Octubre de 2024

Mes de la concientización sobre la seguridad cibernética

¡Protéjase!

1. **Tenga cuidado con los correos electrónicos fraudulentos (*phishing*)**
   El *phishing* es cuando los criminales cibernéticos intentan robar información con correos electrónicos fraudulentos. Fingen ser alguien que no son y pretenden que usted haga clic en enlaces peligrosos. Si recibe un correo electrónico extraño, tenga cuidado; revise quién lo envió y que coincida con el remitente.

2. **Utilice un proceso de autenticación de factor múltiple (MFA)**
   Cuando se inicia sesión con un proceso de autenticación de factor múltiple (*Multi-Factor Authentication*, MFA), se obtiene una capa de protección adicional en contra de los piratas cibernéticos. Es como un texto con un código secreto que caduca después de un solo uso.

3. **Utilice una contraseña segura o una frase de seguridad**
   No use la misma contraseña en todas partes. Use letras, números y símbolos.
   Cuanto más larga la contraseña, mejor. Las frases de seguridad también son una buena opción.

4. **Mantenga los programas actualizados**
   Esto reduce el riesgo de que su computadora se infecte con un programa informático instalado por piratas cibernéticos para robar su información o propagar virus en su computadora.

5. **Manténgase alerta y seguro en las redes sociales**
   Cuando comparte información personal, como su fecha de cumpleaños completa, dirección residencial o ubicación, la pueden usar para robarle su identidad o hacerle *bullying*.

6. **Protéjase utilizando una conexión segura de wifi**
   Las conexiones públicas no son seguras. Cualquiera puede ver lo que está haciendo en línea, como cuando accede a su correo electrónico o sus cuentas bancarias.

7. **Tenga cuidado con las estafas creadas con inteligencia artificial**
   Los ciberdelincuentes utilizan inteligencia artificial avanzada para crear imágenes, texto, voces y videos realistas. Con esto logran que sea mucho más difícil detectar el *phishing* y otras estafas. Esté vigilante y revise varias veces los mensajes (verifique la fuente, busque indicadores de alerta de inteligencia artificial y "artificios" como lenguaje urgente, voces poco naturales o imágenes ligeramente distorsionadas, etc.) antes de confiar en cualquier mensaje inesperado.

NYC Public Schools

diit