Taller de Ciberseguridad y Ciberacoso para Adultos con Discapacidades en el Desarrollo

Este taller ofrece herramientas prácticas de protección digital a adultos con discapacidades, combinando educación en seguridad en internet y estrategias para enfrentar ciberacoso.

Los participantes aprenderán a navegar de manera segura en el mundo digital mediante explicaciones claras, ejemplos visuales y actividades participativas, utilizando un lenguaje accesible y herramientas visuales para comprender conceptos de ciberseguridad.

¿Qué es la Ciberseguridad?

Protección Digital

La ciberseguridad es como tener un escudo invisible que protege nuestra información personal cuando usamos internet, computadoras o teléfonos celulares.

Cuidado de Dispositivos

Incluye mantener seguros nuestros dispositivos electrónicos mediante contraseñas, actualizaciones y programas de protección que evitan que personas malintencionadas accedan a nuestros datos.

Navegación Responsable

Significa aprender a identificar sitios web confiables, evitar descargas peligrosas y compartir información personal únicamente cuando sea necesario y seguro hacerlo.

¿Qué es el Ciberacoso?

Definición Fundamental

El ciberacoso consiste en comportamientos repetidos y deliberados dirigidos a causar daño emocional o psicológico a través de medios digitales. Incluye mensajes amenazantes, difusión de información privada sin consentimiento, y exclusión deliberada de espacios digitales.

Este tipo de acoso utiliza tecnologías como redes sociales, aplicaciones de mensajería, correo electrónico y plataformas de juegos para intimidar, humillar o acosar a las víctimas de manera persistente.

Características Distintivas

A diferencia del acoso tradicional, el ciberacoso puede ocurrir las 24 horas del día, alcanzar audiencias masivas instantáneamente, y permitir el anonimato del agresor. La naturaleza digital hace que las evidencias puedan preservarse, pero también que el daño se amplifique rápidamente.

Los efectos pueden incluir ansiedad, depresión, aislamiento social y reluctancia a utilizar tecnologías digitales, afectando significativamente la calidad de vida de las personas vulnerables.

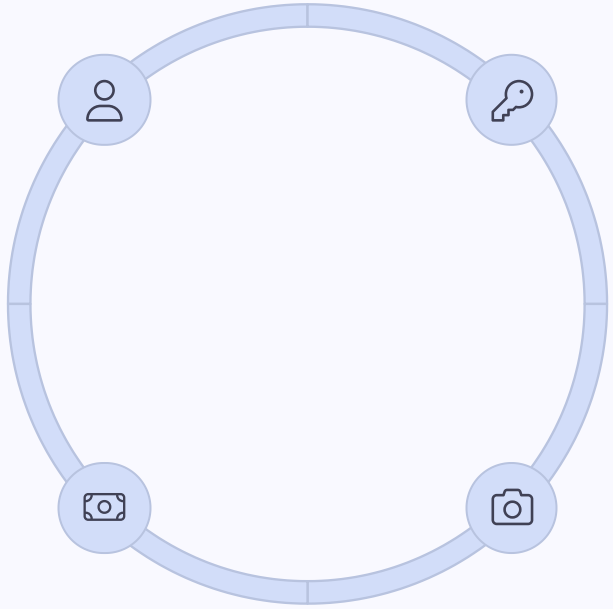
Información Personal: ¿Qué Debemos Proteger?

Datos de Identidad

Nombres completos, números de identificación, direcciones físicas y fechas de nacimiento son información sensible que debe mantenerse privada.

Información Financiera

Números de tarjetas de crédito, códigos de seguridad, información bancaria y detalles de cuentas de pago digital son objetivos principales de criminales cibernéticos.

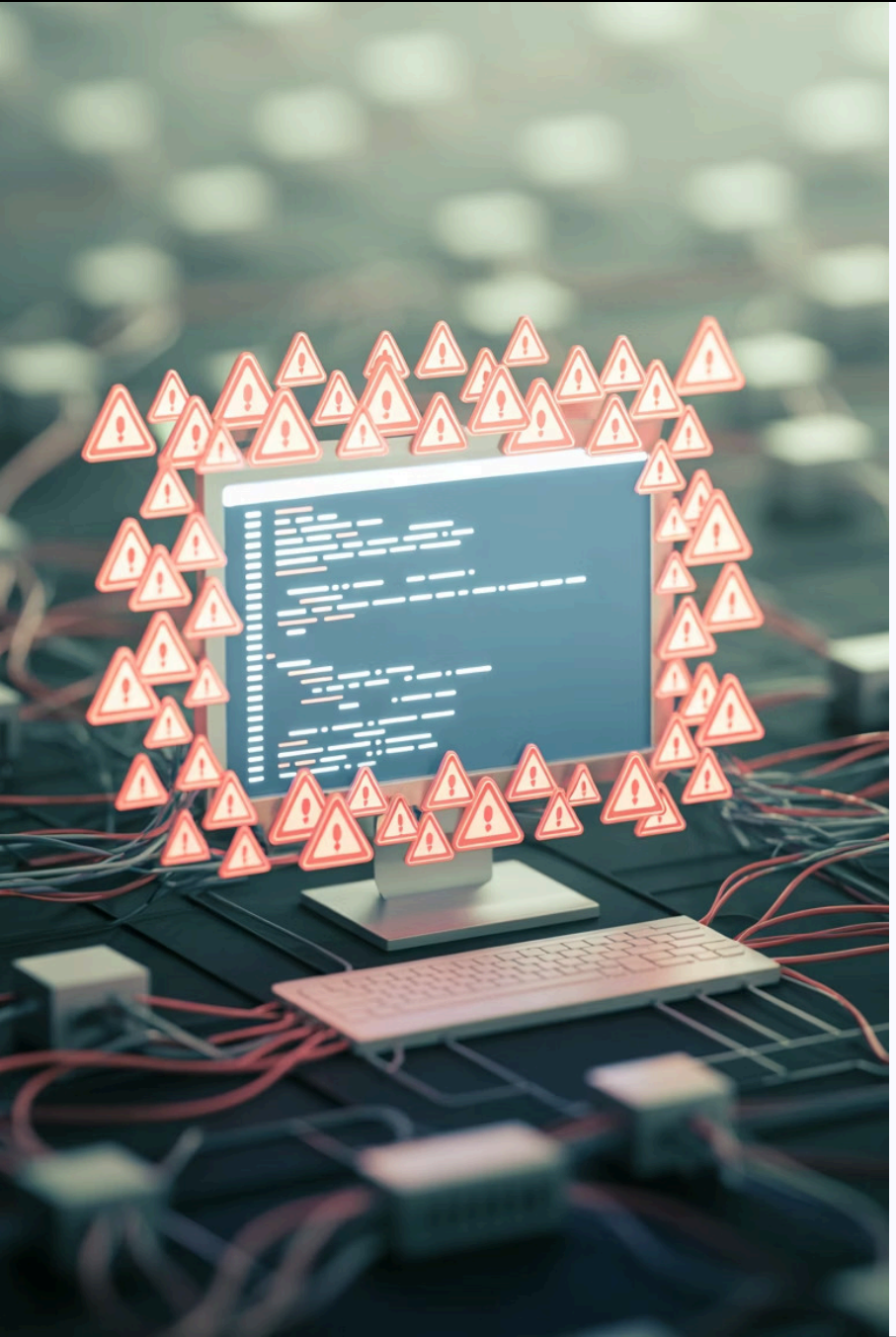


Credenciales de Acceso

Contraseñas, códigos PIN, preguntas de seguridad y datos de acceso a cuentas bancarias o servicios digitales requieren máxima protección.

Contenido Multimedia

Fotografías personales, videos familiares y grabaciones privadas pueden ser utilizados de manera maliciosa si caen en manos equivocadas.



Riesgos en Internet

Contactos Desconocidos

Personas que se presentan como amigos en redes sociales o aplicaciones, solicitando información personal, fotografías o datos de contacto sin tener una relación legítima establecida.

Sitios Web Fraudulentos

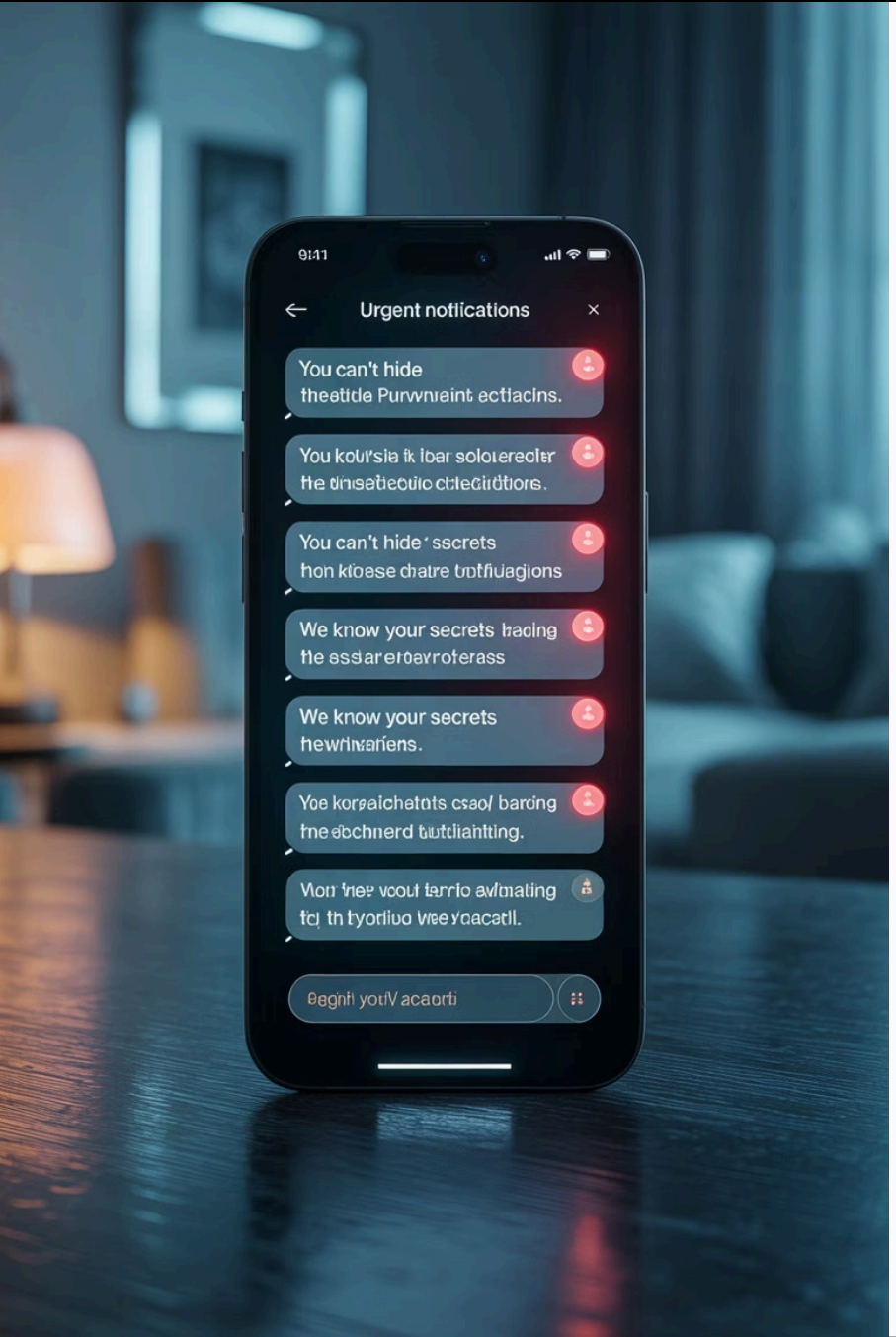
Páginas que imitan sitios legítimos de bancos, tiendas o servicios gubernamentales para robar credenciales de acceso, información financiera o datos personales de usuarios desprevenidos.

Mensajes Engañosos

Correos electrónicos, mensajes de texto o notificaciones que aparentan provenir de instituciones confiables, pero buscan obtener información confidencial mediante técnicas de ingeniería social.

Descargas Maliciosas

Archivos, aplicaciones o programas que contienen virus, malware o software espía diseñado para comprometer la seguridad del dispositivo y acceder a información privada.



Señales de Ciberacoso

Comunicación Hostil

Mensajes repetitivos que contienen amenazas directas, insultos personales, comentarios despectivos o lenguaje intimidatorio a través de cualquier plataforma digital.

- Amenazas de violencia física o emocional
- Insultos basados en características personales
- Chantaje o extorsión digital

Violación de Privacidad

Difusión no autorizada de información privada, fotografías personales o contenido íntimo sin el consentimiento explícito de la persona afectada.

- Publicación de fotos sin permiso
- Revelación de información confidencial
- Creación de perfiles falsos con datos reales

Exclusión Social Digital

Eliminación deliberada de grupos de chat, bloqueo coordinado por múltiples usuarios, o campañas organizadas para aislar socialmente a la víctima en espacios digitales.

- Exclusión de grupos importantes
- Cancelación sistemática de invitaciones
- Difusión de rumores falsos

Cómo Crear Contraseñas Seguras

Combinación de Caracteres

Utiliza letras mayúsculas y minúsculas, números del 0 al 9, y símbolos especiales como @, #, $ para crear contraseñas complejas que sean difíciles de descifrar mediante ataques automatizados.

Evitar Información Personal

Nunca uses fechas de nacimiento, nombres de familiares, mascotas, direcciones o cualquier información que pueda ser fácilmente obtenida a través de redes sociales o registros públicos.

Renovación Periódica

Cambia tus contraseñas cada 3-6 meses, especialmente para cuentas importantes como banca en línea, correo electrónico principal y redes sociales que contienen información sensible.

Contraseñas Únicas

Utiliza una contraseña diferente para cada cuenta o servicio digital. Si una cuenta se ve comprometida, las demás permanecerán seguras y protegidas contra accesos no autorizados.

Navegación Segura

Verificación de Sitios Seguros

Busca siempre el protocolo "https://" en la barra de direcciones y el símbolo del candado antes de introducir información personal. Estos indicadores confirman que la conexión está cifrada y es segura para transmitir datos confidenciales.

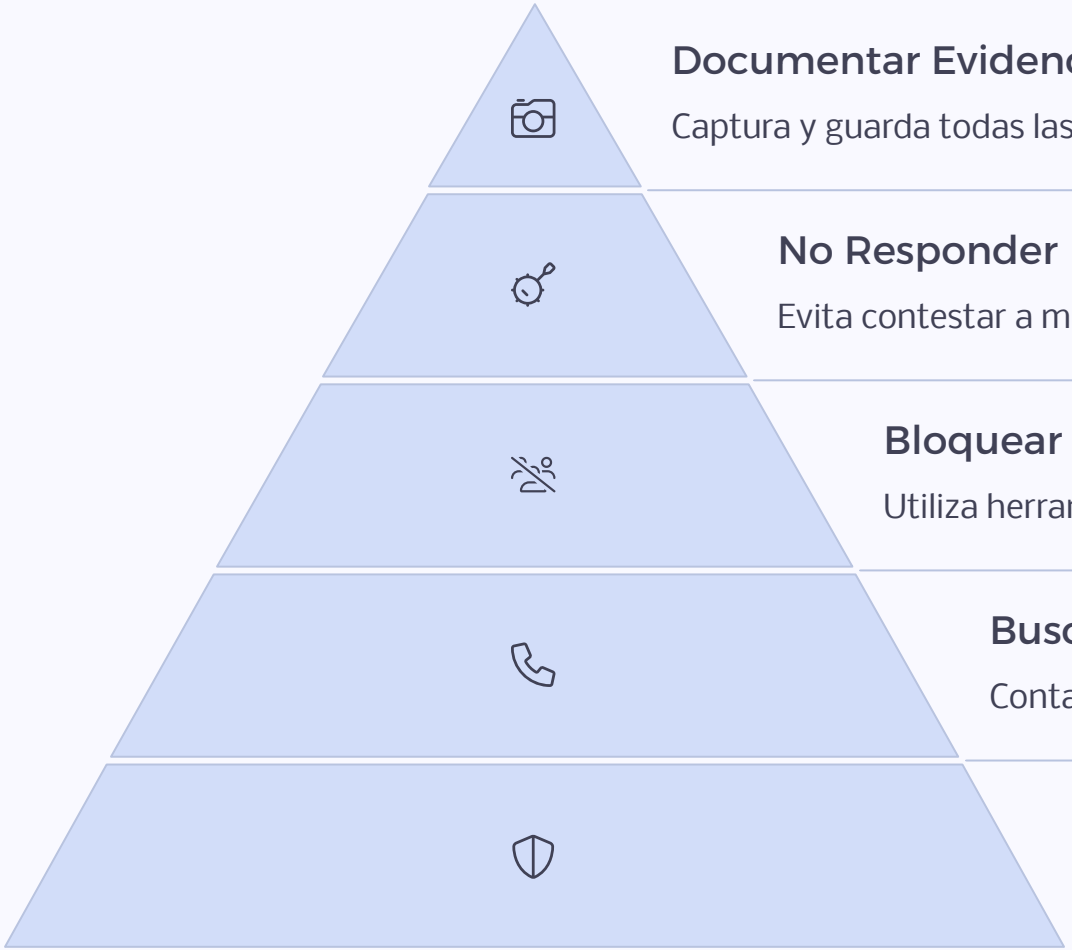
Evaluación de Enlaces

Antes de hacer clic en cualquier enlace, especialmente los recibidos por correo electrónico o mensajes, pasa el cursor sobre él para ver la dirección real de destino. Evita enlaces acortados de fuentes desconocidas y verifica que la URL corresponda al sitio legítimo esperado.

Cierre de Sesiones

Siempre cierra sesión adecuadamente al terminar de usar servicios en línea, especialmente en computadoras compartidas o públicas. Utiliza la opción "cerrar sesión" en lugar de simplemente cerrar la ventana del navegador para garantizar la protección completa.

¿Qué Hacer Si Sufres Ciberacoso?



Documentar Evidencias

Captura y guarda todas las pruebas del acoso

No Responder

Evita contestar a mensajes hostiles o provocativos

Bloquear al Agresor

Utiliza herramientas de bloqueo en todas las plataformas

Buscar Apoyo

Contacta a personas de confianza y profesionales

Reportar el Incidente

Denuncia el acoso a las plataformas y autoridades

A Quién Pedir Ayuda

Círculo Familiar y Social

Familiares cercanos, amigos de confianza y cuidadores que conocen tu situación personal pueden ofrecer apoyo emocional inmediato y ayuda práctica para manejar situaciones de ciberacoso. Su conocimiento personal te permitirá explicar la situación de manera cómoda y recibir orientación personalizada.

Profesionales Especializados

Trabajadores sociales, psicólogos, terapeutas y profesionales de apoyo especializados en discapacidades del desarrollo pueden proporcionar estrategias específicas y recursos adaptados a tus necesidades particulares. Estos profesionales tienen experiencia en casos similares y conocen las mejores prácticas de intervención.

Servicios de Emergencia

Líneas telefónicas de crisis, servicios de emergencia comunitarios y organizaciones especializadas en ciberseguridad ofrecen asistencia inmediata las 24 horas. Muchos de estos servicios cuentan con personal capacitado para atender a personas con discapacidades y pueden guiarte paso a paso en situaciones urgentes.

Actividades Prácticas

Identificación de Mensajes

Practica distinguiendo entre comunicaciones legítimas y sospechosas mediante ejemplos reales de correos electrónicos, mensajes de texto y notificaciones de redes sociales.

Simulación de Situaciones

Participa en escenarios controlados que recrean situaciones de riesgo digital, practicando respuestas apropiadas y estrategias de protección en un entorno seguro y supervisado.

Creación de Contraseñas

Trabaja en equipo para desarrollar contraseñas seguras usando técnicas de memorización, combinaciones de caracteres y herramientas de gestión de contraseñas accesibles.

Uso de Herramientas de Bloqueo

Aprende a navegar por las configuraciones de privacidad y seguridad de diferentes plataformas digitales para bloquear usuarios y reportar contenido inapropiado.

Recordatorio Final: Tus Derechos Digitales

1

Navegación Segura

Tienes el derecho fundamental a acceder y utilizar internet de manera segura, sin temor a ser acosado, estafado o manipulado por otros usuarios malintencionados.

2

Solicitud de Ayuda

Posees el derecho inquebrantable a buscar y recibir asistencia inmediata cuando te sientas incómodo, amenazado o confundido por cualquier situación digital que experimentes.

3

Control de Información

Tienes la autoridad completa para decidir qué información personal compartir, con quién compartirla y cuándo hacerlo, manteniendo siempre el control sobre tu privacidad digital.

Recuerda que la tecnología debe ser una herramienta que mejore tu vida, no una fuente de estrés o peligro. Estos derechos digitales te pertenecen independientemente de tu condición, y existen recursos y personas dispuestas a ayudarte a ejercerlos plenamente. La educación continua y el apoyo comunitario son fundamentales para mantener una experiencia digital positiva y segura.