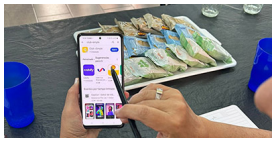

El gobierno porteño realiza charlas y capacitaciones gratuitas para empoderar a las personas mayores a través del uso independiente y seguro de la tecnología.

Cada vez más actividades se trasladan al entorno digital y estos cambios van modificando la forma de vida de las personas y sus hábitos. Ya sea para comunicarse con otros, informarse o entretenerse, sacar un turno médico o realizar un trámite bancario, las personas dependen cada vez más de las herramientas online y de la capacidad para manejarse con ellas.

En línea con las tendencias mundiales, en la Ciudad de Buenos Aires existe una aceleración en la demanda de tecnología, en particular en dos segmentos de la población que a menudo enfrentan desafíos únicos: personas mayores y personas con discapacidades.

La conexión en línea aporta numerosos beneficios.

Estar conectados promueve la actividad mental y puede mejorar la calidad de vida al utilizar nuevas tecnologías, ya que estas herramientas pueden reforzar la independencia y favorecer la autonomía. Participar en actividades grupales en línea fomenta habilidades y enriquece la interacción social.

En este contexto, la seguridad en línea y la protección de los datos en todos los entornos digitales se ha vuelto una necesidad crítica en la vida diaria y un aspecto crucial del bienestar digital, para aprovechar al máximo los beneficios de la tecnología de manera segura y confiada.

El Programa de ABC Digital de la Secretaría de Bienestar está dirigido a personas mayores y personas con discapacidades, con el objetivo de empoderar y enriquecer sus vidas a través del uso independiente y seguro de la tecnología en su vida diaria.

Todas las charlas y capacitaciones de este programa son gratuitas y abiertas a la comunidad. La propuesta completa, con toda la información de los distintos encuentros y el cronograma para participar, está disponible en la app Club +Simple, una plataforma integral de beneficios y servicios para el segmento +60.

¿Cuáles son los riesgos que conlleva la conectividad y cómo podemos evitarlos?

Existen numerosas situaciones y escenarios frecuentes en los que las personas pueden enfrentarse a amenazas en línea. El equipo de capacitaciones de la Gerencia Operativa de Economía Plateada del Gobierno de la Ciudad identifica las siguientes amenazas como las más comunes, y da consejos para prevenirlas.

Phishing: una técnica en la que los atacantes se hacen pasar por entidades confiables para engañar a las personas y obtener información confidencial, como contraseñas o detalles de tarjetas de crédito.
¿Cómo evitarlo? Desconfiar de correos electrónicos, mensajes o enlaces que soliciten información personal o financiera, y verificar siempre la autenticidad de la fuente antes de proporcionar datos.
Ser cauteloso ante solicitudes inusuales o urgentes de información, y confirmar la autenticidad de las solicitudes a través de canales alternativos antes de responder.

Virus y Malware: Son un tipo de software diseñado para dañar o infiltrarse en un sistema informático sin el conocimiento o consentimiento del usuario.
Para prevenir que estos programas se instalen en nuestros dispositivos, es necesario mantener actualizado el software antivirus y realizar escaneos periódicos, así como evitar descargar archivos adjuntos o hacer clic en enlaces sospechosos.

Contraseñas Débiles: Una contraseña débil es vulnerable a los ataques de los ciberdelincuentes y pueden poner en peligro la seguridad y la privacidad online.
Utilizar siempre contraseñas fuertes que incluyan combinaciones de letras, números y caracteres especiales. Evitar el uso de información personal obvia, como nombres y fechas de nacimiento.

Accesos no Autorizados: Los accesos no autorizados pueden tener como consecuencia la pérdida de información confidencial y la exposición a riesgos de seguridad.
Para prevenirlos y detectarlos, es necesario monitorear de cerca las actividades de inicio de sesión en cuentas en línea, y configurar la autenticación de dos pasos para agregar una capa adicional de seguridad, requiriendo un segundo método de verificación además de la contraseña.

Sitios Web Falsos: Encontrarnos con una página web falsa, es más habitual de lo que parece. Hay sitios que se crean simplemente para estafar, robar contraseñas o datos personales.
Por eso siempre es necesario verificar la autenticidad de los sitios web antes de ingresar información sensible. Prestar atención a la URL, asegurándose de que comience con "https://" para indicar una conexión segura.

Otros consejos útiles: Ser selectivo al compartir información personal en línea. Evitar proporcionar detalles innecesarios en perfiles y foros públicos.

- Mantener todos los programas y sistemas operativos actualizados con las últimas versiones y parches de seguridad para prevenir vulnerabilidades.
- Conectar solo a redes Wi-Fi seguras y evitar el uso de redes públicas para transacciones

sensibles.

- Monitorizar Actividades Financieras, revisar regularmente extractos bancarios y reportes de crédito para detectar cualquier actividad sospechosa.
- No hacer clic en enlaces ni descargar archivos de fuentes no verificadas. Activar la autenticación de dos pasos cuando esté disponible.
- Revisar y ajustar regularmente las configuraciones de privacidad en redes sociales y otras plataformas en línea. Limitar la información compartida públicamente.