

SEGURIDAD CIBERNÉTICA



Las amenazas cibernéticas son reales y están en aumento. Ya sea que estés en casa, en el trabajo o fuera de ella, con unos sencillos pasos puedes mantener tus datos a salvo

Utiliza Contraseñas Seguras

- Al menos 12 caracteres
- Utiliza una combinación de letras, números y símbolos
- Evita nombres o palabras comunes

Habilitar la Autenticación de Múltiples Factores

- Agregar una capa extra de protección a los inicios de sesión
- Mantener el Software Actualizado
- Aplicar parches y actualizaciones a aplicaciones, sistemas operativos y navegadores

Piensa Antes de Hacer Clic

- No abras enlaces o archivos adjuntos sospechosos
- Ten cuidado con los correos electrónicos de phishing

Haga Una Copia de Seguridad de Sus Datos

- Utilice un almacenamiento seguro en la nube o unidades externas

Prepárese Hoy. Listos Mañana.
northtexasprepares.nctcog.org

AMENAZAS CIBERNÉTICAS COMUNES

- Phishing: correos electrónicos, mensajes de texto o sitios web falsos que intentan robar información
- Ransomware: malware que bloquea tus archivos hasta que pagas
- Robo de identidad: información personal robada que se utiliza para cometer fraude
- Ingeniería social: manipularte para que reveles información

PREGUNTAS Y RESPUESTAS SOBRE AMENAZAS CIBERNÉTICAS

¿Cómo puedo identificar un intento de phishing?

- Saludo genérico (“Estimado Usuario”)
- Lenguaje urgente o amenazante
- Enlaces o archivos adjuntos inusuales
- Direcciones de correo electrónico que no coinciden

¿Qué debo hacer si me hackean?

- Cambia las contraseñas de inmediato
- Notifique a su departamento de TI o proveedor
- Revisa tus cuentas financieras
- Ejecute análisis antivirus/malware