UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

SECRETARÍA GENERAL

Prevención y Protección UANL

La excelencia por principio la educación como instrumento

Guía de prevención en seguridad digital

Centro de Atención y Respuesta a Emergencias (CARE): 8113404066
Denuncia anónima UANL (CARE): 8113404089
Línea de Emergencia (Red UANL): ext. *911
Correo electrónico: prevencion@uanl.mx

UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

SECRETARÍA
GENERAL

La excelencia por principio la educación como instrumento

Prevención y Protección UANL

Dr. med Santos Guzmán López.
RECTOR

Dr. Mario Alberto Garza Castillo.
SECRETARIO GENERAL

M.C. David Iván Gómez Velázquez.
DIRECTOR DE PREVENCIÓN Y PROTECCIÓN UNIVERSITARIA

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

SECRETARÍA GENERAL

Prevención y Protección UANL

La excelencia por principio la educación como instrumento

Dirección de Prevención y Protección Universitaria

DIRECTOR
David Iván Gómez Velázquez.

COLABORADORES

Subdirector de Atención y Servicios
Juan Rosas.

Subdirector de Prevención
Sergio Aranda.

Subdirector de Protección
Leonel Garza.

Coordinadora de Inteligencia Preventiva
Cristal Romero.

Nicolle Vargas.

Jissel Lopez.

Daniela Zavala.

Keila Sánchez.

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

SECRETARÍA GENERAL

Prevención y Protección UANL

La excelencia por principio la educación como instrumento

Contenido

Objetivo

Aplicar acciones de prevención y protección en respuesta ante amenazas cibernéticas en redes sociales y dispositivos de telecomunicación, minimizando el impacto de posibles incidentes, fomentando al mismo tiempo una cultura de ciberseguridad entre la comunidad universitaria mediante la provisión de materiales de apoyo visual que refuercen la conciencia y las prácticas seguras en el uso de estas tecnologías.

Alcance

A todas las personas que integran la comunidad de la Universidad Autónoma de Nuevo León.

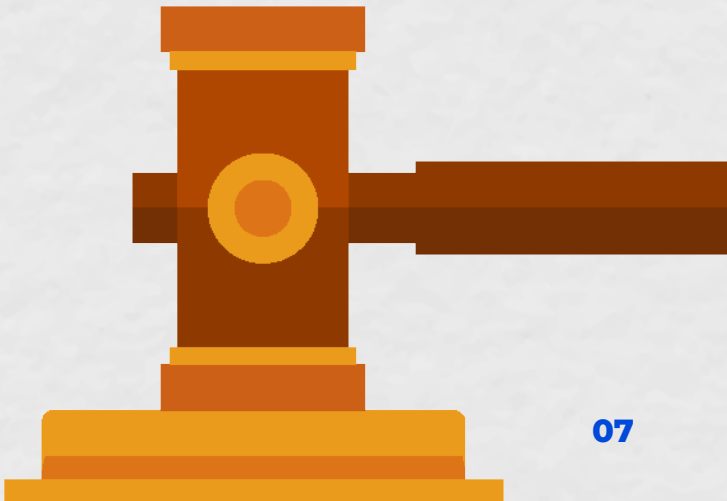
Marco Jurídico

Para el presente documento se tomó como base las conductas y situaciones contempladas en:

Estatuto General
UANL

Reglamento General sobre la Disciplina y el Buen Comportamiento dentro de las Áreas y Recintos Universitarios.
UANL

Código Penal para el Estado de Nuevo León.



Recomendaciones Generales

¿Qué Sí hacer?

Usa antivirus.

Respalda archivos.

Mantén actualizados todos los programas y aplicaciones.

Usa contraseñas seguras (cambiala periódicamente).

Activa la doble autentificación.

Recomendaciones Generales

¿Qué Sí hacer?

Informa a padres, tutores, docentes o persona de confianza sobre cualquier contenido dañino, amenaza o situación negativa.

Desactivar el bluetooth si no se está usando y no aceptar ninguna vinculación y/o archivos de dispositivos desconocidos.

En caso de cualquier amenaza cibernética toma captura y guarda fotos, links, videos y/o audios que puedan utilizarse como evidencia.

Recomendaciones Generales

¿Qué NO hacer?

Compartir información personal en redes sociales ni con personas desconocidas.

Publicar actividades rutinarias.

Abrir correos electrónicos o archivos adjuntos de remitentes desconocidos.

Compartir contraseñas, pin y/o códigos con terceros por cualquier medio.

Guardar nombres de usuario y contraseñas en el navegador.

Recomendaciones Generales

¿Qué NO hacer?

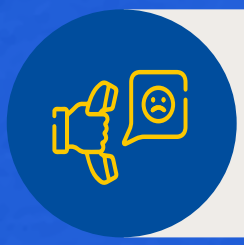
Organizar encuentros con desconocidos ni acceder a hacerlo si algún extraño lo solicita.

Aceptar las cookies de las páginas web que visitas.

Aceptar solicitudes de perfiles desconocidos, ya sea mensaje, amistad o seguir.

Escanear códigos QR desconocidos.

Amenazas más comunes a la Ciberseguridad



Secuestro virtual

Art. 395, fracción VIII y IX del Código Penal de Nuevo León

Llamada de extorsión

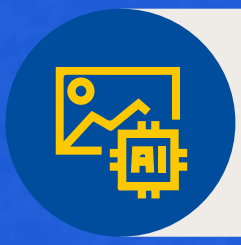
Art. 395, fracción VIII del Código Penal de Nuevo León

Phishing

Art. 385 del Código Penal de Nuevo León

Ingeniería Social

Art. 385 del Código Penal de Nuevo León



Inteligencia Artificial

Amenazas con IA.
Art. 6, fracción VIII Ley de Acceso de las Mujeres a una vida libre de violencia.

Suplantación de Identidad

Art. 444 del Código Penal de Nuevo León

Secuestro virtual

El secuestro virtual es una modalidad de extorsión en la que los delincuentes hacen creer a la víctima que un ser querido ha sido secuestrado. En realidad, no existe ningún secuestro físico, pero los estafadores utilizan tácticas psicológicas y tecnológicas para manipular a la víctima y obtener dinero.

¿Cómo sucede?

Existen diversas formas de operar, la más común es:

Llamada telefónica: Los estafadores llaman y pueden usar gritos, grabaciones con *Inteligencia Artificial,* llantos falsos para parecer real, pueden fingir ser de alguna dependencia gubernamental o banco.

¿Qué le piden realizar a la víctima?

Exigen dinero: Piden un pago inmediato, a menudo a través de transferencias y depósitos bancarios tardados de rastrear.
Manipulación: Crean pánico y urgencia para que la víctima no verifique la situación.

Art. 395 .- COMETE EL DESLITO DE EXTORSIÓN Y SERÁ SANCIONADO CON PENA DE CUATRO A DIEZ AÑOS DE PRISIÓN, EL QUE, CON ÁNIMO DE CONSEGUIR UN LUCRO O PROVECHO; COACCIONE, AMEDENTRE O AMENACE, POR CUALQUIER MEDIO A OTRO CON CAUSAR DAÑOS MORALES, FÍSICOS O PATRIMONIALES, QUE AFECTEN AL AMENAZADO O A PERSONA FÍSICA O MORAL CON QUIEN ÉSTE TUVIERA LIGAS DE CUALQUIER ORDEN, QUE LO DETERMINEN A PROTEGERLA.

VIII. Se utilice la vía telefónica, correo electrónico, redes sociales, aplicaciones móviles o cualquier medio de comunicación electrónica, radial o satelital, para cometer el delito;
IX. Se logre que el sujeto pasivo o un tercero, entregue al activo o a alguna otra persona que actúe en representación de éste o deposite en lugar determinado por éstas, alguna cantidad de dinero o bienes de manera reiterada, por concepto de cobro de cuotas de cualquier índole.

Secuestro virtual

Recomendaciones

- No contestes ni regreses llamadas ni mensajes a números desconocidos y/o cuelga de inmediato.
- Guarda la calma.
- Bloquea el número o perfil.
- Evita proporcionar información a desconocidos que pueda identificarte a ti o a tu familia.
- Considera no realizar transferencias o depósito de dinero.
- No sigas sus instrucciones.
- Mantén una comunicación constante y efectiva con tu familia.
- Denuncia ante las autoridades correspondientes.

Art. 395 .- COMETE EL DESLITO DE EXTORSIÓN Y SERÁ SANCIONADO CON PENA DE CUATRO A DIEZ AÑOS DE PRISIÓN, EL QUE, CON ÁNIMO DE CONSEGUIR UN LUCRO O PROVECHO; COACCIONE, AMEDENTRE O AMENACE, POR CUALQUIER MEDIO A OTRO CON CAUSAR DAÑOS MORALES, FÍSICOS O PATRIMONIALES, QUE AFECTEN AL AMENAZADO O A PERSONA FÍSICA O MORAL CON QUIEN ÉSTE TUVIERA LIGAS DE CUALQUIER ORDEN, QUE LO DETERMINEN A PROTEGERLA.

VIII. Se utilice la vía telefónica, correo electrónico, redes sociales, aplicaciones móviles o cualquier medio de comunicación electrónica, radial o satelital, para cometer el delito;
IX. Se logre que el sujeto pasivo o un tercero, entregue al activo o a alguna otra persona que actúe en representación de éste o deposite en lugar determinado por éstas, alguna cantidad de dinero o bienes de manera reiterada, por concepto de cobro de cuotas de cualquier índole.

Llamada de extorsión

Es un tipo de fraude donde se utiliza la intimidación a través de llamadas telefónicas para chantajear a la víctima, a menudo fingiendo un secuestro, realizando amenazas, exigiendo dinero o haciéndose pasar por autoridades, paqueterías u otras empresas. En algunos casos, también emplean grabaciones o voces generadas con inteligencia artificial para hacer que la situación parezca real.

Recomendaciones

- Evita contestar y/o regresar llamadas a números desconocidos.
- Si contestaste, cuelga de inmediato.
- Guarda la calma y permanece en el lugar donde te encuentras.
- No brindes datos personales o familiares.
- Activa el identificador de llamadas en tu teléfono móvil.
- Considera no realizar transferencias o depósito de dinero.
- En caso de ser alertado sobre una emergencia familiar, inmediatamente verifica la situación y comunícate con tus familiares.
- No sigas sus instrucciones y de inmediato denuncia ante las autoridades.

Art. 395 .- COMETE EL DESLITO DE EXTORSIÓN Y SERÁ SANCIONADO CON PENA DE CUATRO A DIEZ AÑOS DE PRISIÓN, EL QUE, CON ÁNIMO DE CONSEGUIR UN LUCRO O PROVECHO; COACCIONE, AMEDENTRE O AMENACE, POR CUALQUIER MEDIO A OTRO CON CAUSAR DAÑOS MORALES, FÍSICOS O PATRIMONIALES, QUE AFECTEN AL AMENAZADO O A PERSONA FÍSICA O MORAL CON QUIEN ÉSTE TUVIERA LIGAS DE CUALQUIER ORDEN, QUE LO DETERMINEN A PROTEGERLA.

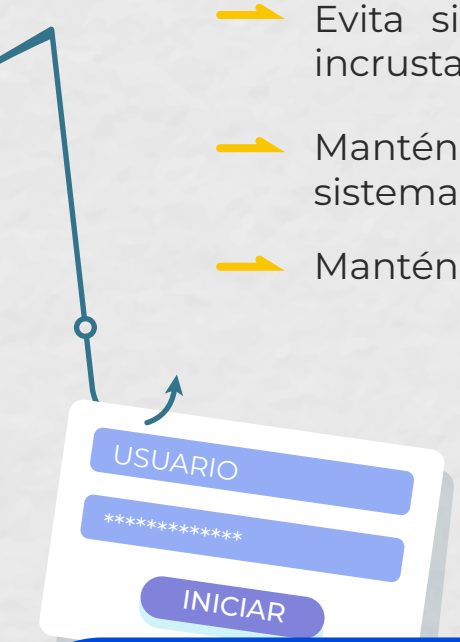
VIII. Se utilice la vía telefónica, correo electrónico, redes sociales, aplicaciones móviles o cualquier medio de comunicación electrónica, radial o satelital, para cometer el delito;

Phishing

Es una táctica engañosa donde los atacantes envían mensajes (anzuelos), correos electrónicos o mensajes de texto fraudulentos, como supuestos avisos de haber ganado un premio, que contienen enlaces a sitios web que pueden contener un virus o pueden engañar a los usuarios para que revelen información confidencial (como contraseñas) o transfieran dinero.

Recomendaciones

- Actúa con sentido común antes de compartir información personal y/o confidencial.
- No abras archivos adjuntos de correos electrónicos sospechosos.
- Evita siempre hacer clic en vínculos incrustados.
- Mantén actualizados el software y el sistema operativo.
- Mantén la seguridad de las contraseñas.



(REFORMADO, P.O. 05 DE ABRIL DE 2023)
ARTÍCULO 385. COMETE EL DELITO DE FRAUDE QUIEN ENGAÑANDO A UNO O APROVECHANDOSE DEL ERROR EN QUE ESTE SE HALLE. SE HAGA ILÍCITAMENTE DE UNA COSA O ALCANCE UN LUCRO INDEBIDO EN BENEFICIO PROPIO O DE UN TERCERO.

Ingeniería social

Es una técnica que se puede emplear con ataque a nivel físico, nivel psicológico y social para manipular y engañar a los usuarios (por ejemplo, haciendose pasar por un conocido o una persona amigable) y poder obtener información confidencial o acceso a dispositivos informáticos para controlarlos.

Recomendaciones

- Evita compartir información importante y personal a desconocidos y/o en redes.
- Comprueba que el mensaje proviene de un sitio web de confianza o un número de teléfono legítimo.
- No descargar archivos adjuntos, ni ceder el control de nuestros dispositivos por medio de algún software.
- Si algo parece demasiado bueno para ser cierto, seguramente sea falso.

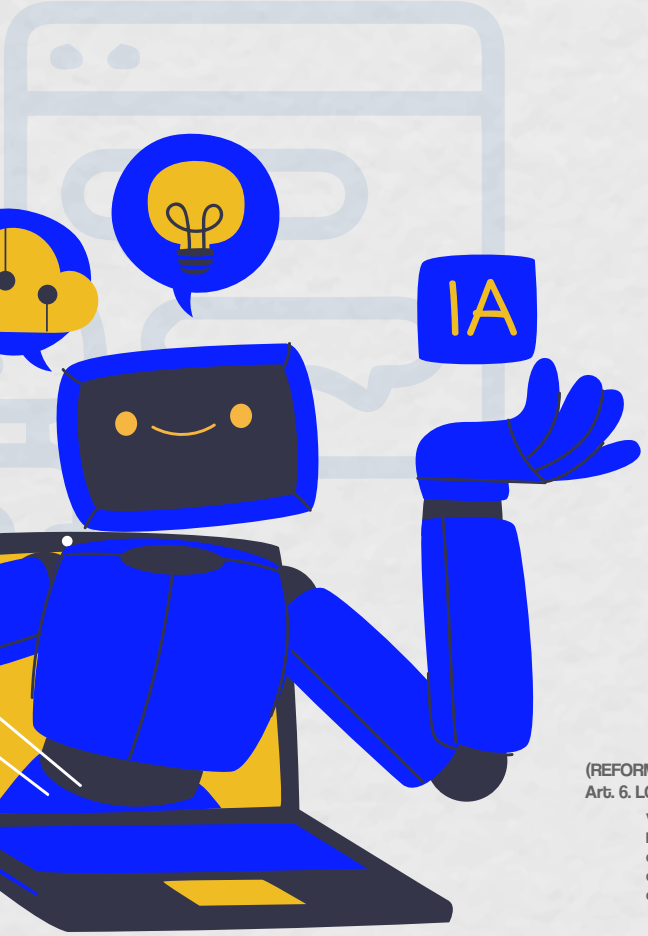
(REFORMADO, P.O. 05 DE ABRIL DE 2023)
ARTÍCULO 385. COMETE EL DELITO DE FRAUDE QUIEN ENGAÑANDO A UNO O APROVECHÁNDOSE DEL ERROR EN QUE ÉSTE SE HALLE, SE HAGA ILÍCITAMENTE DE UNA COSA O ALCANCE UN LUCRO INDEBIDO EN BENEFICIO PROPIO O DE UN TERCERO.

Inteligencia Artificial

La inteligencia artificial, o IA, es tecnología que permite que las computadoras simulen la inteligencia humana y las capacidades humanas de resolución de problemas.

Delitos que se pueden cometer con la inteligencia artificial:

Estafas, fraudes, suplantaciones de identidad, deepfakes o contenido falso, entre más.



Recomendaciones

Verifica la fuente:

- Analiza la calidad del contenido: Coherencia y gramática.
- Vídeo: Parpadeos y movimientos faciales, Incongruencias entre el rostro y el cuerpo, y calidad del sonido.
- Audio: Tono y ritmo, ruido de fondo y contexto del discurso.
- Imagen: Detalles finos e Iluminación y sombras.

(REFORMADA, P.P. 24 DE MARZO 2025)
Art. 6. LOS TIPOS DE VIOLENCIA CONTRA LAS MUJERES SON:

VIII. Violencia digital: Es toda acción dolosa realizada mediante el uso de tecnologías de la información, la comunicación y de Inteligencia Artificial Generativa, por la que se elabore, edite, altere, exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie, comparta o genere imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.

Suplantación de identidad en redes sociales y/o apps de mensajería instantánea

Es un delito en el cual alguien se apropia de la identidad de otra persona o empresa con motivos malintencionados, para obtener datos o información confidencial, hacer fraude económico (fraudes en compras en línea, estafas de inversión, ofertas de trabajo falsas), o causar algún tipo de daño reputacional.

Recomendaciones

- Utiliza un doble factor de autenticación en tus redes sociales.
- Configura los perfiles de tus cuentas lo más privados posibles.
- Revisa las comunicaciones recibidas, tanto por correo electrónico, como por mensajes de texto. En cuanto al remitente, asegúrate de que procede de la red social y de que no se trata de una estafa.

(REFORMADO, P.O. 27 DE OCTUBRE DE 2023)
ARTÍCULO 444. COMETE EL DELITO DE SUPLANTACIÓN DE IDENTIDAD QUIEN SE ATRIBUYA POR CUALQUIER MEDIO LA IDENTIDAD DE OTRA PERSONA U OTORGUE SU CONSENTIMIENTO PARA LLEVAR A CABO LA SUPLANTACION DE SU IDENTIDAD, PRODUCIENDO CON ELLO UN DAÑO MORAL O PATRIMONIAL A LA PERSONA SUPLANTADA O A OTRA PERSONA. SEGÚN SEA EL CASO. U OBTENIENDO UN LUCRO O UN PROVECHO INDEBIDO PARA SI O PARA OTRA PERSONA. ESTE DELITO SE SANCIONARA CON PRISIÓN DE TRES A OCHO AÑOS Y MULTA DE MIL A DOS MIL CUOTAS..

Navegación segura

Usa contraseñas seguras (larga, combina letras, números y símbolos, y evita datos personales) y cámbialas regularmente.

Actualiza tus programas y dispositivos.

Restringe tu perfil en redes sociales.

Verifica la autenticidad de los sitios web.

Evita hacer clic en enlaces sospechosos.

Sé cauteloso con las descargas de internet.

No confíes en redes de WiFi públicas.

Cierra sesión en cuentas compartidas y dispositivos públicos.

Utiliza antivirus.

Actuación en caso de amenaza en las redes sociales y el mundo digital

1. Mantén la tranquilidad.

2. Informa sobre los hechos a un adulto de confianza o personal institucional.

3. Avisa de inmediato a las autoridades pertinentes.

4. Busca un lugar seguro si estás en peligro y no puedes reportar la situación.

5. Si recibes una amenaza, conserva evidencias, guarda enlaces y toma captura de pantalla o fotografía de todo.

Centro de Atención y Respuesta a Emergencias (CARE): **8113404066**
Denuncia anónima UANL (CARE): **8113404089**
Línea de Emergencia (Red UANL): **ext. *911**
Correo electrónico: **prevencion@uanl.mx**

**Aplica en recintos universitarios.*

Concientización

Difusión constante del material visual de esta guía y mantener vinculación entre las escuelas o dependencias y la Dirección de Prevención y Protección Universitaria.

"La ciberseguridad se trata de proteger los dispositivos que todos usamos y los servicios a los que accedemos en línea tanto en casa y escuela como en el trabajo. A través de ella se busca evitar el acceso no autorizado a la información personal que almacenamos en estos dispositivos y en línea."

(Centro Nacional de Ciberseguridad del Reino Unido)

Diagrama de proceso

Se recibe la amenaza

Mantén la tranquilidad

¿Pone en riesgo tu vida?

NO

Informa sobre los hechos a tus padres, tutor, familiar, oficial de seguridad, docente y/o personal administrativo quienes pueden proporcionar apoyo inmediato

SÍ

En caso de no poder reportar la situación, busca un lugar seguro y notifica a las autoridades correspondientes y/o de la institución y al CARE

Sigue las recomendaciones que te brinden tus padres, tutor, familiar, oficial de seguridad, docentes y/o personal administrativo

**Aplica en recintos universitarios.*

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

SECRETARÍA GENERAL

Prevención y Protección UANL

La excelencia por principio la educación como instrumento

¿CÓMO PUEDEN TOMAR CONTROL DE TU CUENTA DE WHATSAPP?

1

Llamada perdida, al no contestar se canaliza a tu buzón de voz.

2

Acceden a tu buzón de voz sin contraseña para obtener código.

3

Registran tu cuenta en otro equipo e ingresan el código.

4

Activan la doble autenticación en el equipo donde registraron tu número.

5

Restringen tu acceso a la cuenta, no podrás acceder aunque seas el propietario.

6

Engañan a tus contactos solicitándoles dinero.

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

SECRETARÍA GENERAL

Prevención y Protección UANL

La excelencia por principio la educación como instrumento

GUÍA PARA VERIFICACIÓN EN 2 PASOS EN WHATSAPP

1. Abre la app, ve a **Ajustes > Cuenta > Verificación en dos pasos** y haz clic en Activar.
2. **Crea y confirma** tu PIN de 6 dígitos.
3. Introduce un correo electrónico para **recuperar la cuenta** en caso de que pierda el pin.
4. Listo ya tiene activado el doble factor de autenticación.

RECUERDA:

NO Compartas el código de seguridad.

Agrega un código a tu buzón de voz o elimina el buzón.

FRAUDES MÁS COMUNES POR MEDIO DE WHATSAPP

Engaños al azar para obtener datos personales:

Se hace pasar por alguien que supuestamente conoces y pide ayuda por un presunto percance en el que necesita tus datos personales para resolverlo.

Extorsión y suplantación de identidad:

Se hacen pasar por un familiar que erróneamente ha solicitado el envío de una clave a tu número celular, con dicho código, el atacante obtiene acceso al dispositivo móvil.

Falsas ayudas económicas:

Comienza con un mensaje sobre un programa de ayuda solidaria, para inscribirte en él debes completar un formulario, esta información es la que recolectan quienes están detrás de este engaño.

Nunca entregues credenciales de acceso a plataformas y cuentas a través de ninguna App.

Activa la verificación en 2 pasos para mayor seguridad.

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

SECRETARÍA GENERAL

Prevención y Protección UANL

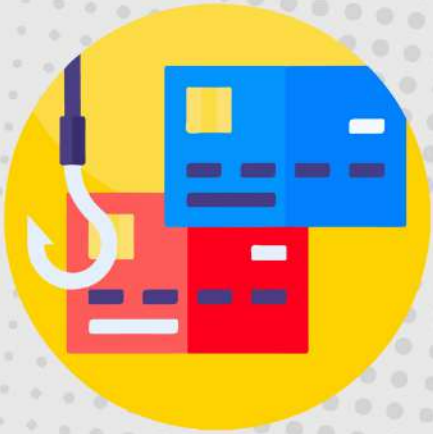
La excelencia por principio la educación como instrumento

¿QUÉ ES EL PHISHING?

Desconfía de textos que tengan **errores de ortografía**.

No compartas tus datos confidenciales.

No hagas clic en enlace, accede a la página web directamente desde tu navegador.



EXTORSIÓN TELEFÓNICA

EVITA contestar llamadas de números desconocidos.

NO DES información personal familiar o de trabajo.

NUNCA realices ningún tipo de pago (transferencia y/o depósito en cajero).

CONSEJOS PARA PREVENIR LA SUPLANTACIÓN DEL ID EN WHATSAPP

- No habilites tu cuenta de Whatsapp en sitios públicos.
- Deshabilita tus datos personales de modo público.
- Cuida el acceso físico al dispositivo.
- Seguridad del dispositivo.

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
SECRETARÍA GENERAL
Prevención y Protección UANL
La excelencia por principio la educación como instrumento

LLAMADA DE EXTORSIÓN

#QUENOTEPASE

¿CÓMO FUNCIONAN?

Son llamadas telefónicas que mediante engaños intentan obtener dinero o información. Los delincuentes fingen ser familiares en peligro, autoridades, o inventan deudas para asustarte y hacer que actúes rápido.

¿QUÉ HACER?

1. **Mantén la calma.** No dejes que el miedo te controle.
2. **Cuelga de inmediato.** Si ya contestaste, no te enganches en la conversación; termina la llamada.
3. **No compartas información personal.** Nunca confirmes o proporciones datos personales o financieros.
4. **No sigas instrucciones del extorsionador.** No envíes dinero ni realices las acciones que te piden.
5. **Verifica la información.** Contacta directamente a la persona involucrada o a familiares.
6. Verifica que tu **identificador de llamadas** está activo.

REPORTA DE INMEDIATO A LAS AUTORIDADES

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
SECRETARÍA GENERAL
Prevención y Protección UANL
La excelencia por principio la educación como instrumento

CÓMO PREVENIR UN SECUESTRO VIRTUAL

Cómo funciona:

1 Se comunican contigo (mensaje o llamada) **dicen ser alguna autoridad**, que pusiste una denuncia o que son de un **grupo de la delincuencia organizada**.

2 **Te ordenan** que hagas lo que dicen si no quieres que te dañen a ti o a tu familia.

3 Te piden no contestar llamadas o mensajes de tus contactos, que les des información que te preguntan, tomarte fotos en ese momento, pueden **tomar control** de tu **cuenta de Whatsapp.**

4 Hacen que te **muevas** a un centro comercial, cibercafé o algún lugar donde dicen **estar vigilándote**.

5 Mientras todo esto pasa, se comunican por mensajes o llamadas de whatsapp con tu familia, **les hacen creer** que te tienen y **exigen un pago**.

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

SECRETARÍA GENERAL

Prevención y Protección UANL

La excelencia por principio la educación como instrumento

CREO QUE ESTOY SUFRIENDO UN SECUESTRO VIRTUAL, ¿QUÉ HAGO?

Conserva la calma

Cuelga la llamada y bloquea número.

Infórmale a tu familia que estás bien y dónde te encuentras.

Si diste datos personales, avisa a tu familia y conocidos para evitar engaños.

Acércate a las autoridades y denuncia.

Ten mucho cuidado, no seas una víctima más

SIM SWAPPING

NUEVA MODALIDAD DE SECUESTRO VIRTUAL

MODUS OPERANDI

1. Personas fingen ser empleados de compañías telefónicas.
2. Ofrecen tarjetas SIM con saldo gratuito a víctimas potenciales.
3. Para hacer el cambio piden sus datos personales.

4. Al insertar la nueva SIM, la línea telefónica con la compañía anterior deja de funcionar.
5. Toman control del número, permitiéndoles realizar llamadas y enviar mensajes desde su línea.
6. Llaman a contactos fingiendo un secuestro y exigen un rescate.

UANL | SECRETARÍA GENERAL | Prevención y Protección UANL | VISIÓN UANL 2040 | La excelencia por principio la educación como instrumento

¿Qué es un RANSOMWARE?

Es un programa malicioso que secuestra tus archivos y los bloquea para poder extorsionar a los usuarios. Luego, te piden dinero (normalmente en criptomonedas) para devolvértelos.

¿Cómo puede afectarte?

- Tus archivos se encriptan y ya no puedes abrirlos.
- Aparece un mensaje que exige un pago.
- Secuestran documentos administrativos o bases escolares.
- Puede propagarse a computadoras conectadas en la red.

¿Cómo prevenir?

- No abras archivos de correos desconocidos.
- Haz respaldos frecuentes (nube o disco).
- Mantén tu antivirus actualizado.
- No uses USBs sospechosos o desconocidos.
- Actualiza tu sistema y programas.

¿Qué hacer si te pasa?

- No pagues el rescate.
- Desconéctate de internet y otros equipos.
- Reporta a ciberseguridad.
- Restaura con un respaldo limpio.

Haz respaldo de archivos importantes en disco externo sin conexión a internet.

¿Dónde denunciar en NL?

Policía Cibernética Nuevo León

https://www.fiscalianl.gob.mx

ciberpol.fc.ssp@nuevoleon.gob.mx

+52 81 3110 7032

UANL | SECRETARÍA GENERAL

Prevención y Protección UANL

VISIÓN UANL 2040

La excelencia por principio la educación como instrumento

¿Qué es un MALWARE?

Es un software intruso que está diseñado deliberadamente para provocar daños en equipos y sistemas informáticos. Incluye amenazas como virus, spyware, adware, ransomware, entre otro tipo de softwares maliciosos.

¿Cómo puede afectarte?

- Tu computadora o celular se vuelve lenta.
- Aparecen ventanas o anuncios extraños.
- Se bloquea tu información y piden dinero para liberarla.
- Se roban tus contraseñas o datos personales.

¿Cómo prevenir?

- No abras archivos de remitentes desconocidos.
- Usa antivirus confiable y mantenlo actualizado.
- No conectes USBs que no conozcas.
- Descarga solo de sitios oficiales.
- Actualiza tu sistema y apps.

¿Qué hacer si te pasa?

- Desconecta tu equipo de internet.
- Haz escaneo con antivirus.
- Cambia tus contraseñas desde otro equipo.
- Informa de inmediato a sistemas o ciberseguridad.

¿Dónde denunciar en NL?

Policía Cibernética Nuevo León

https://www.fiscalianl.gob.mx

ciberpol.fc.ssp@nuevoleon.gob.mx

+52 81 3110 7032

UANL | SECRETARÍA GENERAL | Prevención y Protección UANL | VISIÓN UANL 2040 | La excelencia por principio la educación como instrumento

¿Qué es el PHISHING?

Utiliza correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos para engañar a las personas y hacer que compartan datos confidenciales, o se expongan a la ciberdelincuencia.

¿Cómo puede afectarte?

- Recibes un correo o mensaje que parece de tu banco, escuela o familiar.
- Te piden actualizar datos en un enlace falso.
- Roban tus datos o secuestran tus cuentas.

¿Cómo prevenir?

- No abras mensajes sospechosos.
- Verifica el remitente y el enlace.
- No compartas contraseñas ni datos.
- Activa verificación en dos pasos.
- Usa antivirus y navegador actualizados.

¿Qué hacer si te pasa?

- No des clic ni descargues archivos.
- Cambia tus contraseñas.
- Informa a sistemas o ciberseguridad.
- Contacta a tu banco si diste datos.

¿Dónde denunciar en NL?

Policía Cibernética Nuevo León

https://www.fiscalianl.gob.mx
ciberpol.fc.ssp@nuevoleon.gob.mx
+52 81 3110 7032

UANL | SECRETARÍA GENERAL

Prevención y Protección UANL

VISIÓN UANL 2040

La excelencia por principio la educación como instrumento

¿Qué es el BLUEJACKING?

Es el envío de mensajes no solicitados vía Bluetooth a otros dispositivos cercanos. Puede usarse para molestar, confundir o engañar al receptor.

¿Cómo puede afectarte?

- Recibes mensajes o archivos extraños.
- Te mandan archivos o imágenes desconocidas.
- Puede usarse para bromas, acoso o enlaces fraudulentos.
- Aunque no roba información, sí invade tu privacidad.

¿Cómo prevenir?

- Apaga el Bluetooth si no lo usas.
- Activa el modo "no visible".
- No aceptes mensajes o archivos de extraños.
- Evita usar Bluetooth en lugares públicos

¿Qué hacer si te pasa?

- Rechaza cualquier solicitud o mensaje desconocido.
- Desactiva tu Bluetooth inmediatamente.
- Bloquea números o dispositivos sospechosos.

Si te llega un mensaje raro vía Bluetooth, ignóralo y desactiva la función.

¿Dónde denunciar en NL?

Policía Cibernética Nuevo León

https://www.fiscalianl.gob.mx

ciberpol.fc.ssp@nuevoleon.gob.mx

+52 81 3110 7032

UANL | SECRETARÍA GENERAL | Prevención y Protección UANL | VISIÓN UANL 2040 | La excelencia por principio la educación como instrumento

¿Qué es el BLUESNARFING?

Se conectan a tu celular sin permiso, por medio de Bluetooth, y roban tu información.

¿Cómo puede afectarte?

- Roban tus fotos o documentos personales.
- Acceden a mensajes o correos privados.
- Obtienen números telefónicos y contactos.
- Pueden modificar o borrar información.

¿Cómo prevenir?

- Apaga el Bluetooth si no lo usas.
- No aceptes conexiones desconocidas.
- Activa el modo oculto/no visible.
- Usa contraseñas para vincular.
- Mantén tu sistema y aplicaciones actualizadas.

¿Qué hacer si te pasa?

- Apaga el Bluetooth de inmediato.
- Cambia las contraseñas de tus cuentas.
- Revisa y elimina accesos no autorizados.

OFF

No dejes activado el Bluetooth todo el día, solo úsalo cuando sea necesario.

¿Dónde denunciar en NL?

Policía Cibernética Nuevo León

https://www.fiscalianl.gob.mx

ciberpol.fc.ssp@nuevoleon.gob.mx

+52 81 3110 7032

UANL | SECRETARÍA GENERAL

Prevención y Protección UANL

VISIÓN UANL 2040

La excelencia por principio la educación como instrumento

¿Qué es una DEEPFAKE?

Es una forma de inteligencia artificial (IA) que se puede utilizar para crear imágenes, sonidos y videos engañosos convincentes.

¿Cómo puede afectarte?

- Difunden noticias o situaciones falsas.
- Afectan la reputación de estudiantes y docentes.
- Crean videos falsos de autoridades o personal docente.
- Se usan para fraudes, extorsión o desinformación en redes.

¿Cómo prevenir?

- No compartas videos sin verificar.
- Usa herramientas para revisar contenido.
- Sé cauteloso con videos virales.
- Cuida tu identidad y lo que publicas.

¿Qué hacer si te pasa?

- No difundas el contenido.
- Guarda evidencia (capturas de pantalla, links).
- Denúncialo en redes sociales y avisa a sistemas o ciberseguridad.

Desconfía de videos o audios que parezcan escandalosos o contradictorios.

¿Dónde denunciar en NL?

Policía Cibernética Nuevo León

https://www.fiscalianl.gob.mx

ciberpol.fc.ssp@nuevoleon.gob.mx

+52 81 3110 7032

UANL | SECRETARÍA GENERAL | Prevención y Protección UANL | VISIÓN UANL 2040 | La excelencia por principio la educación como instrumento

¿Qué es el KEYLOGGER?

Es un programa o dispositivo que graba todo lo que escribes en tu computadora o celular: contraseñas, mensajes, correos.

¿Cómo puede afectarte?

- Vigilan tu actividad digital.
- Capturan conversaciones.
- Roban contraseñas de redes o cuentas bancarias.
- Acceden a sistemas escolares.

¿Cómo prevenir?

- No descargues de sitios desconocidos.
- Mantén antivirus y sistema actualizados.
- No uses USBs desconocidos osospechosos.
- Cambia contraseñas con regularidad.
- Usa teclado virtual en computadoras públicas.

¿Qué hacer si te pasa?

- Haz un escaneo completo con tu antivirus.
- Cambia tus contraseñas desde un equipo seguro.
- Revisa accesos sospechosos en tus cuentas.

Si tu equipo va lento o notas accesos raros a tus cuentas, podría ser un keylogger

¿Dónde denunciar en NL?

Policía Cibernética Nuevo León

https://www.fiscalianl.gob.mx

ciberpol.fc.ssp@nuevoleon.gob.mx

+52 81 3110 7032

UANL | SECRETARÍA GENERAL | Prevención y Protección UANL | VISIÓN UANL 2040 | La excelencia por principio la educación como instrumento

MAN-IN-THE-MIDDLE

¿Qué es?

Es cuando un atacante se mete en medio de tu comunicación con otra persona o sistema, sin que se den cuenta.

¿Cómo puede afectarte?

- Roban tus datos al usar WiFi públicas.
- Interceptan conversaciones o correos.
- Pueden redirigirte a páginas falsas aunque parezcan reales.

¿Cómo prevenir?

- No uses WiFi públicas abiertas.
- Usa VPN en redes desconocidas.
- No ingreses contraseñas en redes públicas.
- Revisa que el sitio tenga un candado de seguridad (https://).
- Actualiza tu navegador y aplicaciones.

¿Qué hacer si te pasa?

- Cierra todas tus sesiones de inmediato.
- Cambia tus contraseñas desde una red segura.
- Informa de inmediato a sistemas o ciberseguridad.
- Revisa movimientos sospechosos en tus cuentas bancarias.

¿Dónde denunciar en NL?

Policía Cibernética Nuevo León

https://www.fiscalianl.gob.mx
ciberpol.fc.ssp@nuevoleon.gob.mx
+52 81 3110 7032

Glosario

Amenaza. Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos como incendios o inundaciones; o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado).

CARE. Centro de Atención y Respuesta a Emergencias.

Cookies. Pequeño archivo de texto enviado por un sitio web y almacenado en el navegador del usuario, cuyas actividades y preferencias captura.

Deepfake. Mediante el empleo de IA es posible recrear de manera idéntica la voz e incluso imagen de personas, de políticos y altas personalidades comunicando cierta información o mostrando determinadas conductas que no es real.

DPyPU. Dirección de Prevención y Protección Universitaria.

Phishing. Son técnicas para engañar a una víctima haciéndose pasar por una entidad de confianza, como una persona, empresa o servicio legítimo, con el objetivo de manipular a la víctima para que realice acciones no deseadas, como revelar información confidencial o hacer clic en enlaces maliciosos.

UANL. Universidad Autónoma de Nuevo León.

Referencias Bibliográficas

¿Qué es la inteligencia artificial (IA)?. (s.f). International Business Machines Corporation, IBM México. https://www.ibm.com/mx-es/topics/artificial-intelligence

10 consejos para navegar seguro por internet — Perallis Security. (s. f.). https://www.perallis.com/noticias/10-consejos-para-navegar-seguro-por-internet-1

Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? | Empresas | INCIBE. (s. f.). https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? | Empresas | INCIBE. (s. f.-b). https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Art. 271 BIS 5. del Código Penal de Nuevo León.

Art. 291 del Código Penal de Nuevo León.

Art. 385. del Código Penal de Nuevo León.

Art. 395, fracción VIII y IX del Código Penal de Nuevo León.

Art. 444 del Código Penal de Nuevo León.

Art. 4 del Reglamento general de disciplina y buen comportamiento de la Universidad Autónoma de Nuevo León.

Art. 6, fracción VIII de la Ley de Acceso de las Mujeres a una vida libre de violencia.

De Gobernación, S. (s. f.). El secuestro virtual es una nueva modalidad de #ExtorsiónTelefónic. . . gob.mx. https://www.gob.mx/segob/articulos/sabes-que-es-el-secuestro-virtual/

De Seguridad y Protección Ciudadana, S. (s. f.). Delitos cibernéticos. gob.mx. https://www.gob.mx/sspc/articulos/conoce-los-principales-delitos-ciberneticos-y-siguenuestras-recomendaciones-para-prevenir-que-tus-hijas-e-hijos-sean-posibles-victimas

De Seguridad y Protección Ciudadana, S. (s. f.-b). Delitos cibernéticos. gob.mx. https://www.gob.mx/sspc/articulos/conoce-los-principales-delitos-ciberneticos-y-sigue-nuestras-recomendaciones-para-prevenir-que-tus-hijas-e-hijos-sean-posibles-victimas

Cookie. (s.f). Diccionario de la Lengua Española | Real Academia Española. https://dle.rae.es/cookie

Inteligencia Artificial (IA) y ciberseguridad | Ciudadanía | INCIBE. (s. f.). https://www.incibe.es/ciudadania/tematicas/inteligencia-artificial

Maldonado, Mario, Eduardo (2024) Inteligencia Artificial y delito. Nuevos retos en el ámbito legislativo. Centro de Estudios de Derecho e Investigaciones Parlamentarias. https://portalhcd.diputados.gob.mx/PortalWeb/Micrositios/49b2406e-31d1-451b-b123-f901f75e880a.pdf

Referencias Bibliográficas

Maneras de evitar ataques de ingeniería social. (2023, 25 septiembre). www.kaspersky.es. https://www.kaspersky.es/resource-center/threats/how-to-avoid-social-engineering-attacks

Phishing: Spot and report scam emails, texts, websites and calls. (s. f.). https://www.ncsc.gov.uk/collection/phishing-scams

QR Codes - what's the real risk? (s. f.). https://www.ncsc.gov.uk/blog-post/qr-codes-whats-real-risk

Secretaría de Infraestructura, comunicaciones y transporte. (2024) Guía de Ciberseguridad para el uso de redes y dispositivos de telecomunicaciones gob.mx https://www.gob.mx/sct/documentos/guia-de-ciberseguridad-en-apoyo-a-la-educacion

Secretaría de Seguridad y Protección Ciudadana. (s.f) Ciberguía. gob.mx https://comisioncontralatrata.segob.gob.mx/work/models/Comision_Intersecretarial/Documentos/pdf/Biblioteca/CIBERGUIA-comprimido.pdf

Suplantación de identidad | Menores | INCIBE. (s. f.). https://www.incibe.es/menores/tematicas/suplantacion-de-identidad

Suplantación y robo de identidad en las redes sociales, un riesgo para las empresas | Empresas | INCIBE. (s. f.). https://www.incibe.es/empresas/blog/suplantacion-y-robo-identidad-las-redes-sociales-riesgo-las-empresas

Todo lo que debes saber acerca de las estafas y la prevención de phishing. (2024, 2 febrero). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

Treviño, R. (s. f.). Extorsiones telefónicas: qué son, características cómo evitarlas. Tecnológico de Monterrey. https://conecta.tec.mx/es/noticias/nacional/sociedad/extorsiones-telefonicas-que-son-caracteristicas-y-comoevitarlas#:~:text=%E2%80%9CLa%20extorsi%C3%B3n%20telef%C3%B3nica%20es%20un,resultado%20que%20obtienen%20muchas%20veces

Universidad Autónoma de Nuevo León. (2024) Estatuto General. http://transparencia.uanl.mx/secciones/normatividad_vigente/archivos/Normatividad_vigente/03EstatutoGeneral.pdf

Centro de Atención y Respuesta a Emergencias (CARE): **8113404066**
Denuncia anónima UANL (CARE): **8113404089**
Línea de Emergencia (Red UANL): **ext. *911**
Correo electrónico: **prevencion@uanl.mx**

OCTUBRE 2025, EDICIÓN 1

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

SECRETARÍA GENERAL

Prevención y Protección UANL

La excelencia por principio la educación como instrumento