TIPS DE SEGURIDAD INFORMÁTICA

En la actualidad hay una extensa cantidad de estafadores informáticos, por lo cual, le recomendamos poner en práctica los siguientes tips de seguridad para el buen uso de Internet en su hogar u empresa:

Sobre privacidad:

- Nunca divulgue sus nombres de usuario y contraseñas. Sus nombres de usuario y contraseña son únicos y sin ellos, nadie puede tener acceso a sus cuentas o servicios.

- Cambie periódicamente sus contraseñas, más aún si sospecha que alguien extraño las conoce. No utilizar claves estándares para el acceso a las cuentas de usuarios. Se recomienda usar un password que contenga al menos 3 referencias de los siguientes caracteres: números, letras mayúsculas, letras minúsculas, símbolos; además que tenga mínimo 8 caracteres de longitud.

- Evite usar software u otras opciones, con la finalidad de que no tenga que escribir su contraseña la siguiente vez que tenga acceso al mismo sitio desde la misma computadora. Este tipo de software les podría dar a otros usuarios acceso a sus cuentas o servicios si llegaran a utilizar su computadora.

- No deje su computadora desatendida mientras tenga acceso a servicios bancarios en línea.

- Siempre salga de los Servicios en Línea cuando haya terminado de realizar sus operaciones.

- Borre los archivos temporales de Internet siempre que salga de los Servicios en Línea. Cada vez que accede a Internet, su navegador guarda automáticamente una copia de las páginas de Internet que usted ha visitado.

- Nunca envíe información confidencial (tal como números de cuenta de cualquier tipo, usuario, contraseña, etc.) por medio de correo electrónico.

- Revise sus estados de cuenta en forma regular y reporte a su banco inmediatamente cualquier discrepancia.

- En caso de extraviar sus tarjetas electrónicas, comuníquese inmediatamente con su banco.

- No utilizar computadoras de uso compartido para realizar operaciones bancarias, ya que no ofrecen las condiciones mínimas de seguridad, y estafadores informáticos pueden fácilmente capturar los datos que usted ingrese.

Para proteger la información que guarda en su computadora:

- **Utilice un software de firewall.** Antes de conectar su computadora a Internet, active el firewall de su sistema operativo preferido, instalado en su computador.

- Actualice periódicamente el sistema operativo y los programas de su computadora.

- **Instale un antivirus.** Instale y mantenga actualizado un antivirus de marca reconocida. El software antivirus es un programa que puede venir preinstalado en su computadora o que necesita instalar, para ayudarle a proteger su computadora contra virus, "Caballos de Troya" y otros intrusos no deseados.

- **Deshabilite la compartición de archivos.** La compartición o intercambio de archivos es una facilidad que le da su sistema operativo, que permite a otras computadoras tener acceso a su computadora personal, aún por medio de Internet. Para hacer esto, seleccione Inicio, posteriormente Configuración, Conexiones de red y acceso telefónico. Con el botón de la derecha, haga clic en Conexión de área local y posteriormente en Propiedades. En la pantalla que aparece, asegúrese que la casilla Compartir impresoras y archivos para redes Microsoft esté desactivada. Finalmente haga clic en Aceptar.

Sobre la suplantación de identidad en Internet (phishing)

- Si recibe un correo electrónico o una ventana de mensaje emergente solicitándole información personal o financiera, no responda, ni tampoco haga clic en el enlace o vínculo del mensaje.

- No envíe información sensible a través de Internet. Antes verifique si el sitio Web es seguro.

- Nunca responda a solicitudes de información personal a través de correo electrónico. Si tiene alguna duda, póngase en contacto con la empresa que supuestamente le ha enviado el mensaje.

- Ponga atención en el URL del sitio Web que visita. Los sitios Web maliciosos pueden parecer idénticos a los sitios legítimos, pero el URL puede tener variaciones o un nombre de dominio diferente.

- Asegúrese que el sitio Web utiliza cifrado (https://....).

- Instale una barra antiphishing en su navegador, conocidas también como anti-phishing blocker. Estas herramientas están disponibles para los principales navegadores de internet.

CONSEJOS DE SEGURIDAD DE INTERNET PARA NIÑOS Y ADOLESCENTES

- **Información personal.** No proporcionen información personal sin el permiso de sus padres. Lo anterior significa que no deben compartir sus apellidos, direcciones particulares, nombres de escuela o números de teléfono. Recuerden, el hecho de una persona les pida información sobre ustedes no significa que tienen la obligación de dársela.

- **Nombre de pantalla.** Cuando creen su nombre de pantalla, no incluyan ninguna información personal, tal como apellidos o fechas de nacimiento.

- **Contraseñas.** No compartan sus contraseñas con nadie, a excepción de sus padres. Cuando utilicen una computadora pública, asegúrense de cerrar las sesiones de las cuentas a las que accedieron antes de dejar la terminal.

- **Fotografías.** No publiquen fotografías o videos en Internet sin permiso de sus padres.

- **Amigos de Internet.** No acepten encontrarse con amigos de Internet a menos que cuenten con el permiso de sus padres. Desafortunadamente, muchas veces las personas se hacen pasar por otras personas. Recuerden que no todo lo que leen en Internet es verdad.

- **Propagandas en Internet.** No compren nada en Internet sin hablar antes con sus padres. Algunas propagandas pueden engañarlos ofreciéndoles cosas gratis o diciéndoles que han ganado algo como una manera de obtener su información personal.

- **Descargas.** Hablen con sus padres antes de abrir un documento adjunto a un mensaje de correo electrónico o descargar software. Los documentos adjuntos muchas veces incluyen virus. Nunca abran un documento adjunto de alguien a quien no conocen.

- **Intimidación.** No envíen ni respondan a mensajes crueles o insultantes. Informen a sus padres si reciben uno. Si sucede algo en Internet que los hace sentir incómodos, hablen con sus padres o un profesor en la escuela.

- **Redes sociales.** Muchos sitios web de redes sociales (como Facebook, Twitter, etc.) y sitios web que hospedan a blogs tienen un requerimiento de edad mínima para registrarse. Dichos requerimientos existen para proteger a los usuarios.

- **Investigación.** Hablen con su profesor o padre sobre los sitios web seguros y exactos para la investigación. La biblioteca pública ofrece numerosos recursos. Si utilizan información de Internet en un proyecto escolar, asegúrense de explicar dónde obtuvieron la información.

CONCEPTOS ÚTILES

Virus: Programas malignos diseñados para alterar el normal funcionamiento o robar información del dispositivo final infectado. Los medios con los que usualmente se propagan son: Pendrive, correo electrónico o redes para compartir archivos.

Phishing: Técnica de engaño que consiste en el envío de e-mails falsos para robar información.

Computadoras de Uso Compartido: Son aquellas ubicadas en cybers, hoteles, aeropuertos y demás lugares públicos.

Firewall: Es un hardware o software que le ayuda a prevenir que intrusos o virus ingresen a su máquina.

Internet: Es la "red de redes", es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí.

Facebook: Es una herramienta social que conecta a la gente con sus amigos y otras personas que trabajan, estudian y viven en su entorno.

Twitter: Es una aplicación web gratuita de microblogging que reúne las ventajas de los blogs, las redes sociales y la mensajería instantánea.

URL: Es la ruta que se encuentra en la caja de texto ubicada en la barra de navegación del navegador, sirve para ubicar de manera precisa en un servidor, cualquier recurso: una imagen, un video o una página web.

Compartición: Expresión que define el número de usuarios asignados a un determinado canal compartido.

Usuarios: Número de individuos que acceden al servicio.

Ancho de banda: Es la medida de datos y recursos de comunicación disponible o consumida expresados en bits/s o múltiplos de él (Mbits/s, Gbits/s, Terabits/s, etc).