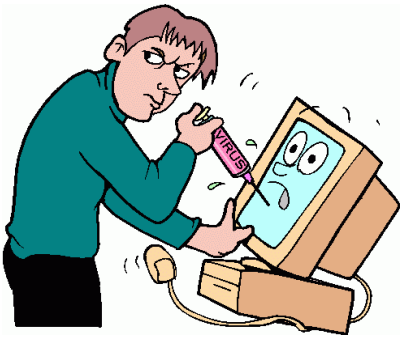
SEGURIDAD PARA LA COMPUTADORA



Hoy en día hay muchas amenazas tanto en el mundo virtual como en el mundo real.

Sabemos más o menos cómo protegernos a nosotros mismos y a nuestras posesiones, porque muchas veces podemos ver las amenazas.

Por experiencia sabemos cerrar la puerta de nuestra casa e inclusive poner barrotes en las ventanas.

Sabemos que no debemos dejar las cosas de valor a la vista, ser discretos con el dinero, etc.

Estamos preocupados pensando lo que nos puede pasar en el mundo virtual (con toda nuestra información), pero tristemente, muchos de nosotros no sabemos cómo mejorar nuestra seguridad virtual.

Es importante que leas este material y que prestes atención. Tu reacción frente a la seguridad informática puede afectar a mucha gente a tu alrededor. Pensar que a ti no te va a pasar nada puede ser un gran error.

Para TODOS los misioneros

Riesgos Potenciales con tu computadora y lo que puedes hacer

1. Pérdida y robo de computadoras e información. (Es recomendable tener una copia de seguridad/backup)
2. Intercepción de las comunicaciones en toda la red de internet. (Ten cuidado siempre en lo que dices y recibes). O que algún hacker ingrese a tu información.
3. Virus y malware. (Tener un buen antivirus actualizado y una copia de seguridad de tu información)

Copia De Seguridad

Debes hacer una copia de seguridad cada semana (o más frecuentemente si estás haciendo un trabajo que no te gustaría perder). La mejor manera de hacer una copia de seguridad es en un disco duro externo, luego guarda el disco duro en otro lugar o en otra oficina. Hay un programa gratuito que está disponible para colgar tu copia en internet: Cobian Backup: http://www.cobian.se/

Contraseñas Seguras

Las contraseñas seguras consisten en por lo menos 8 caracteres e incluyen tanto mayúsculas y minúsculas como números. Evita usar contraseñas que son muy fáciles de adivinar.

Usa diferentes contraseñas para cosas diferentes. Tu claves financieras deben ser protegidas con una contraseña que no la uses en otro sitio.

Seguridad en el Correo Electrónico

- No abras un documento adjunto de un correo cuando no conoces a la persona que te lo envió.
- No abras un documento adjunto de un correo si el título es cuestionable o inesperado.
- Nunca hagas clic en un link de una página web desde un correo electrónico. En vez de eso, manualmente escribe el link de la pagina web o corta y pega el link en la barra de dirección de la web (es más seguro que hacer clic en el link) ¿Por qué? Las personas que mandan correos basuras (spammers) a menudo ponen enlaces en los correos que pueden ir a un lugar (una página que tiene buena seguridad) pero en realidad van a otra página, que podría infectar tu computadora con spyware (software que se instala en tu computadora y transmite información sobre tu computadora) o con una falsa página y tratar de obtener información tuya. A esto se le llama “Phishing”.
- Borra todas las cadenas, spam, mensajes de “advertencia” o de “rumor” sobre virus.
- Nunca mandes contraseñas, números de cuentas o cualquier información privada o personal en un correo. Si lo debe hacer, manda por partes la información y en diferentes correos.
- Mantén e imprime la base de datos de tus correos así como cualquier información que bajo ningún motivo quisieras perder.

SKYPE ES SEGURO hasta cierto punto

Skype es el único programa de mensajería instantánea que actualmente ofrece conexiones seguras y animamos a los miembros del equipo a usarlo con la misma confiabilidad de siempre. Las conversaciones telefónicas del “Skype out” para teléfonos fijos y celulares no son seguras, por favor sigue estas medidas de seguridad.

Para misioneros en países de acceso restringido

Nota: Estas pautas no sólo son para tu protección, sino también para la protección de toda la familia del equipo misionero en situaciones inseguras. No seas el punto débil del equipo.

*****“No dejes que unan los puntos de la INFO”*****

Cuando trabajas en un país de acceso restringido, en ninguna situación o comunicación debes unir más de uno de los tres puntos mencionados:

IN= Información (nombres, correos electrónicos, números telefónicos, etc.)

F= Función (nombre del lugar, país, ciudad, etc.)

O= Organización (nombre de la organización o agencia)

Además para que nunca unan la INFO, sugerimos que consideres desarrollar y utilizar constantemente **seudónimos** para la información de la INFO, por ejemplo puede utilizar:

"Mi Jefe" en vez de decir Dios, "la empresa" en vez de decir iglesia, "nuevos empleados" en vez de decir nuevos creyentes, etc.

Suposiciones:

1. No podemos controlar ni confiar en las acciones de otros, por eso, usamos un lenguaje diferente o códigos de palabras para que nos escriban. (Sin embargo, PODEMOS controlar nuestras propias comunicaciones).
2. Todas las comunicaciones están potencialmente abiertas.
3. Todas las computadoras están en peligro.

Recomendaciones de Seguridad

Recordar constantemente a las personas que reciben tus cartas y correos que tomen medidas de seguridad al abrir tus documentos. Aquí hay un ejemplo que te puede ayudar:

***TODA LA INFORMACIÓN DE ESTA CARTA ES CONFIDENCIAL.

NO PUEDE SER COMPARTIDA, NI PUBLICADA, COMENTADA A OTROS, NI REENVIADA A NADIE SIN AUTORIZACION.

No seas el eslabón perdido de la cadena.

¿Quién no tiene un drive USB?

Todos deben asegurarlo con una clave, escanearlo con el antivirus y el antimalware cada vez que puedas.