Secretariado de Medios de Comunicación Social
DIÓCESIS DE CANARIAS
Las Palmas de Gran Canaria

Curso de Internet a distancia para sacerdotes, religiosos y religiosas

Material de apoyo para las teleclases - Viernes, 14 de octubre 2011
Vea los vídeos resúmenes en: **www.medioscan.es** y **www.teleiglesia.es**
contacto: info@diocesisdecanarias.org
Texo: Mario Santana Bueno

El presente material escrito es el apoyo del vídeo: **Seguridad en Internet: fraudes** que puedes ver en esta dirección: http://goo.gl/wTMQU

¿Cómo trabajar este material?
1.- Vea el vídeo que corresponde a este tema y escriba todas las dudas y cuestiones que no entienda.
2.- Vuelva a ver el video después de haber leído y entendido estos apuntes.
3.- En la teleclase exprese las dudas que aún le queden o utilice el email de contacto, el foro, el teléfono... para hacer llegar sus cuestiones al profesor.

Los fraudes en Internet

Son numerosas las personas que caen y ayudan a que se extiendan los fraudes, los virus y toda clase de problemas por Internet. En la mayoría de las ocasiones son personas que no saben el alcance de lo que hacen. Veamos los posibles fraudes y cómo se extienden por Internet.

1.- Phising

Es intentar adquirir información confidencial de manera fraudulenta. Intentan que les des tu nombre de usuario y contraseñas.
Por ejemplo: cuando recibes un correo de tu banco diciéndote que están renovando la seguridad y que necesitas que entres en una página web y escribas de nuevo tus contraseñas y nombres de usuarios...
Nunca hay que escribir en enlaces que vengan a través del correo. Lo mejor es teclear uno mismo la dirección en la barra de direcciones del navegador.

2.- Spyware

Son programas espías que vigilan todo lo que tú haces en tu ordenador: lo que escribes, tus claves, las páginas que visitas, etc. Esa información es enviada sin que tú te des cuenta a otro ordenador donde alguien vigilará todos tus movimientos.
Por ejemplo: descargas un programa y sin que tú te des cuenta te entra un programa spyware y desde ese momento todo lo que tú hagas estará siempre vigilado.

3.- Spam

Son los correos que recibimos y que no hemos solicitado, son también los llamados «correos basura».
Son los correos que te vienen sin haberlo pedido y te traen cosas como: «un niño hijo de una amiga se está muriendo...» «vas a recibir un correo que te puede borrar el disco duro...» El reenviar presentaciones de PowerPoint, etc.
Nunca hay que reenviar a nadie absolutamente nada que no te haya pedido.

¿Cómo se pueden prevenir estos fraudes?

1.- Programas antiphising
Desconfiar de cualquier página o correo que nos solicite datos confidenciales.
No dar ningún dato confidencial: DNI, nombre de usuario, contraseñas, etc. contestando o en cualquier página que no consideremos segura. Si tienes cualquier duda, te tienes que poner en contacto telefónico con tu banco o con el organismo que supuestamente te está pidiendo los datos y comprobar que efectivamente son ellos quienes los solicita. Los bancos nunca piden ningún dato confidencial por correo.

2.- Programas antispyware
Tener instalado en nuestro ordenador y siempre actualizado un buen programa antispyware.
Hay antivirus que también son capaces de detectar este tipo de programas espías.

3.- Programas antispam
Lo mejor es tener dos cuentas de correo electrónico. Una cuenta la utilizaremos para cosas menos importantes y la otra para usos más serios y oficiales.

¿Cómo proteger nuestro ordenador?

1.-Protegernos de los virus
Los virus informáticos son pequeños programas que dan órdenes a nuestro ordenador y van poco a poco estropeando nuestra máquina.
Algunas señales de que nuestro ordenador está infectado por algún virus son:
- El ordenador se vuelve más lento
- Empiezan a atascarse los programas que utilizábamos sin problemas
- El ordenador se queda atascado y no responde ni el teclado ni el ratón

Los virus para poder entrar en nuestro ordenador necesitan de otros medios como por ejemplo el correo. La mayoría de los virus entran a nuestra máquina por el correo electrónico.

2.- Protegernos de los «gusanos»
Estos programas no necesitan de otros medios para entrar en el ordenador. Se descargan sin que nos demos cuenta simplemente visitando una web, etc.

3.- Protegernos de los «troyanos»
Son programas aparentemente normales pero que cuando los descargamos en nuestro ordenador hace que otro programa malo entre en nuestra máquina.
Los troyanos son programas muy difíciles de eliminar y en muchas ocasiones hay que «formatear» (borrar) todo el disco duro y tener que volver a instalar todo lo que teníamos previamente instalado.

Los remedios para todos estos tipos de virus es tener un buen antivirus, los hay gratuitos y de pago **siempre actualizados**.

Orientaciones para los hijos:
- Hay programas de «control parental»
- Hay que utilizar filtros de contenidos
- Hay que asegurarse que el navegador tiene activados los filtros de contenidos.

Buscar en Internet en Google

El presente material escrito es el apoyo del vídeo: **Buscar en Internet en Google**
que puedes ver en esta dirección: http://goo.gl/AfcZg

¿Cómo trabajar este material?
1.- Vea el vídeo que corresponde a este tema y escriba todas las dudas y cuestiones que no entienda.
2.- Vuelva a ver el video después de haber leído y entendido estos apuntes.
3.- En la teleclase exprese las dudas que aún le queden o utilice el email de contacto, el foro, el teléfono... para hacer llegar sus cuestiones al profesor.

Ya hemos comentado que en Internet existen miles de millones de páginas es por ello que tenemos que buscar la manera de encontrar con facilidad lo que vamos buscando. Para buscar algo tenemos los buscadores que son programas que nos ayudan a encontrar rápidamente cualquier cosa que busquemos en la red.

En la actualidad el mejor buscador es GOOGLE. Puedes descargarlo en www.google.es y ponerlo como página de inicio.

A través de Google podemos encontrar con mucha facilidad textos, libros, imáganes, vídeos, etc.

Correos electrónicos: email

El presente material escrito es el apoyo del vídeo: **Correos electrónicos: email**
que puedes ver en esta dirección: http://goo.gl/dl34D

¿Cómo trabajar este material?
1.- Vea el vídeo que corresponde a este tema y escriba todas las dudas y cuestiones que no entienda.
2.- Vuelva a ver el video después de haber leído y entendido estos apuntes.
3.- En la teleclase exprese las dudas que aún le queden o utilice el email de contacto, el foro, el teléfono... para hacer llegar sus cuestiones al profesor.

- Para ver el correo en nuestro ordenador
Para poder ver el correo electrónico necesitamos descargar en nuestro ordenador un programa de correos como puede ser Outlook, Windows Live Mail, etc.
Con el programa en nuestro ordenador descargamos los correos en nuestra máquina.

- También podemos ver el correo en línea, sin descargarlo en nuestro ordenador, es lo que se llama WEBMAIL
Hay programas de correos en línea, esto es, programas que no necesitan ser descargados en nuestro ordenador.
Normalmente, los webmail son gratuitos.
Hay tres direcciones de correos que son las más utilizadas:

- Gmail
Es un servicio de correo electrónico.
Dispone de muchísimo espacio gratuito en el que puedes recibir tus correos.
Puedes mandar documentos de hasta 10 Megas (MB) cuando lo normal en un correo es hasta 2 MB.
Puedes hacer una lista de tus contactos y enviarles el mismo correo a todos juntos.

- Yahoo Mail
También lo podemos ver en webmail.

- Hotmail (Windows Live Hotmail)
También lo podemos ver en webmail.

¿Qué ocurre si tengo una cuenta gratuita de correo y no la utilizo?
Si no utilizas tu correo la propia empresa la borrará a los pocos meses y también borrará todos los correos que hayas recibido.
Las cuentas inactivas se borran en:
- Gmail a los 9 meses de inactividad.
- Yahoo a los 4 meses de inactividad.
- Hotmail a los 3 meses de inactividad.