Navegación segura por Internet

Las vulnerabilidades que se detectan en los programas informáticos más utilizados (navegadores de Internet, procesadores de texto, programas de correo, etc.) suelen ser, precisamente por su gran difusión, un blanco habitual de los creadores de virus. Para evitarlo, una vez detectada una vulnerabilidad, las compañías fabricantes de software ponen rápidamente a disposición de sus clientes actualizaciones, llamadas "parches de seguridad", en Internet. Usted, como usuario, para estar protegido, necesita visitar periódicamente los sitios Web de estas compañías e instalar dichas actualizaciones.

¿Cómo me protejo?

Para ello debe utilizar el sistema de actualizaciones "Windows Update" (si su equipo tiene instalado Windows), las actualizaciones de Apple (para los equipos con MacOS), y las actualizaciones de las distintas distribuciones de Linux o Unix (en caso de usar estos sistemas operativos).
En el momento de conectarse a Internet es conveniente que, además de cuidar los aspectos básicos del ordenador, se tengan en cuenta otras medidas de prudencia para poder navegar de una forma más segura:

- Utilizar versiones actualizadas de los navegadores para que esté protegido frente a vulnerabilidades.
- Navegar por sitios Web conocidos.
- No dejar desatendidos los ordenadores mientras están conectados.
- No aceptar la ejecución de programas cuya descarga se active sin que nos lo solicite.
- No descargues/ejecutes ficheros desde sitios sospechosos porque pueden contener código potencialmente malicioso.
- No aceptar certificados de servidor de páginas Web si su navegador le indica que no lo reconoce. Pueden tratarse de páginas falsas ideadas para capturar información personal o privada.
- Analiza con un antivirus todo lo que descargas antes de ejecutarlo en tu equipo.
- Configura el nivel de seguridad de tu navegador según tus preferencias.
- Instala un cortafuegos que impida accesos no deseados a/desde Internet.
- Descarga los programas desde los sitios oficiales para evitar suplantaciones maliciosas.
- Puedes utilizar programas anti pop-up para eliminar las molestas ventanas emergentes que aparecen durante la navegación, o configurar tu navegador para evitar estas ventanas.
- Utiliza un usuario sin permisos de Administrador para navegar por Internet, así impides la instalación de programas y cambios en los valores del sistema.
- Borra las cookies, los ficheros temporales y el historial cuando utilices equipos ajenos (públicos o de otras personas) para no dejar rastro de tu navegación

Decálogo de normas de seguridad

1	No abra nunca mensajes electrónicos de origen desconocido.
2	No facilite nunca sus datos personales ni ningún tipo de códigos de acceso.
3	No abra nunca archivos de remitentes desconocidos.
4	No apunte sus contraseñas en ningún documento, ni las comparta con otros usuarios.
5	No deben utilizarse contraseñas cortas o fáciles de deducir. No utilice las mismas contraseñas en Sistemas de Alta Seguridad (Bancos, Universidad) que en Sistemas menos seguros.
6	No hay que responder a los mensajes que soliciten información de forma urgente. El STIC o su banco nunca le solicitarán ningún dato personal suyo vía electrónica.
7	Debe tener el software antivirus de la UAL instalado en su equipo. (Para PAS y PDI)
8	Es conveniente instalarse un software antiespia para evitar el Spyware.
9	Mantenga actualizado con los diferentes parches o actualizaciones de seguridadtanto el sistema operativo de su equipo como su navegador de Internet. Hagacopias de seguridad con frecuencia para evitar la pérdida de datos importantes.
10	Es altamente recomendable **mantener su equipo congelado** (salvo para realizar actualizaciones de seguridad) **mediante el software de congelación de equipos que le proporciona el STIC** (DeepFreeze). (Para PAS y PDI)

Redes sociales

¿Qué es?

Las redes sociales online son servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado.

Estos nuevos servicios se configuran como poderosos canales de comunicación e interacción, que permiten a los usuarios actuar como grupos segmentados: ocio, comunicación, profesionalización, etc.
El incorporarse a una red social implica ceder una serie de datos personales, cosa que se hace de un modo voluntario, pero no siempre consciente. Montados como estamos en la sociedad de la información, quizá lo hacemos llevados de una "ola" donde no se calibran bien las consecuencias. Es usted quien debe poner en un platillo de la balanza las ventajas que le ofrecen las redes sociales, y en el otro los problemas derivados de su uso.

¿Cómo me protejo?

El incorporarse a una red social (Facebook, Tuenti, hi5) implica ceder una serie de datos personales, cosa que se hace de un modo voluntario, pero no siempre consciente. Montados como estamos en la sociedad de la información, quizá lo hacemos llevados de una "ola" donde no se calibran bien las consecuencias. Es usted quien debe poner en un platillo de la balanza las ventajas que le ofrecen las redes sociales, y en el otro los problemas derivados de su uso.
Pautas recomendables:

- Si el sitio lo permite, es una buena idea limitar el acceso a tu perfil. No permita que personas extrañas adquieran información acerca de usted.

- Mantenga su información privada. Nunca envíe su nombre completo, Cédula, etc.

- Elije un alias que sea diferente de su nombre real. Evite el uso de cualquier información personal que ayude a identificar o localizar a alguien que estuviera en línea.

- Piénselo dos veces antes de publicar su fotografía. Las fotos pueden ser utilizadas para identificar al usuario que está en línea. También las fotos pueden ser alteradas o compartidas sin su conocimiento.

- No publique información que le haga vulnerable a un ataque físico, por ejemplo, su horario de clases o domicilio, etc.

- Si es contactado por un extraño, averigüe si alguno de sus amigos establecieron contactos con dicha persona. Si está de acuerdo en reunirse con algún contacto, que sea en un lugar público y siempre en compañía de otros amigos de confianza.

- Confíe en sus instintos. Si se siente amenazado o incómodo durante una conversación en línea, no continúe con el diálogo. Informe de cualquier comportamiento ofensivo al administrador del sitio Web de redes sociales que corresponda.

- Controle su lista de contactos. Valore con quién quiere compartirla y configure las opciones de privacidad de manera acorde. Antes de agregar a nuevas personas a la red social, piense que el usuario podrá ver tus datos personales y fotos, enviarte mensajes, etc. Asegurate de que le ofrece confianza.

Phising

¿Qué es el phishing?

Cualquier mensaje que recibes, bien por email, bien por SMS, o por cualquier otro medio, que suplanta a entidades que son de tu confianza solicitándote datos personales o contraseñas.

¿Qué entidades pueden ser suplantadas?

- Bancos
- Administraciones Públicas (Hacienda, policía,...)
- Universidades
- El Servicio de Tecnologías de la Información y las Comunicaciones (STIC) de la UAL
- etc.

¿Qué finalidad tiene el phishing?

- Fraude y robo bancario
- Envío de virus y spam
- Realización de ataques informáticos
- Robo de datos personales
- Suplantación de tu identidad

¿Cómo funciona el phishing?

- Haciéndote contestar a un email con tus datos personales, bancarios, o con tu usuario y contraseña.
- Haciendo que hagas clic en un enlace del correo electrónico que te lleva a una web similar a la de la entidad suplantada donde se te pide usuario y contraseña.
- Haciéndote enviar un SMS con tu usuario y contraseña.

¿Cómo saber que un email es phishing?

Ninguna entidad te pedirá que introduzcas tu usuario y contraseña en un email, ni en una web que se abra al hacer clic en un enlace de un email.

Otras pistas para identificar el phishing:

- Ortografía y gramática deficientes.
- Se dirigen a ti de forma genérica como "Estimado usuario" o "Estimado cliente".

No obstante, aunque en el email aparezca tu nombre y la ortografía sea buena, insistimos: nunca des tu usuaria y contraseña si te lo solicitan por email.

Consejos útiles:

Ten siempre un antivirus actualizado. http://antivirus.ual.es

• Nunca abras ningún fichero PDF, DOC o EXE contenido en un correo sospechoso.

• Consulta la web de tu entidad bancaria y obtendrás información específica sobre phishing bancario.