Protegiendo a Nuestros Mayores: “Prevención de Estafas y Fraudes en la Tercera Edad"

Cómo detectar, prevenir y actuar frente a estafas dirigidas a adultos mayores

Cuando no sabes…. que no sabes….
Eres vulnerable

Que es una estafa o fraude, que tienen en común?

Que es una estafa o fraude, que tienen en común? → EL ENGAÑO

Ustedes fueron engañados por mí, se les dijo que hay una campaña de vacunación…y puessss no hay tal… era mercadotecnia y como ya están aquí pues vamos a aprovechar para decirles como evitar caer en los engaños de la vida diaria….

El engaño data desde Eva con la manzana hasta los ciberdelincuentes de hoy día pasando por el viene viene, por los eñgañiles, por los de los vasos y la bolita, los del fajo de billetes de periódico y asi cientos o miles de modalidades un poco más sofisticadas.

Diferencia entre estafas y fraudes:

Estafas → yo doy la información , ingeniería social, no hay "garantías" o posibilidades de recuperación legal

Fraudes → malware, hackeo,ransomware, troyanos etc. No me doy cuenta, a veces se puede reclamar a bancos o instituciones.

Pero igual cualquiera de los 2 ……quieren tus datos y al final tu dinero

¿Por Qué Son Vulnerables los Adultos Mayores?

- 🧠 1. ***Factores psicológicos y cognitivos***

Deterioro de la memoria o del juicio
El envejecimiento puede afectar la capacidad de razonar con rapidez o identificar situaciones sospechosas.

Soledad o aislamiento social
Muchas víctimas viven solas y se sienten agradecidas por la atención de un desconocido, lo que los hace más propensos a confiar.

Deseo de ayudar o ser útiles
Los adultos mayores tienden a ser amables, solidarios y deseosos de apoyar a otros, incluso en situaciones ficticias.

Negación del riesgo
Algunos no creen que puedan ser víctimas y no toman medidas de precaución.

¿Por Qué Son Vulnerables los Adultos Mayores?

2. *Factores tecnológicos*

•**Baja alfabetización digital**
Desconocen cómo funcionan correos electrónicos, páginas web o redes sociales, lo que los expone a engaños digitales (phishing, enlaces falsos, suplantación).

•**Uso de contraseñas simples o compartidas**
Muchos no actualizan sus claves o las usan en varios sitios a la vez.

•**Falta de medidas de seguridad**
No usan antivirus, verificación en dos pasos, o ignoran señales de alerta en sus dispositivos.

3. Factores sociales y económicos

•**Pérdida de independencia económica**
Algunas personas mayores manejan su dinero sin apoyo y sin asesoría, lo que facilita errores ante estafas.

•**Desconocimiento de derechos y recursos legales**
No saben cómo ni dónde denunciar, o piensan que no serán escuchados.

•**Falta de educación financiera o digital**
Nunca recibieron formación sobre fraudes, bancos, estafas online o cómo protegerse.

4. *Factores relacionados con los estafadores*

- **Estafadores altamente especializados**
  Muchos delincuentes se hacen pasar por empleados de bancos, seguros o familiares usando lenguaje creíble.

- **Técnicas de manipulación emocional**
  Usan el miedo (“su hijo tuvo un accidente”), la urgencia (“transfiera ahora o perderá su cuenta”), o la culpa (“si no ayuda, algo malo pasará”).

- **Uso de redes criminales organizadas**
  Algunas estafas provienen de bandas que recopilan datos y atacan sistemáticamente

¿Por qué este tema es importante?

Cada año, miles de adultos mayores son víctimas de estafas causando pérdidas económicas y emocionales.

La información es la mejor protección.

Clasificación de las estafas o fraudes

- **Físicos**
- **Financieras**
- **Digitales**

Físicos

- **Llamadas telefónicas**
  - Llamadas de supuestos bancos, empresas de servicios mensajería, etc. (Validan claves y datos personales)
  - Una impostor llama diciendo que es un hijo o nieto en apuros (accidente, arresto, secuestro) y necesita dinero urgente.
  - Se les informa que ganaron un premio, pero deben pagar "gastos de envío" o "impuestos" antes de recibirlo.
  - El famoso “curriculum” (pagos atractivos por trabajo simple y luego te sacan datos para enviarte $) L1
  - Llaman y cuelgan (Wangiri) (cobros llamada regreso o validación de numero real para actualizar y vender datos)

- **Suplantación de identidad**

  Alguien se hace pasar por una persona conocida o una autoridad (policía, hacienda, SAT , etc.) para obtener dinero o información. L L2 L3

- **Ofertas de productos milagro**

  Venta de suplementos o tratamientos falsos para enfermedades, especialmente aquellos que prometen curar dolencias relacionadas con la edad.

Físicos

- **Técnicos de reparación falsos**
  Se hacen pasar por empleados de empresas de servicios para acceder a el hogar y robar o secuestrar

- **Falsos servicios:**

Estafadores que ofrecen reparaciones o asesoría, cobran por adelantado y luego no cumplen o realizan un trabajo deficiente.

- **Robos por RFID**
  Delincuentes con acceso a lectores de terminales RFID que los acercan a las carteras de las victimas para hacer cargos contacless sin que se de cuenta la victima L

- **Estafas románticas**
  Relación por internet con una persona que luego pide dinero por motivos personales o “urgencias”.

- **Montadeudas:**
  Ofrecen préstamos rápidos y atractivos, pero después de pagar "gastos de gestión" no entregan el dinero, y en algunos casos, utilizan la extorsión para cobrar.
- **Fraude de falso empleo:**
  Se publican ofertas de empleo falsas donde se pide un pago por adelantado o datos personales que luego son usados para fraudes.
- **Venta de productos apócrifos:**
  Vendedores que anuncian productos en buenas condiciones, pero al momento de la entrega, resultan defectuosos o de baja calidad, y es casi imposible obtener un reembolso.

Digitales o cibernéticas

Phishing
Se trata de una estafa para obtener información confidencial (como contraseñas, datos bancarios o información personal) mediante correos electrónicos que piden actualizar datos, mensajes de texto o sitios web falsos que parecen legítimos. L L2 L3 L4 L5 L6

Malware
Se refiere al software malicioso, como virus, troyanos, ransomware o spyware, que se instala en un dispositivo para robar información, dañar archivos o tomar el control del sistema sin que te des cuenta, se propaga a través de descargas de archivos adjuntos, enlaces en correos electrónicos o sitios web infectados.

Robo de identidad
Es el uso de los datos personales de otra persona (nombre, dirección, información bancaria, etc.) para suplantar su identidad y cometer fraudes o estafas, se realiza a través de llamadas telefónicas, encuestas telefónicas o físicas o la explotación de vulnerabilidades de seguridad para obtener datos personales.

Ciberacoso (Ciberbullying y Grooming)
El primero es el acoso o la intimidación a través de medios digitales como redes sociales, mensajes de texto o correos electrónicos y el segundo es del tipo donde un adulto establece una relación en línea con un menor para abusar sexualmente.

Hackeo
Es el acceso no autorizado y la extracción de datos de sistemas informáticos, archivos o redes sin el consentimiento del propietario. L1 L2 L3 L4

Digitales o cibernéticas

Fraude en comercio electrónico:
Comprar productos que nunca llegan o que llegan defectuosos, especialmente en plataformas como redes sociales y marketplaces.

Suplantación de identidad (SIM Swapping):
Los estafadores obtienen un nuevo chip SIM del número telefónico de la víctima, lo que les da acceso a sus aplicaciones que usan SMS como verificación.

Financieras

Estafas de inversión:

Prometen ganancias rápidas y elevadas en negocios falsos o esquemas piramidales, donde se utiliza el dinero de los nuevos inversionistas para pagar a los anteriores. L1

- Cajero automático con lector “dañado”
- Lectura no autorizada de tarjeta para clonar
- Personas que sustituyen las tarjetas en los cajeros
- Cargos pequeños y recurrentes en bancos (IKP Gautex) L1
- Transferencias de terceros “por error” triangulando a un tercero
- Transferencias o depósitos “en validación” con el soporte de Banxico
- Oportunidades de inversión inmobiliaria irreal (anticipos o promesas falsas de venta)
- Remate de casas (no compran casas…compran juicios)
- Preventas de inmuebles
- Fraudes financieros o abuso por familiares o cuidadores (abuso de poderes legales, uso indebido de cuentas bancarias, robo de propiedades o pensiones)

Señales de alerta

Presión para decidir rápido
Solicitud de dinero urgente
Promesas o precios “demasiado buenas para ser verdad”
Petición de datos personales por medios inseguros

Como prevenir? Como me protejo?

Desconfiar de llamadas urgentes

Si alguien llama diciendo que un familiar está en peligro o necesita dinero, cortar la llamada y **verificar con otro familiar**.

Sé cauto con las solicitudes de dinero:

Nunca envíes dinero a personas que no conoces o a través de servicios de pago o transferencias electrónicas.

Proteger información personal

Nunca compartir contraseñas, números de cuenta o datos de la tarjeta por teléfono o Internet. **No compartas información personal:**

Nunca des tus contraseñas, PIN o datos de tu tarjeta a través de correos electrónicos o mensajes sospechosos. L1

Como prevenir? Como me protejo?

✉ No abrir enlaces o archivos sospechosos

Evitar hacer clic en correos o mensajes que prometan premios o pidan datos bancarios. L1

Verificar antes de abrir la puerta

No dejar entrar a técnicos o vendedores sin confirmar con la empresa o un familiar.

🏠🧠 Consultar antes de actuar

Pedir ayuda a un hijo, nieto o vecino de confianza antes de hacer compras, transferencias o donaciones.

Como prevenir? Como me protejo?

- Para entrar a una pagina suceptible donde hay que meter datos o de compras es mandatorio que **se teclee la url** por prevención de estafa homógrafa. L1
- **Usar contraseñas seguras L1 L2**

- **Frases de seguridad L1**

- **Activa la verificación en dos pasos:**
  Esto agrega una capa adicional de seguridad a tus cuentas en línea

- **Verifica la seguridad de pagos:**
  Asegúrate de que los sitios web donde compras o realizas transacciones utilicen el protocolo "https" y tengan un candado de seguridad. Pero SIEMPRE de paginas oficiales…ojo con esto

Como prevenir? Como me protejo?

- **Desconfía de ofertas irreales:**
  Si una oferta suena demasiado buena para ser verdad, es muy probable que sea un engaño.

- Pónganle clave a su SIM y activen el bloqueo antiapagado para evitar el SIM swapping

- Alerta inmobiliaria, alerta buro de crédito, alerta bancos,etc.

- Comprar carteras anti fraude bloqueo RFID

Como prevenir? Como me protejo?

- No cargar celulares en kioscos públicos , solo apagado
- No conectarse a wifis públicos o gratis (hotspots engañosos)
- No instalar app fuera de Playstore o App Store
- No guardar passwords en Google, es el primer lugar donde buscan los robots que buscan backdoors y la gran mayoría de los equipos de red NO tienen firewall y pueden entrar a la red domestica por cámaras chinas, impresoras wifi o módems antiguos.
- No instalar apps de TV gratis ni en el cel ni en TV ni tvbox porque se abren las puertas de par en par.
- Abrir QR no es peligroso, lo peligroso es que se hace después.
- No abrir ninguna promoción del día del *** que parezca irreal
- No aceptar trabajos de tareas simples y repetitivas como ver videos, dar likes, comentar, etc porque dan “en tu cuenta” y al acumular cierta cantidad te piden tus datos bancarios para transferir incluyendo tu nip y ahí ya perdieron.

Como prevenir? Como me protejo?

- **ACTIVAR la VERIFICACION EN 2 PASOS** L
  (Wats,Google,Face,bancos)
- Establecer correo electrónico de rescate
- Programar y ejecutar respaldos de cuentas en forma automática y periodica para usarse en restauraciones.

- **Es recomendable el uso de 2 celulares**
  - Uno **exclusivo** para apps bancarias con antivirus y antimalware instalado con CERO apps adicionales a las de fabrica, especialmente juegos y este cel SIEMPRE debe de estar en casa u oficina, no en la calle. (Maletin)
  - El otro para el uso diario que no tengan ninguna app que involucre dinero

  - Buenas practicas L

Como prevenir? Como me protejo?

- Establezcan una **pregunta o frase de seguridad** para validar que si es la persona que parece ser por ejemplo
  - De que color es el gato? R= SANDIA … algo ilógico

- DESCONFIEN pero no al punto de ser paranoicos, pero si lo suficiente para no vivir una pesadilla.

La Ingeniería Social

La **ingeniería social** es el uso de **técnicas de manipulación psicológica** por parte de ciberdelincuentes para engañar a las personas y obtener información confidencial, acceso no autorizado a sistemas o realizar acciones perjudiciales, como descargar software malicioso o realizar transacciones fraudulentas. Estos ataques se basan en explotar *la confianza, la credulidad o la curiosidad humana* en lugar de vulnerar la seguridad de los sistemas informáticos.

Cómo protegerse?

- **Desconfiar de correos y mensajes inesperados:** Sea escéptico ante solicitudes de información confidencial o acciones urgentes.
- **Verificar la fuente:** Investigue si el contacto es realmente quien dice ser antes de tomar cualquier acción.
- **No hacer clic en enlaces sospechosos:** Evite abrir archivos adjuntos o hacer clic en enlaces de correos electrónicos o mensajes no solicitados.
- **Mantener el software actualizado:** Las actualizaciones de software suelen incluir parches de seguridad importantes.
- **Capacitar a las personas:** Realizar formaciones y simulaciones de phishing

La Ingeniería Social

REFLEXIONES

- Confiar es bueno….pero desconfiar es MEJOR
- Desconfío , luego valido o verifico y luego actúo
- Aplicar la regla del NO, si decir SI me afecta o afecta a alguien que quiero entonces es NO

REFLEXIONES

- En el mundo real existe la policía y te pueden ayudar, en el ciberespacio estamos solos , por esto debemos de aprender a cuidarnos
- La forma mas fácil de vulnerar un sistema es solicitar el password (Ingenieria social), la segunda es que algo obtenga este password (keylogger o software espia) y la mas difícil es que alguien lo obtenga (Hacker /Cracker)
- Te tienes que convertir en la presa menos fácil de cazar, no seas Bambi en la pradera
- No hay nada gratis en el mundo….menos las apps.

Entre mas sepas menos daño pueden hacerte

r/Monterrey 2 days ago
Ok-Butterfly-9157

Probable estafa

Política Local

CONVOCATORIA EMPLEO 2025
REPRESENTANTE REGIONAL PROGRAMAS SOCIALES; PROGRAMAS DE DESARROLLO INSTITUCIONAL FEDERAL, vacante de trabajo disponibles en todos los municipios del país. Enviar solicitud de empleo o CV por este medio para su revisión y programación de cita presencial en oficina Gubernamental de su ciudad de residencia actual.

VACANTE: REPRESENTANTE REGIONAL PROGRAMAS SOCIALES; PROGRAMAS DE DESARROLLO INSTITUCIONAL FEDERAL.
Publicado: SNE, LinkedIn.
Modalidad: Presencial / Horarios Flexibles
Género: Indistinto
Edad: Indistinta
Actividades: Supervisión programas federales en su ciudad de residencia actual, realizar reportes mediante evidencias de los programas en desarrollo y en curso, implementar reuniones con autoridades de los tres niveles de gobierno, coordinar proyectos de desarrollo social e infraestructura.
Beneficios: Todas las prestaciones de Ley, seguridad social, vales de despensa y combustible, vehículo institucional, beneficios en programas de la iniciativa privada y sector público.
Horarios: Flexibles.
Días: Lunes a viernes.
Nómina: $26,000.00 M.N.

Enviar su CV solicitud@seccionsindical.com como fecha límite el **MIERCOLES 16 / JULIO 2025** con el objetivo de realizar seguimiento y posterior asignación de cita en oficina gubernamental. El proceso inicial de entrevistas lo realiza nuestra agencia de reclutamiento especializada en gestión de personal calificado con el objetivo de contratar a los candidatos más calificados.

LN. JENNY ZAPATA TELLEZ
Recursos Humanos / Gestión RH
solicitud@seccionsindical.com

Me llegó este correo, supongo que es estafa, pero me gustaría saber si es real o no, y si es estafa para advertir a los demás, estaba en mi carpeta de spam

22 9 Share

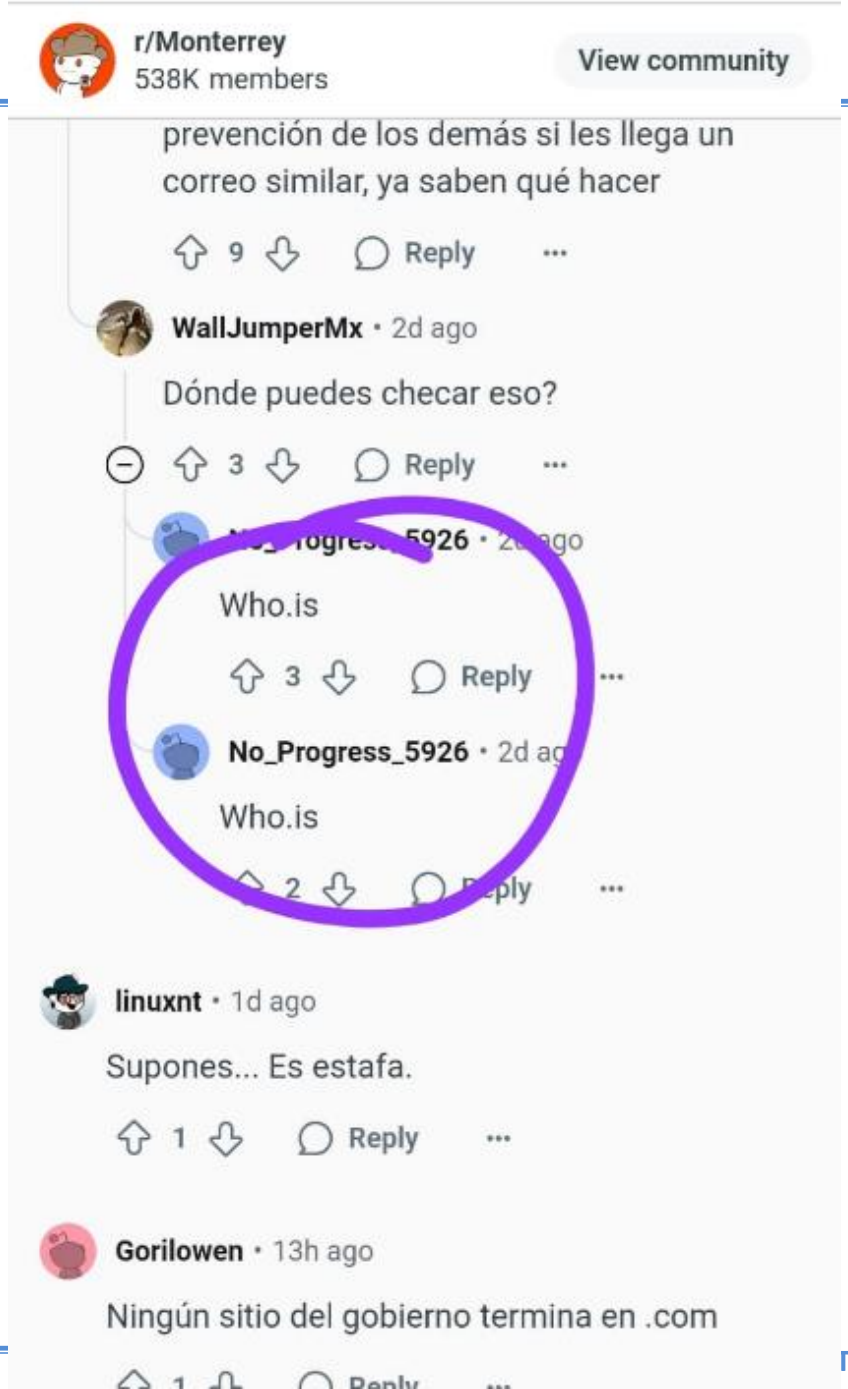
Política Local

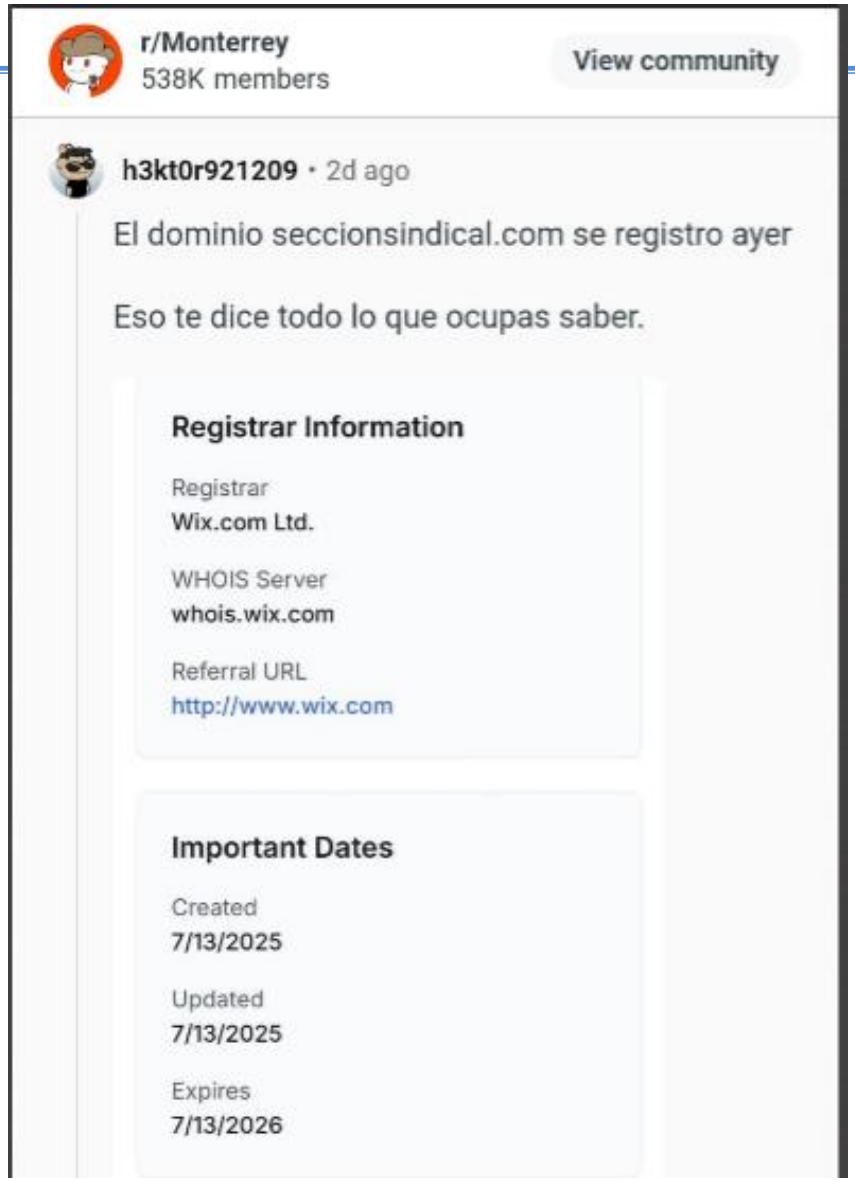
CONVOCATORIA EMPLEO 2025
REPRESENTANTE REGIONAL PROGRAMAS SOCIALES; PROGRAMAS DE DESARROLLO INSTITUCIONAL FEDERAL, vacante de trabajo disponibles en todos los municipios del país. Enviar solicitud de empleo o CV por este medio para su revisión y programación de cita presencial en oficina Gubernamental de su ciudad de residencia actual.

VACANTE: REPRESENTANTE REGIONAL PROGRAMAS SOCIALES; PROGRAMAS DE DESARROLLO INSTITUCIONAL FEDERAL.
Publicado: SNE, LinkedIn.
Modalidad: Presencial / Horarios Flexibles
Género: Indistinto
Edad: Indistinta
Actividades: Supervisión programas federales en su ciudad de residencia actual, realizar reportes mediante evidencias de los programas en desarrollo y en curso, implementar reuniones con autoridades de los tres niveles de gobierno, coordinar proyectos de desarrollo social e infraestructura.
Beneficios: Todas las prestaciones de Ley, seguridad social, vales de despensa y combustible, vehículo institucional, beneficios en programas de la iniciativa privada y sector público.
Horarios: Flexibles.
Días: Lunes a viernes.
Nómina: $26,000.00 M.N.

Enviar su CV solicitud@seccionsindical.com como fecha límite el **MIERCOLES 16 / JULIO 2025** con el objetivo de realizar seguimiento y posterior asignación de cita en oficina gubernamental. El proceso inicial de entrevistas lo realiza nuestra agencia de reclutamiento especializada en gestión de personal calificado con el objetivo de contratar a los candidatos más calificados.

LN. JENNY ZAPATA TELLEZ
Recursos Humanos / Gestión RH
solicitud@seccionsindical.com


r/Monterrey
538K members
View community
prevención de los demás si les llega un correo similar, ya saben qué hacer
9
Reply
WallJumperMx • 2d ago
Dónde puedes checar eso?
3
Reply
Who.is
3
Reply
No_Progress_5926 • 2d ag
Who.is
2
linuxnt • 1d ago
Supones... Es estafa.
1
Reply
Gorilowen • 13h ago
Ningún sitio del gobierno termina en .com


r/Monterrey
538K members
View community
h3kt0r921209 • 2d ago
El dominio seccionsindical.com se registro ayer
Eso te dice todo lo que ocupas saber.
Registrar Information
Registrar
Wix.com Ltd.
WHOIS Server
whois.wix.com
Referral URL
http://www.wix.com
Important Dates
Created
7/13/2025
Updated
7/13/2025
Expires
7/13/2026


lunes, 11 de agosto
Paquetexpress te informa: Rastreo:211220013198 Guia: http://pqtx.mx/eCQgd Fecha: 11/08/2025 15:37 Para: CESAR GONZALEZ IBARRA Status: Documentacion en Linea
4:37 p.m.
04:41 p. m.


2:50
+529834641869
Este mensaje es de un número no guardado.
Cuídese de los fraudes de suplantación de identidad por llamada de voz y mensaje de texto.
Bloquear número
martes, 8 de julio
BBVA: 12:11 hrs. Operacion realizada en APPLE.COM/BILL por $8,000.00 M.N CUENTA** REF:8567. Fecha: 08/07. No reconoces esta compra? llama al: 55 9602 3035.
12:15 p.m.

Si ocurre una estafa…….

No sentir vergüenza ni miedo

Aplicar acciones de contención:

Informar al banco, policía y familiares
Cambiar claves de apps
Cancelar tarjetas si es necesario
Activar alertas (bancos, buro crédito, inmobiliarias,etc)
Denunciar para efectos legales y de seguros

Corregir practicas para evitar caer de nuevo

Conclusión

Las estafas en adultos mayores **no ocurre solo por ingenuidad o edad**, sino por una **combinación de factores personales, sociales y tecnológicos**.

Por eso la solución debe ser **multidisciplinaria**, con enfoque en:

Educación preventiva

Apoyo familiar y comunitario

Protección digital y financiera

Intervención legal eficaz

La prevención empieza con la información

Todos podemos proteger a nuestros adultos mayores

¿Preguntas o experiencias para compartir?


TikTok
@ joan_tito

Por su atención…

Ya están vacunados….!!!!!