DELL Technologies

Hoja de referencia de ciberseguridad

En un mundo cada vez más virtual, la ciberdelincuencia aumenta a un ritmo alarmante, y esto no es ninguna sorpresa. De hecho, **la ciberdelincuencia generó unos 6 billones de dólares en 2021**, por lo que se ha convertido en la tercera fuerza económica mundial después de EE. UU. y China*. Los atacantes son cada vez más inteligentes y sofisticados, pero es fácil protegernos mientras navegamos por Internet si estamos al tanto de las amenazas más recientes y tomamos las medidas de protección correspondientes. **Estas son algunas de las amenazas que intentan impedir a toda costa los expertos en ciberseguridad de Dell. Verá también algunos consejos para proteger su lugar de trabajo y su hogar.**

Descargas ocultas

SUGERENCIA: *Mantenga actualizados los navegadores y plugins*

Su conexión no es segura.

Cuando se encuentra con un sitio web poco seguro o en riesgo, hay agentes maliciosos que pueden obtener acceso a su sistema.

Cómo detectarlo:

Tiene archivos o conexiones de red nuevos en el sistema que usted no ha añadido

Tiene solicitudes de información sobre la configuración que no ha pedido

Hardware poco seguro

SUGERENCIA: *Realice compras solo en distribuidores autorizados*

¿Sabía que se puede hackear una impresora?

Los atacantes insertan las vulnerabilidades directamente en el hardware y los accesorios.

Cómo detectarlo:

Ofertas demasiado buenas para ser ciertas

Ingeniería social

SUGERENCIA: *Los organismos gubernamentales (IRS, etc.) se ponen en contacto primero a través de USPS.*

¿Me están suplantando?

Los estafadores manipulan a sus víctimas fingiendo ser una persona jurídica o cualquier otro organismo con autoridad a fin de robar **información financiera o personal** confidencial. Este suceso recibe el nombre de "suplantación de identidad". El código malicioso se envía mediante enlaces o archivos adjuntos en correos electrónicos, mensajes directos y mensajes de texto.

Cómo detectarlo:

Tiene correos electrónicos o mensajes no solicitados que le piden información personal con instrucciones para abrir enlaces o archivos adjuntos

La dirección de correo electrónico, la forma de expresarse o la ortografía del remitente son sospechosas

Ataques de malware mediante USB

SUGERENCIA: *Tenga cuidado con las unidades USB, aunque sean de sus amigos*

Mmm... ¿Pasa algo si conecto esta unidad USB?

El criminal utiliza dispositivos de almacenamiento extraíbles, como unidades USB, discos duros portátiles, teléfonos inteligentes, reproductores de música, tarjetas SD y medios ópticos (CD, DVD, Blu-ray, etc.) para infectar un equipo o una red.

Cómo detectarlo:

Acceso inesperado a archivos o creación de nuevos archivos en el dispositivo

Relación de confianza

SUGERENCIA: *Use contraseñas seguras y únicas*

¿Quién es usted?

Los hackers atacan a un tercero de confianza, como la consulta de un médico, y usan su reputación para aprovecharse de los pacientes.

Cómo detectarlo:

Comportamiento inesperado de inicio de sesión

Cómo garantizar la ciberseguridad:

LO QUE DEBE HACER

Use autenticación multifactorial y contraseñas seguras y únicas en todas las cuentas.

Cualquier dispositivo con acceso a Internet puede sufrir un ataque. Mantenga el software siempre actualizado.

Esté alerta y sea escéptico. Aprenda a reconocer tácticas de estafa.

Sea honesto. Informe de los ataques al equipo de tecnología informática y avise a sus compañeros, familiares y amigos.

LO QUE NO DEBE HACER

No sea perezoso. Siga siempre todos los protocolos de seguridad.

No haga clic en enlaces insertados en correos electrónicos o mensajes directos que no haya solicitado.

No ignore las advertencias del navegador, por ejemplo: "Su conexión no es segura" o "Su conexión no es privada".

SUGERENCIA: *Si necesita más información, visite:* Dell.com/Endpoint-Security

DELL Technologies

*Cybersecurity Ventures; 2022 Cybersecurity Almanac; 100 Facts, Figures, Predictions and Statistics