



DETECTA:

¿ME HACKEARON O ME
ESTÁN
MANIPULANDO?
APRENDE A
INVESTIGAR RIESGOS
DIGITALES EN LA ERA
DE LA IA

AMIZADAY HERNÁNDEZ

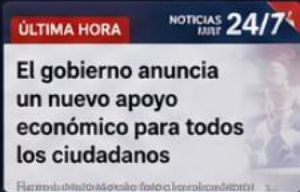
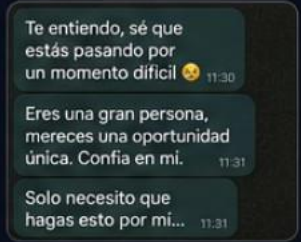
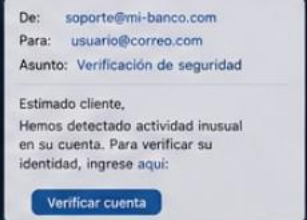
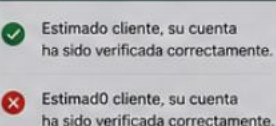
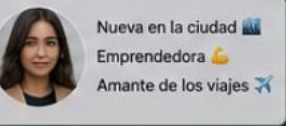
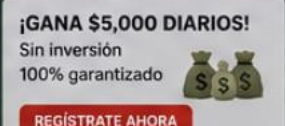
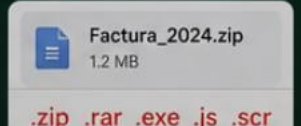


¿CONFIARÍAS EN TUS PROPIOS OJOS?



NADIE SE DESPIERTA PENSANDO...

**HOY VOY A CAER EN
UNA ESTAFA.**

 MANIPULACIONES CON IA Buscan influir en tus emociones, decisiones o comportamiento sin que lo notes.	DEEPPAKES (VIDEOS O AUDIOS FALSOS)  Un video falso puede hacer decir algo que nunca dijo.	LLAMADAS DE VOZ CLONADA  Hola mamá, soy yo, necesito que me hagas un favor... Clonan la voz de un familiar o conocido para pedir dinero o información.	NOTICIAS FALSAS GENERADAS CON IA  Artículos o imágenes falsas creadas para generar miedo, caos o manipular opiniones.	OFERTAS Y ANUNCIOS FALSOS CON IA  Anuncios falsos y páginas que imitan tiendas reales para robar datos o dinero.	BOTS E IA EN REDES SOCIALES  Cuentas automatizadas que promueven fraudes, desinformación o estafas.	MANIPULACIÓN EMOCIONAL CON IA  Usan IA para generar empatía falsa y manipuarte para obtener lo que quieren.
 HACKEOS POTENCIADOS CON IA Usan IA para acceder, robar, dañar o tomar control de tus sistemas y cuentas.	PHISHING INTELIGENTE CON IA  Correos ultra personalizados sin errores, generados por IA para parecer legítimos.	MALWARE INTELIGENTE Y EVASIVO  Esta amenaza usa técnicas de IA para evadir antivirus y permanecer oculta.	ATAQUES A CÁMARAS CON IA (DEEPPVIEW)  La IA analiza patrones de movimiento para detectar cámaras vulnerables y acceder a ellas.	ROBO DE IDENTIDAD SINTÉTICA CON IA  Generan identidades falsas muy realistas para abrir cuentas, solicitar créditos o cometer fraudes.	INGENIERÍA SOCIAL AUTOMATIZADA  Bots con IA mantienen conversaciones creíbles para extraer información sensible.	ATAQUES A WI-FI E IOT POTENCIADOS CON IA  La IA identifica redes vulnerables y dispositivos para infiltrarse sin ser detectada.
 SEÑALES VISIBLES PARA DETECTAR Detalles que pueden indicar que algo no es legítimo.	URLS SOSPECHOSAS  Domínios extraños, letras cambiadas o subdominios sospechosos.	ERRORES SUTILES EN TEXTOS  Errores gramaticales o de redacción poco comunes en empresas reales.	IMÁGENES GENERADAS CON IA  Manos deformes, sombras extrañas, texturas raras, detalles inconsistentes.	PERFILES FALSOS  Sin amigos, fotos de stock, publicaciones repetitivas o generadas por IA.	OFERTAS DEMASIADO BUENAS PARA SER CIERTAS  Promesas exageradas, urgencia y presión para actuar rápido.	ADJUNTOS Y ARCHIVOS SOSPECHOSOS  Archivos inesperados o con extensiones peligrosas.

EL OBJETIVO NUNCA
FUE TU
COMPUTADORA.

EL OBJETIVO SIEMPRE FUE TU **DECISIÓN.**

LA MAYORÍA DE LOS ATAQUES

**EXITOSOS NO COMIENZAN
CUANDO ALGUIEN ROMPE UN
SISTEMA. COMIENZAN CUANDO
UNA PERSONA INTERPRETA
INCORRECTAMENTE LO QUE
ESTA OCURRIENDO.**

**DETECTA NACIÓ PARA AYUDAR A REDUCIR ESA
INCERTIDUMBRE ANTES DE ACTUAR.**

**MARCO METODOLÓGICO PARA INVESTIGAR, VALIDAR Y RESPONDER DE FORMA INFORMADA ANTE
POSIBLES RIESGOS DIGITALES.**

D E T E C T A

DETENTE

EVALÚA

TRIANGULA

EXAMINA

CONFIRMA

**TOMA UNA
DECISIÓN**

ACTÚA

**EN LA ERA DE LA INTELIGENCIA ARTIFICIAL, QUIZÁ LA
HABILIDAD DIGITAL MÁS IMPORTANTE YA NO SEA
SABER USAR LA TECNOLOGÍA. QUIZÁ SEA SABER
CUÁNDO NO CONFIAR EN ELLA.**

CASO PRÁCTICO: “Mi ex publicó fotos íntimas desde mi Facebook”

No sabes exactamente qué pasó. Antes de actuar, aplica DETECTA para investigar y tomar decisiones informadas.

DETECTA

Tu proceso para investigar antes de decidir

LA SITUACIÓN



Recibes mensajes de amigos diciendo que alguien publicó fotos íntimas tuyas en Facebook.

No sabes si:

- Te hackearon
- Tu ex tenía tu contraseña
- Dejaste una sesión abierta
- Fue un dispositivo autorizado
- O es un perfil falso

POSIBLES CAUSAS



Acesso no autorizado (hackeo)



Contraseña compartida o conocida



Sesión abierta en otro dispositivo



Perfil falso usando tu información



Phishing previo para robar acceso

POSIBLES IMPACTOS



Difusión de contenido íntimo sin consentimiento



Afectación emocional y psicológica



Daño a tu reputación online



Consecuencias legales para el agresor



Riesgo de más accesos o extorsión



IMPORTANTE

DETECTA no reemplaza la denuncia ni el apoyo legal o psicológico. Es un proceso para investigar y tomar decisiones basadas en evidencia.

APLICA DETECTA PASO A PASO

D
↓

DETENTE

No actúes impulsivamente. Respira y evita borrar o modificar evidencia.



¿QUÉ HACER?

- No borres las publicaciones aún.
- No confrontes al agresor.
- No cambies nada hasta tener información.

E
↓

EVALÚA

Entiende qué está ocurriendo y qué información necesitas obtener.



- ¿Puedo iniciar sesión?
- ¿Sigo teniendo control de mi cuenta?
- ¿Recibi alertas de Facebook o por correo?
- ¿Cuándo se publicaron las fotos?

T
↓

TRIANGULA

Busca información en múltiples fuentes. No te quedes con una sola versión.



- Revisa tu correo, Facebook y dispositivos.
- Pregunta a amigos qué ven exactamente.
- Verifica en otros dispositivos si puedes acceder.

E
↓

EXAMINA

Analiza la evidencia disponible.



- Revisa inicios de sesión recientes.
- Dispositivos activos.
- Cambios de contraseña o correo.
- Descarga y guarda capturas.

C
↓

CONFIRMA

Valida la información con fuentes oficiales o confiables.



- ¿Realmente hubo acceso no autorizado?
- ¿Fue una sesión que tú dejaste abierta?
- ¿Hubo cambio de contraseña o correo?
- ¿Es un perfil falso?

T
↓

TOMA UNA DECISIÓN

Elige la mejor acción según la evidencia.



- Cambiar contraseña.
- Cerrar sesiones activas.
- Reportar el contenido y el perfil.
- Guardar evidencia para posible denuncia.

A

ACTÚA

Ejecuta la acción correcta.



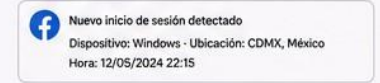
- Cambia tu contraseña y activa 2FA.
- Reporta las publicaciones y/o perfil falso.
- Guarda toda la evidencia (capturas, correos).
- Acude a las autoridades si corresponde.

EJEMPLOS / HERRAMIENTAS

Publicación vista en tu perfil:



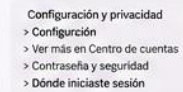
Correo de alerta de Facebook:



Amigo te envía captura:



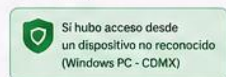
Dónde verlo:



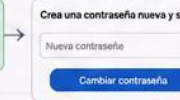
Inicios de sesión



Confirmación:



Facebook te pide cambiar contraseña:



Opciones:



Resultado esperado:

- ✓ Cuenta protegida
- ✓ Contenido reportado
- ✓ Evidencia guardada
- ✓ Proceso legal iniciado (si aplica)



RECUERDA:



La información es poder. Investiga antes de asumir.



Tu seguridad digital está en tus manos.



DETECTA te da el proceso. Tú tomas el control.

¿CUÁNDO APLICA DETECTA?



SÍ APLICA

cuando hay incertidumbre y necesitas investigar antes de actuar.



Correos y mensajes sospechosos

Phishing, notificaciones falsas, enlaces dudosos.



Llamadas y mensajes inesperados

Suplantación, ingeniería social, voz clonada.



Sitios web y enlaces

Páginas falsas, inicios de sesión, formularios.



Contenido generado con IA

Deepfakes, audios, imágenes, videos manipulados.



Incidentes de seguridad

Accesos no autorizados, malware, actividad sospechosa.



Suplantación de identidad

Perfiles falsos, robo de cuentas, impersonación.



NO APLICA

DETECTA no reemplaza servicios especializados.



Emergencias o riesgo de vida

Llama a emergencias. No investigues.



Atención médica

Consulta a profesionales de la salud.



Asesoría legal

Acude a un abogado o autoridad competente.



Análisis forense digital

Requiere herramientas y expertos especializados.



Respuesta a incidentes (CSIRT/SOC)

Es un proceso de investigación inicial, no de respuesta.

**LA IA SEGUIRÁ
APRENDIENDO A PARECER
HUMANA. Y PUEDE
CONVERTIRSE EN UNA
HERRAMIENTA PARA
PERSONAS MAL
INTENCIONADAS PERO...**

**¿Y NOSOTROS APRENDEREMOS A DETENERNOS ANTES DE
DECIDIR?**

SOY SPEAKER EN

DEV DAY 4
Women



HERNÁNDEZ ANGULO AMIZADAY

Docente de tecnologías, Instructora
Lider, ingeniera en software y redes
estudiante de maestria en
Ciberseguridad

 NOVARTIS



devday4w.com



Muchas Gracias!

