

¿Sabes que es el Malware?



¿HAS ESCUCHADO EL TÉRMINO MALWARE?

Te comento que un Malware, es un término utilizado para referirse a cualquier tipo de “malicious software” (software malicioso) diseñado para infiltrarse en tu dispositivo. Y sí, es una amenaza que puede involucrar a toda la información que haya en tu dispositivo e incluso pudiera extenderse a la red a la cual estás conectado. Es decir, el impacto, dependerá del objetivo para el cual ha sido programado este software.

¿EXISTEN VARIOS TIPOS DE MALWARE?

Efectivamente, te los comento de manera rápida y simple:

- ✓ Los Troyanos, se filtran en el dispositivo como un software válido e incluso descargar malware adicionales. ¡Gran dolor de cabeza y sin control alguno!
- ✓ Los Spyware, reúne la información de tu dispositivo o de la red para ser enviada al ciberdelincuente. ¡Podrían utilizar estos datos para realizar otros tipos de delitos!
- ✓ Gusanos, infectan un dispositivo para luego que este se replique a otros equipos. ¡Sería como una infección masiva, pero en línea!
- ✓ Adware, somete a la víctima a publicidad no deseada. Sería como: ¡Abrir y cerrar ventanas no deseadas!
- ✓ Ransomware, deniega el acceso del usuario a su dispositivo teniendo que pagar un rescate para su liberación. ¡Imagínate, sería como un secuestro virtual, pero de tu información!

¿CÓMO USUARIO, SOY RESPONSABLE?

Tu responsabilidad es comprometerte a aprender y estar alerta, ya que la mayoría de las infecciones se producen cuando el usuario descarga o instala “involuntariamente” el malware. Debes saber que las acciones que conllevan a esta infección son: Al hacer clic en el vínculo de un correo electrónico desconocido y/o visitar sitios web maliciosos los cuales no hayas verificado su autenticidad. Independientemente, de lo anterior y desde donde lo hayas ejecutado. Es decir, desde tu computador o dispositivo móvil, ya que actualmente, estos softwares maliciosos pudiesen llegar hasta en mensajes de textos.

¿CÓMO SABER SI MI DISPOSITIVO ESTÁ INFECTADO?

- ✓ El dispositivo empieza a funcionar más lento de lo normal.
- ✓ Nota que le falta espacio de almacenamiento.
- ✓ En su dispositivo aparecen ventanas emergentes y programas no deseados.
- ✓ Para el caso de que sea del tipo del Ransomware, debes saber que este anuncia su presencia de inmediato ya que exige un pago a cambio de devolver el acceso a sus dispositivos o a la información que tenga cifrada, esto lo hace diferente de los otros malwares que operan de manera más invisibles.

Tips para prevenir los Malwares en nuestros sistemas

- Mantén actualizado tu dispositivo a través del sistema operativo y sus aplicaciones.
- Deja respaldo constante de la información que tienes en tu dispositivo. (Disco duro externo o en la nube o Cloud).
- Evita hacer clic en un enlace de ventana emergente; solo presiona “X” y sal del sitio que la haya generado.
- Instala o mantén en tu equipo solo las aplicaciones que utilizarás comúnmente. Si tienes aplicaciones que ya no usas, procura desinstalarlas ya que genera que el dispositivo funcione más lento.
- En Internet, no hagas clic en enlaces desconocidos, ya sean provenientes de un correo electrónico, página web poco confiable o red social.
- Presta atención a los correos electrónicos que soliciten tus datos personales o tengan adjuntos archivos desconocidos. Evita responderlos o simplemente eliminalos.
- Navega por sitios web confiables, preferentemente, si deseas hacer alguna compra o transacción, asegúrate que mantengan certificado SSL.
- Y por último, mantén tus dispositivos a salvo mediante la protección de herramientas de seguridad, como por ejemplo: antivirus, antimalware y otros.

El Grupo Zurich, está comprometido con la Seguridad de la información y es por ello, que extendemos la conciencia y la Cultura Ciber hasta tu hogar.

Recuerda: “Que las técnicas de Ingeniería social utilizadas para generar ciberdelitos se han valido incluso del hackeo emocional de los usuarios. Es por ello, que debes estar preparado y alerta”