Uso del Correo Electrónico

A continuación varios consejos que le ayudarán a evitar virus informáticos:

1- **Proteja su equipo con programas antivirus:** Recomendamos un programa antivirus actualizado (antivirus.frcuba.cu), que ayude a proteger su equipo de virus y troyanos. Los programas de este tipo escanean el ordenador, manual o automáticamente, e informan de cualquier problema que se produzca. Existen tres tipos diferentes de análisis: el análisis en tiempo real, el análisis manual y el análisis en línea.

Escáner en tiempo real: Se ejecuta en segundo plano como un servicio del sistema y controla todos los archivos, aplicaciones y servicios. Si la protección antivirus ha encontrado algo sospechoso, normalmente se pregunta primero al usuario cómo debería ser el siguiente procedimiento, para que el usuario tenga el poder de decisión.

Analizadores de virus en línea: Los analizadores en línea comprueban los archivos o todo el equipo a través de Internet. Esto funciona sin instalación y normalmente sin registro. Sin embargo, el software no protege el equipo de nuevas infecciones, sino que sólo detecta las amenazas existentes durante el análisis.

Escáneres manuales: La característica especial es la configuración manual del escáner. El usuario debe iniciar cada escaneo por sí mismo. Si se encuentra un programa peligroso, el programa muestra posibles soluciones para neutralizarlo.
Debe determinarse de antemano que el escáner antivirus se ejecute de forma permanente para que los programas maliciosos puedan detectarse en una fase temprana. También se recomiendan los llamados escaneos completos, que escanean completamente el ordenador.

Los programas antivirus deberían ser obligatorios para todos, ya que esto aumenta drásticamente la seguridad general del ordenador.

2 - **¡Atención a fuentes de datos desconocidas!** - Las fuentes de datos desconocidas incluyen, por ejemplo, memorias USB o discos duros externos. Estos parecen ser seguros a primera vista, pero pueden contener malware o archivos contaminados con virus. Conectar un dispositivo USB puede ser suficiente para infectar el equipo sin ningún signo.

Sugerencia: No conecte ningún dispositivo extraño a su propio equipo, ya que nunca se sabe lo que puede haber en él. También uno no debería prestar sus propios dispositivos a extraños, ya que una transmisión de virus es posible.

3 - **Precaución con archivos desconocidos en Internet** - Como medio de comunicación más importante, el correo electrónico presenta un riesgo especialmente elevado en lo que se refiere a la suplantación de identidad (phishing): por lo tanto, debería comprobar los mensajes de correo electrónico con archivos adjuntos en particular, ya que el malware podría esconderse ahí. ¡No debes abrir archivos adjuntos de correo electrónico de remitentes desconocidos! Puedes utilizar un programa antivirus para comprobar los archivos adjuntos del correo electrónico, de modo que esté seguro. Además, puede optar por varios tipos de cifrado de correo electrónico para evitar posibles ataques de virus por parte de malware. Para protegerse eficazmente, los

mensajes de correo electrónico deben encriptar los registros de correspondencia almacenados y la conexión con su proveedor de correo electrónico.

4 - Cuidado al instalar un software nuevo - Es muy probable que todos los que navegan por Internet ya hayan instalado algún software. También en este caso debe comprobarse de antemano si la fuente tiene buena reputación y en qué medida. Porque al descargar software en su ordenador, el malware puede ser un compañero no deseado.

5- Copias de seguridad regulares - A pesar de todas las precauciones de seguridad, es posible que el equipo se haya infectado con troyanos u otros programas malintencionados. Como resultado, ya no se puede acceder a los datos en el peor de los casos. En resumen: Todo se borra o ya no se puede recuperar. Por lo tanto, recomendamos realizar copias de seguridad periódicas en medios de almacenamiento externos para que las fotos, los vídeos y los documentos se puedan almacenar independientemente del ordenador.

6- Seguridad del Navegador: ¡Utilice actualizaciones! - Los navegadores obsoletos son el objetivo número uno para los ataques de hackers maliciosos. También puede utilizar diferentes navegadores para diferentes servicios. Esto tiene la ventaja de que todos los plug-in, extensiones y cookies pueden ser desactivados en un navegador, ya que son particularmente vulnerables. Como resultado, ya no podrá realizar operaciones bancarias o compras en línea ahí, pero estará más seguro en sitios web supuestamente inseguros.
Además, debería borrar regularmente sus pistas en Internet, como por ejemplo su caché. Esto los hace más difíciles de detectar para los atacantes cibernéticos.

7 - Aprende a identificar claramente los correos electrónicos sospechosos de ser Phishing - Existen algunos aspectos que inequívocamente, identifican este tipo de ataques a través de correo electrónico:
- Utilizan nombres y adoptan la imagen de empresas reales.
- Llevan como remitente el nombre de la empresa o el de un empleado real de la empresa.
- Incluyen webs que visualmente son iguales a las de empresas reales.
- Como gancho utilizan regalos o la perdida de la propia cuenta existente.

8 **- Verifica la fuente de información de tus correos entrantes -** La FRC nunca te pedirá que le envíes tus claves o datos personales por correo. Nunca respondas a este tipo de preguntas y si tienes una mínima duda, llama directamente al Nodo Central para aclararlo.

9 - Nunca entres en la web pulsando en links incluidos en correos electrónicos - No hagas clic en los hipervínculos o enlaces que te adjunten en el correo, ya que de forma oculta te podrían dirigir a una web fraudulenta.
Teclea directamente la dirección web en tu navegador o utiliza marcadores/favoritos si quieres ir más rápido.

Gracias por la atención,

William Ortega Alegría (Seguridad Informática)