EMPODERADO DIGITALMENTE®: TU SEGURIDAD DIGITAL

GUÍA DE RECURSOS DEL PROGRAMA

Patient Empowerment Network

Seguridad digital: Esto significa que puedes reconocer y evitar amenazas en Internet, ayudando a mantener tu información personal segura mientras proteges tu computadora o dispositivo.

Estafa de phishing: Una estafa que busca acceder a la información personal de un usuario, incluyendo contraseñas, números de cuentas o números de Seguridad Social.

Política de privacidad: Lenguaje legal en una página web que describe qué información está recopilando la organización de ti, cómo se está utilizando y con quién podría ser compartida.

Consejos para Identificar Sitios Web Seguros

- Verifica si el dueño del sitio web es una organización en la que confías y reconoces. vinculada al final de la página.
- Si es un sitio web donde tienes que iniciar sesión, asegúrate de que la dirección web comience con “https”. La "s" al final significa que tus datos están seguros y protegidos mediante cifrado.
- Una política de privacidad debe ser fácil de encontrar en el sitio web, y es típicamente información que siempre debe tener salvaguardas para proteger tus datos. Los sitios que te piden información personal siempre deberían tener medidas de protección para tus datos.

Consejos para Evitar Estafas de Phishing

- **No hagas clic en enlaces o abras archivos de fuentes que no conoces o en las que no confías.** Es una buena idea mirar la dirección de correo electrónico completa para asegurarse de que el mensaje proviene de una persona real. Si tienes dudas, no lo abras.
- **Evita cualquier reclamo de que debes dinero o que tienes ganancias pendientes.** Si tienes algún escepticismo sobre correos electrónicos como este, ignóralos. Es probable que seas notificado de otras maneras si estas son reclamaciones legítimas.
- Recuerda que **nadie debe pedirte dinero mediante transferencias bancarias o transferencias de dinero.**

Seguridad en Tabletas y Teléfonos Inteligentes

- Solo **descarga aplicaciones de tiendas de aplicaciones que son recomendadas** por el fabricante de tu teléfono, para proteger la seguridad de tu dispositivo.
- **Configura tu teléfono para que se bloquee automáticamente** con una contraseña cuando no esté en uso, de modo que los extraños no puedan acceder a tu información personal y datos si pierdes tu teléfono.
- **Instala actualizaciones de software a medida que estén disponibles**, para que se implementen las mejoras basadas en la seguridad.
- **Respaldar tus datos utilizando almacenamiento** en la nube para asegurarte de no perder la información personal y los datos que son valiosos para ti.

iamdigitallyempowered.org

Produced by Health Content Collective