RMTELCOM
RM TELECOMUNICACIONES MOMPOS S.A.S
Te conecta con el mundo

Consejos sobre seguridad informática

Relacionados con su equipo informático

- **Actualice regularmente su sistema operativo** y el software instalado en su equipo, poniendo especial atención a las actualizaciones de su navegador web. A veces los sistemas operativos presentan fallos que pueden ser aprovechados por delincuentes informáticos. Frecuentemente aparecen actualizaciones que solucionan dichos fallos. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, le ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.

- **Instale un Antivirus** y actualícelo con frecuencia. Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.

- **Instale un Firewall** o Cortafuegos con el fin de restringir accesos no autorizados de Internet.

- Es recomendable tener instalado en su equipo algún tipo de **software anti-spyware**, para evitar que se introduzcan en su equipo programas espías destinados a recopilar información confidencial sobre el usuario.

Relacionados con la navegación en internet y la utilización del correo electrónico

1. **Utilice contraseñas seguras**, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente además que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos.

2. **Navegue por páginas web seguras y de confianza**. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet. En estos casos reconocerá como páginas seguras aquellas que cumplan dos requisitos:
    - Deben empezar por https:// en lugar de http.
    - En la barra del navegador debe aparecer el icono del candado cerrado. A través de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página.

3. **Sea cuidadoso al utilizar programas de acceso remoto**. A través de internet y mediante estos programas, es posible acceder a un ordenador desde otro situado a kilómetros de distancia. Aunque esto supone una gran ventaja, puede poner en peligro la seguridad de su sistema.

4. **Ponga especial atención en el tratamiento de su correo electrónico**, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc. Por ello le recomendamos que:
    - No abra mensajes de correo de remitentes desconocidos.
    - Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
    - No propague aquellos mensajes de correo con contenido dudoso y que le piden ser reenviados a todos sus contactos. Este tipo de mensajes, conocidos como hoaxes, pretenden avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc. Estas cadenas de e-mails se suelen crear con el objetivo de captar las direcciones de correo de usuarios a los que posteriormente se les enviarán mensajes con virus, phishing o todo tipo de spam.
    - Utilice algún tipo de software Anti-Spam para proteger su cuenta de correo de mensajes no deseados.

En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible.