

CÓMO PERMANECER EN LA ZONA DE LA SEGURIDAD CIBERNÉTICA

CÓMO USTED PUEDE PROTEGER A SUS PACIENTES DE LAS CINCO PRINCIPALES AMENAZAS CIBERNÉTICAS



Ingeniería social



Ransomware



Pérdida por robo de equipos o datos



Pérdida de datos internos de forma accidental o maliciosa



Seguridad de dispositivos médicos conectados a la red

Ingeniería social

- ¡No caiga en la trampa!
- ¿Coincide la URL con el remitente?
Por ejemplo, si el remitente es Jackson Equipment, los enlaces deben ir a www.jacksonequip.com, no a www.knjdlkajfkje.net.
- ¿El mensaje indica que hay que tomar algún tipo de acción rápida, como “responder inmediatamente” o “se requiere una acción inmediata”?

Ransomware

- Utilice la autenticación multifactor (multi-factor authentication, MFA) si su organización la admite. Esto añadirá otra capa de protección para sus datos y sistemas.
- Actualice su software y contraseñas cuando su organización le notifique que lo haga.
- Denuncie cualquier cosa sospechosa. Siempre es mejor estar seguro y notificar a las autoridades de inmediato.

Pérdida por robo de equipos o datos

- Conozca la política de su organización con respecto a llevarse el equipo a casa o de un sitio a otro.
- Utilice una red wifi o VPN segura siempre que acceda a datos de la organización o comparta información confidencial del paciente.
- Conozca las políticas de cifrado de su organización cuando comparta datos por correo electrónico.

Pérdida de datos internos de forma accidental o maliciosa

- Siga su instinto y siempre denuncie lo que no luzca bien o le resulte inadecuado.
- Tenga cuidado con las técnicas de ingeniería social como el *phishing*: estos correos electrónicos se centran intencionadamente en la emoción humana mediante el uso de palabras como “se necesita su acción inmediata”. Lea detenidamente y proceda con precaución.
- Participe en todas las capacitaciones de concienciación sobre seguridad dentro de sus respectivas organizaciones para mantenerse al día con las últimas amenazas y los pasos que puede tomar para evitarlas.

Seguridad de dispositivos médicos conectados a la red

- Conozca los protocolos de su organización para posibles ataques a dispositivos médicos conectados para que pueda reaccionar y actuar de inmediato.
- Conozca a su equipo. ¿Sabe con quién ponerse en contacto si sospecha de un problema con su dispositivo conectado a la red?
- Compruebe las contraseñas. ¿Se cambió la contraseña del fabricante en el dispositivo médico conectado o sigue siendo un nombre de usuario y una contraseña de “administrador”? Las contraseñas predeterminadas deben cambiarse de inmediato.