechosos sin leerlos.
Si deseas leerlos, utiliza el interfaz web **https://correong.uc3m.es**
Nunca abras los ficheros adjuntos que vengan con estos mensajes.

El Servicio de Informática y Comunicaciones nunca solicita la contraseña de acceso, ni envía actualizaciones mediante correo electrónico, por lo que debe desconfiarse de este tipo de mensajes.

Recomendaciones para navegar por Internet

Al navegar por Internet, hay sitios en los que sin ser consciente, el simple hecho de acceder a una página puede suponer la instalación de programas maliciosos en el ordenador. Por ello:

Navega sólo por aquellos servidores conocidos y/o de confianza.

Actualiza tu navegador con los parches y/o versiones más modernas.

Nunca instales programas necesarios para acceder a servicios adicionales (descarga de melodías para móvil, de juegos, etc), suelen cambian tu acceso a Internet utilizando un número de tarificación especial (80x generalmente).

¿Cómo puedo determinar si mi ordenador ha sido infectado?

Cambios en la fecha y/u hora de los ficheros.
Merma de prestaciones (rendimiento o funcionalidades):
- Retardos al iniciar el ordenador o un programa concreto.
- No hay memoria disponible para la ejecución de programas.
- El disco está casi lleno y no se corresponde con los ficheros que tú has guardado en él.
- Ralentización en la conexión a Internet o acceso a servidores de red.

Mensajes de error inusuales o se reinicia.
Han aparecido programas, ficheros o iconos que no has instalado.
Mantiene conexiones extrañas

¿Qué puedo hacer si creo que mi ordenador ha sido infectado?

Comprueba la versión de antivirus y utilízalo para detectar la presencia de virus. Si se trata del equipo de la universidad, puedes contactar con el Centro de Atención y Soporte y solicitar ayuda para la limpieza del equipo. No olvides desconectar el ordenador de la red para evitar que infecte a otros equipos.

Si se trata del ordenador de tu casa lo primero que hay que hacer es actualizar el antivirus para proceder a la limpieza automática del equipo y desconectar el equipo de la red y. Si se desea hacer una limpieza manual, basta con buscar información del virus en **http://antivirus.uc3m.es.**

En **http://www.uc3m.es/portal/page/portal/portal_informatica_antivirus/HouseCall** podrás encontrar herramientas de limpieza on-line. Si tiene un pc con un sistema operativo de la familia Microsoft puede llamar al número de teléfono 902 197 198. En dicho número le ofrecerán soporte gratuito para limpiar su pc.

Enlaces de interés

Puedes recortar esta página para tenerla siempre a mano.
Como elegir una buena contraseña
https://correong.uc3m.es/usuarios/claveok.html
Instalación del antivirus en ordenadores de la universidad
http://www.uc3m.es/portal/page/portal/portal_informatica_antivirus/Officescan
Instalación del antivirus en el ordenador de casa
http://www.uc3m.es/portal/page/portal/portal_informatica_antivirus/InternetSecurity
Información sobre actualizaciones del sistema operativo:
https://asyc.uc3m.es/index.php?Id=50
Actualizaciones del Sistema Operativo Microsoft Windows y Microsoft Office:

http://update.microsoft.com

Guía de utilización del espacio de disco en red

http://sdi.uc3m.es/sistemas/servicios/NT/discos.html

Acceso al correo vía Web

https://correong.uc3m.es

Glosario de términos comunes de seguridad informática

Actualización o Parche: Archivo o conjunto de archivos, que corrige un fallo de seguridad existente en una aplicación informática.
Antivirus: Programa capaz de detectar la presencia de un virus y neutralizar sus efectos.
Botnet: Conjunto de ordenadores que han sido infectados con un programa malicioso que permite al atacante controlar dichas maquinas sin tener acceso físico a ellas y sin el conocimiento del propietario.
Cadena de mensajes: Mensaje de correo electrónico en el que se pide que dicho mensaje sea reenviado a más personas.
Compresor: Programa que estructura la información utilizando técnicas especiales para reducir el espacio necesario para almacenarla.
Cortafuegos: Programa que examina las conexiones de un ordenador y en función de su configuración rechaza las que se consideran maliciosas.
Gusano: Programa malicioso, que utiliza la red de comunicación para atacar a otros ordenadores y se copia aprovechando vulnerabilidades en el sistema operativo o en las aplicaciones instaladas.
P2P, Peer-to-Peer: Tipo de programa que actúa simultáneamente como cliente y servidor. Generalmente se utilizan para compartir ficheros.
Service Pack: Conjunto de parches agrupados para facilitar la instalación por parte del usuario.
Troyano: Programa que a primera vista realiza una función (por ejemplo visualizar una imagen), pero que además realiza otras funciones no visibles (por ejemplo instala programas maliciosos o permite acceso remoto al ordenador).
Virus: Programa malicioso, similar al gusano, pero que modifica ("infecta") un programa existente para asegurarse la transmisión de un ordenador a otro.
Vulnerabilidad: Fallo de diseño o programación en una aplicación informática que da lugar a un problema de seguridad.
Zombi: Ordenador personal que tras haber sido infectados por algún tipo de programa malicioso, pueden ser utilizados por una tercera persona para ejecutar actividades ilícitas. Este uso se produce sin la autorización o el conocimiento del usuario del equipo.