Universitat d'Alacant
Universidad de Alicante

BIBLIOTECA UNIVERSITARIA

Seguridad Informática

Material formativo

BUA
Biblioteca de la Universitat d' Alacant
Biblioteca de la Universidad de Alicante

CI2
COMPETENCIAS
INFORMÁTICAS E
INFORMACIONALES

ÍNDICE

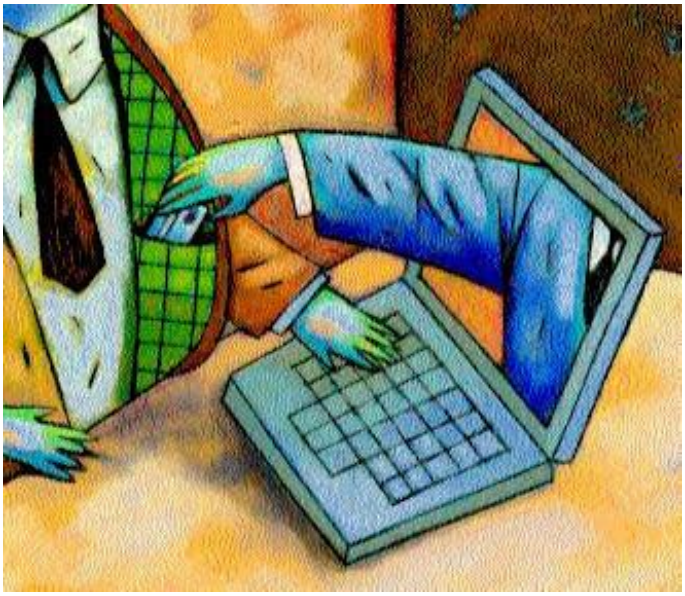
SEGURIDAD INFORMÁTICA

El uso de las tecnologías tiene una gran importancia en la actualidad; la extensión y popularización de las TIC ha supuesto, entre otras cosas, que disminuya la desconfianza a la hora de utilizar el ordenador o el móvil con conexión a internet. Pero las amenazas informáticas están siempre presentes, y has de concienciarte para tomar las mayor cantidad posible de medidas para protegerte de quienes tratan de sacar provecho de tus datos y tus posibles descuidos.

En el blog del servicio de informática de la Universidad de Alicante hay entradas acerca de la seguridad que pueden resultarte de interés como información complementaria a este tema.
Puedes consultar las entradas relacionadas con temas de seguridad en el siguiente enlace http://blogs.ua.es/si/tag/seguridad/

Protección en el correo electrónico

El correo electrónico es una de las herramientas más utilizadas y un canal muy usado por los atacantes. Es por esto que has de tratar de aumentar la seguridad en él con el objetivo de prevenirte de ataques debidos al uso descuidado del e-mail.



Spam

Se llama spam (o correo basura) al envío de mensajes masivos no deseados, normalmente de remitente desconocido

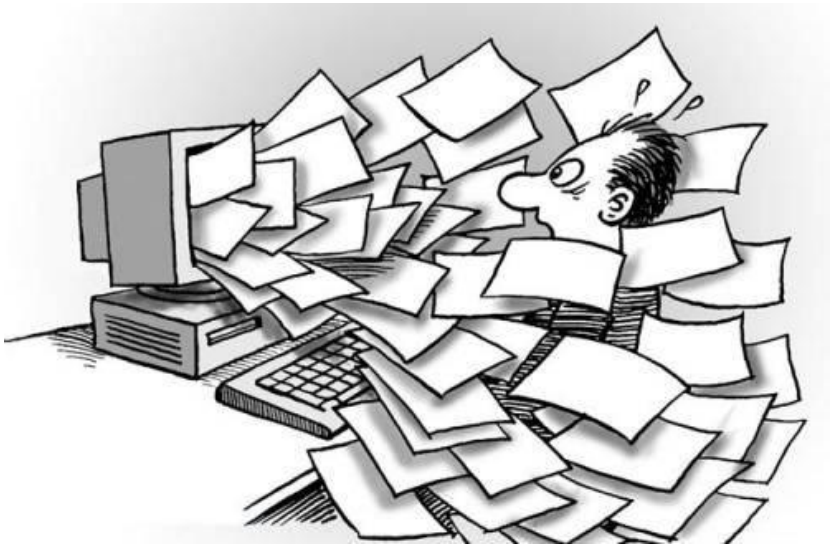
La forma más común en la que puedes advertir el spam es en el correo electrónico pero también se puede ver de manera parecida en el uso de mensajería instantánea, búsquedas en Internet, blogs, móviles, foros de Internet, etc.

El spam ha resultado siempre económico para los atacantes ya que realizarlo no supone coste más allá de la gestión de las listas de correo. Es por esto que existe una gran cantidad de servicios que tratan de publicitarse, atacantes que tratan de enviar virus y aprovechar los despistes de los usuarios, etc. que hacen uso del spam, cuyo volumen de correo no deseado es muy alto (en 2011 se estima que la cifra de correos no deseados es de alrededor de 7 billones de dólares).

Actualmente el spam es un tema de legislación en muchas jurisdicciones

Recomendaciones para evitar el envío de correo masivo y la propagación de código:

- No confíes en correos cuyo remitente no resulte conocido o pueda resultar sospechoso; menos aún en archivos adjuntos que puedan contener dichos correos.
- Presta atención a la extensión de los archivos adjuntos (indica que tipo de archivo es), ya que algunas técnicas de engaño alteran las extensiones para ocultarse.
- Evita publicar tu dirección de correo en páginas web que tengan una dudosa reputación. Utilizar otra cuenta de correo electrónico puede ser útil para proteger tu cuenta de correo principal.
- No respondas nunca a un correo no deseado. De esta manera no se pierde tiempo ni se confirma a los responsables de hacer spam que la cuenta de correo está activa.
- Utiliza los filtros anti-spam que proporcione el proveedor de correo electrónico; filtrarán los correos en otra carpeta y no te molestarán.
- Bloquea las imágenes en correos recibidos y acéptalas sólo cuando consideres que el correo no es dañino (esta técnica la suelen utilizar los proveedores de correo).



Phishing

El phishing es una forma de intentar adquirir información (como nombres de usuarios, contraseñas, detalles de tarjetas de crédito, etc.) tratando de enmascararse como una entidad de confianza utilizando una comunicación electrónica.

Su ámbito principal es **la banca,** y normalmente consiste en obtener de manera fraudulenta información confidencial e intentar realizar algún tipo de estafa relacionada con obtener dinero de los usuarios.

También se puede ver esta técnica de estafa, aunque en menor medida, mediante mensajería instantánea e incluso en llamadas telefónicas.

Ejemplos de phishing son aquellos correos que piden introducir los datos en una página para evitar que una cuenta sea cancelada, enviar datos personales por correo electrónico, confirmación de datos, etc.

Es muy importante recordar que las entidades bancarias nunca piden datos personales mediante correo electrónico u otro medio como tampoco piden a los usuarios que cambien su contraseña. Y menos alguna entidad bancaria de la que no se es cliente pida datos bancarios.

Se están realizando movimientos para crear leyes que castiguen la práctica de phishing y campañas para concienciar a los usuarios y sean advertidos de su peligro.

Algunas medidas para evitar ser víctimas del phishing son las siguientes:

- Las entidades bancarias no piden nunca datos confidenciales por correo electrónico para minimizar las posibilidades de que la técnica tenga éxito. Por tanto, nunca reveles datos confidenciales pese a que el correo tenga un aspecto que pueda parecer confiable.

- No hagas clic en enlaces que aparecen en el cuerpo del mensaje ya que pueden llevarte a una página web clonada de una página de entidad financiera y hacerte creer que te encuentras en la verdadera página web.

- Comprueba que la dirección de la página web utiliza un protocolo seguro. Para ello fíjate en que la dirección no comience por http:// sino por https://, la 's' final en http indica que es una página segura y que la información que se deposita viaja de manera cifrada.

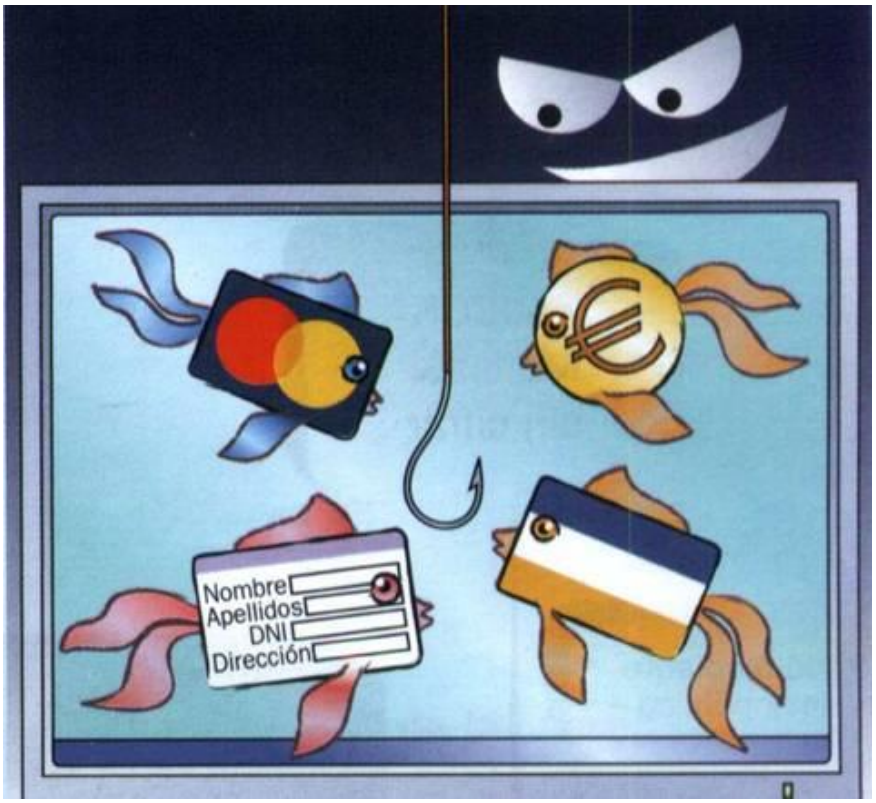
- Verifica que existe un certificado digital en la página web. El certificado se puede visualizar haciendo clic sobre el icono de candado que debe aparecer.

- Si tienes dudas de la legitimidad del correo electrónico, llama a la entidad financiera o acude a una oficina para descartar un posible engaño.

- Nunca envíes contraseñas, números de tarjeta de crédito u otra información confidencial a través de correo electrónico.

- Examina periódicamente las cuentas bancarias, con el fin de detectar posibles irregularidades relacionadas con la manipulación de la cuenta o transacciones no autorizadas.

- Denuncia casos de phishing (cuando puedas) a la entidad de confianza. De esta manera también colaboras con la seguridad en la navegación en Internet y ayudas a cortar la actividad del sitio malicioso.



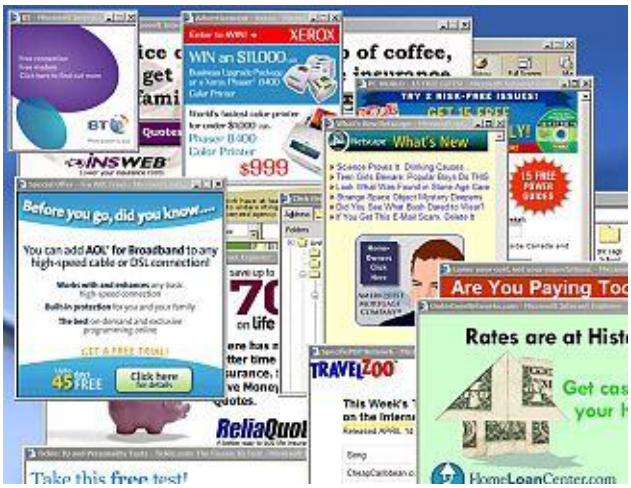
Ignora las ventanas emergentes (PopUps)

Durante la navegación, es posible que aparezcan ventanas emergentes (conocidas como *popups*).

Estas ventanas emergentes resultan pueden resultar molestas o bien atraerte para que hagas click en ellas.

Hay que tener cuidado ya que la algunas se tratan de publicidad simplemente, pero otras animan a descargar un programa (para ver un video, por ejemplo) y pueden contener algún tipo de virus.

Existen utilidades para bloquear las ventanas emergentes, tanto a nivel del propio navegador como de software externo.



Uso de contraseñas seguras y renovación periódica

La contraseña es la forma de autentificación que utilizas para probar tu identidad u obtener acceso a un recurso.

Debido a la importancia de la contraseña, existen varias **recomendaciones** aque puedes tener en cuenta a la hora de definirla:

- Crea una contraseña que utilice diferentes tipos de caracteres, como letras, números y símbolos. Te aconsejamos que tenga una longitud mínima de 8 caracteres y que no pueda ser encontrada en un diccionario.
- Utiliza una contraseña creada de manera aleatoria, aunque tengan el inconveniente de que son más difíciles de memorizar.
- Cambia las contraseñas de manera periódica.
- Te recomendamos, en la medida de lo posible, que utilices opciones de autentificación que ofrezcan las entidades bancarias u otras entidades, ya sea mediante un certificado digital o DNI electrónico, en lugar de autentificarte mediante el uso de contraseña.

Es importante que crees una contraseña difícil de averiguar para otras personas pero que sea fácil de recordar para ti.

Ajustes de privacidad en la navegación y Redes Sociales

Navegación

Recomendaciones para mejorar la seguridad en la navegación:

- Realiza la descarga de aplicaciones de seguridad únicamente desde la página web oficial, de manera que se evita la posibilidad de descargar archivos que puedan haber sido previamente manipulados con fines maliciosos.

- En caso de instalar complementos extras como barras de tareas, extensiones, protectores de pantalla, comprueba previamente su autenticidad.

- Realiza ajustes en la configuración del navegador web para poder minimizar el riesgo de ataques maliciosos.

- Instala un programa antivirus que tenga la capacidad de detectar páginas web maliciosas mientras se navega por Internet y que explora los archivos descargados; cada vez son más los antivirus que incluyen estas características.

- Utiliza un cortafuegos (firewall) que bloquee comunicaciones entrantes y salientes; de esta manera se evitará la posibilidad de que alguna aplicación maliciosa intente conectarse con el ordenador e incluso extraer datos.

- Intenta, a ser posible, no acceder a servicios bancarios u otros que utilicen datos confidenciales en ordenadores públicos (como cibers, bibliotecas, hoteles, etc.) incluso en redes Wi-Fi abiertas sin contraseña.

- En caso de navegar por Internet utilizando ordenadores públicos, te recomendamos eliminar los archivos temporales, caché, cookies, historial, contraseñas y formularios en los que hayas introducido datos para evitar que otro usuario tenga acceso a tu información privada.

Redes Sociales

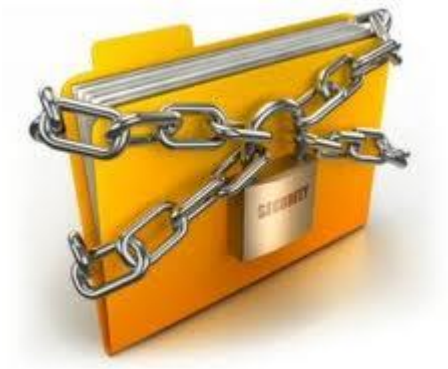
Las redes sociales actualmente son muy populares y masivamente utilizadas. Los atacantes intentan aprovecharse de aquellos usuarios que son más desprevenidos y utilizan las redes sociales con fines maliciosos. Es por esto que es necesario tomar medidas para utilizarlas de la manera más segura posible.

Algunas **recomendaciones** son las siguientes:

- Trata de no publicar información privada, ya que personas desconocidas pueden aprovechar dicha información.
- Cuida, e incluso evita, la publicación de imágenes propias y de tus familiares. Las imágenes se pueden utilizar incluso para complementar actos delictivos de cualquier ámbito.
- Configura los ajustes de privacidad del perfil de usuario; puedes configurarlos para que sea privado y sólo puedan verlo usuarios a quienes se lo permitas.
- Asegúrate de la veracidad de las personas que envían solicitudes antes de aceptarlas.
- Cambia las contraseñas de manera periódica.

Copias de seguridad

Las copias de seguridad (o *backups*) se realizan para tener almacenadas copias de archivos e incluso del estado de un ordenador para que, en caso de pérdida de información (ya sea por una catástrofe informática o por alguna causa accidental), puedas restablecer o restaurar el estado previo de tu ordenador.



Actualizar Sistema Operativo y Aplicaciones

Es recomendable que actualices el sistema operativo y las aplicaciones instaladas en tu ordenador

Los sistemas operativos y las aplicaciones presentan fallos y errores que pueden aprovechar algunos usuarios con fines maliciosos.

Las actualizaciones, además de agregar alguna nueva funcionalidad, sirven para solucionar fallos y agregar nuevas funcionalidades. Por ello estar al día con las actualizaciones de seguridad más importantes ayudará a prevenir ataques maliciosos.

Es importante que descargues actualizaciones de sitios que sean de confianza. Descargar actualizaciones de aquellos de los que se dude su reputación o sitios no oficiales aumenta el riesgo de infección.

Siempre que sea posible, te recomendamos descargar las actualizaciones a través de los mecanismos que ofrece el fabricante.

Configurar el Sistema Operativo

Es importante que realices ajustes el sistema operativo para hacerlo más seguro.

Algunos **consejos** que te ofrecemos son:

- Deshabilita las carpetas compartidas si no las utilizas. Esto evita la propagación de programas maliciosos que las aprovechen para infectar el ordenador.
- Utiliza contraseñas seguras y fáciles de recordar tanto en aplicaciones como a nivel de acceso al ordenador para evitar que puedan acceder personas no deseadas.
- Crea perfiles de usuario con privilegios restringidos, de manera que se limiten las acciones de algunos usuarios que puedan provocar un aumento de posibilidades de infección.
- Deshabilita la ejecución automática de dispositivos de almacenamiento extraíbles (como USB), ya que pueden contener aplicaciones maliciosas que se ejecuten en segundo plano, invisibles al usuario.
- Ten en cuenta que el soporte técnico en versiones antiguas de sistemas operativos y aplicaciones recibe menos atención que en el de las últimas versiones, por lo que por norma general las versiones más antiguas están más expuestas a vulnerabilidades.
- Normalmente los archivos maliciosos se esconden en el sistema como ficheros ocultos, por lo que muchas veces se encuentran configurando el sistema para que se permitan ver los archivos ocultos.
- Es posible configurar la visualización de las extensiones de archivos para que puedas identificar las extensiones de archivos que se hayan descargado y evitar ser víctima de técnicas como la doble extensión.

Para Terminar

-La seguridad informática es ante todo una cuestión de sentido común

-No caigas en la trampa cuando recibas un correo de tu entidad financiera pidiendo claves o cambios de contraseña

-Utiliza contraseñas robustas

-Antes de descargar algo de internet, asegúrate revisando el nombre del archivo que es eso lo que realmente quieres, sobre todo si se han abierto muchas ventanas emergentes.

-Utiliza antivirus actualizados y cortafuegos correctamente configurados.