



GOBIERNO DE
MÉXICO



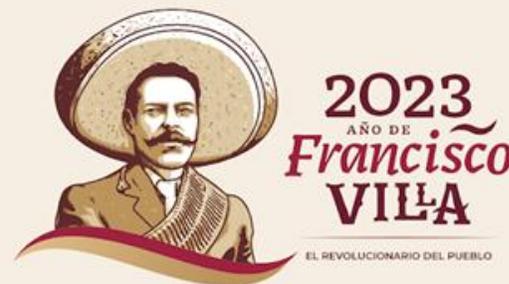
GN
GUARDIA
NACIONAL

Ciberseguridad Financiera Fraudes Cibernéticos

Unidad de Órganos Especializados por Competencia
Dirección General Científica

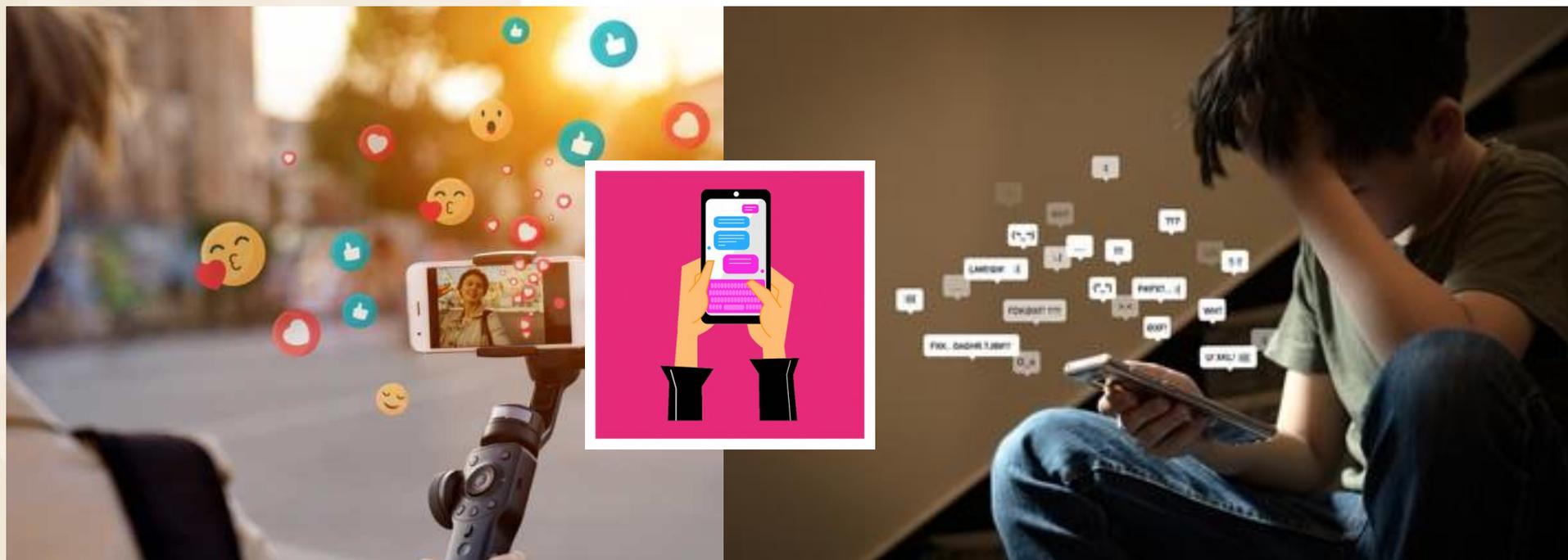
Foro Salud Financiera para Mujeres

28 Marzo 2023



La ciberseguridad es tarea de todas y todos

Los buenos hábitos de ciberseguridad siempre nos protegerán en el ciberespacio, evita riesgos.



El internet puede brindarnos muchos beneficios en nuestras actividades

Principales actividades digitales en México



GOBIERNO DE
MÉXICO



GN
GUARDIA
NACIONAL



- 78% Acceder a contenidos audiovisuales.
- 45.7% Descargar software o aplicaciones.
- 42.3% Interactuar con el Gobierno.
- 42.1% Leer periódicos, revistas o libros.
- 30.1% Comprar productos o servicios.**
- 24.5% Operaciones bancarias en línea.**
- 22.5% Utilizar servicios en la nube.
- 12.6% Ventas por internet.

Horizonte de riesgos globales 2022

Foro Económico Mundial (WEF)



Los riesgos tecnológicos representan un porcentaje latente a nivel mundial.



Categorías de riesgos

- Económicos
- Medioambientales
- Geopolíticos
- Sociales
- Tecnológicos

Fuente: World Economic Forum (2022) "The Global Risks Report 2022 17th Edition" Recuperado de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf



Principales malos hábitos de ciberseguridad



GOBIERNO DE
MÉXICO



GN
GUARDIA NACIONAL

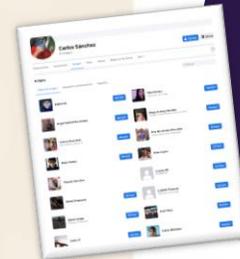
Dejar expuestos datos personales



Publicar al instante un momento que deseamos compartir



Exhibir el patrimonio personal o familiar



Compartir contraseñas y utilizar personas desconocidas



Recibir y enviar contenido ofensivo o inapropiado



Difundir datos sensibles personales, familiares e institucionales



Técnicas de ingeniería social que ponen en riesgo la economía de los cibernautas.



GOBIERNO DE
MÉXICO



SUSCRIPCIONES GRATUITAS
pueden tener códigos maliciosos



SPAM

correos de desconocidos con archivos maliciosos

COMUNICADOS FALSOS
solo buscan confundir



OFERTAS ATRACTIVAS

suelen ser irreales y pueden derivar robos

CORREOS ALARMANTES
para obtener información personal y financiera



PÁGINAS APÓCRIFAS (Phishing)

solicitan donativos o información

SERVICIOS GRATUITOS (SMiShing)
ofrecen premios al entrar a un link



¿Cómo actúa el Phishing?



GOBIERNO DE
MÉXICO



Modalidad de robo de identidad, a través del diseño de **páginas web que simulan ser sitios auténticos de instituciones bancarias, empresas de comercio electrónico y otras instancias dedicadas al pago de servicios**, que son difundidas en mensajes de correo electrónico, mensajería instantánea, motores de búsqueda y redes sociales, principalmente.



Banco General 2014. ¿Qué es el phishing?
<https://www.youtube.com/watch?v=Z34PbwQtGqk>



Evita caer en correos electrónicos apócrifos tipo phishing



GOBIERNO DE
MÉXICO



GN
GUARDIA
NACIONAL

Soporte Gmail <noreply@googleaccounts.com>

Hola,

Debido a cambios recientes en su cuenta de GMail (contraseña e información personal), por seguridad usted debe confirmarla. Si no confirma su cuenta es posible que el Equipo de GMail cierre su cuenta por seguridad. Recuerde tiene un plazo de 3 días para realizarlo. Para confirmar porfavor ingrese al siguiente link:

<http://www.google.com/confirmcontact.php?c=714395034> (Si el enlace no te funcionar al hacer clic, intenta copiar y pegar la dirección en tu navegador.) Si no ingresaste esta dirección como cuenta Gmail, favor de descuidar este mensaje. Consulta <http://www.google.com/help.php?page=173> si tienes alguna pregunta.

Gracias Diviertete!

El equipo Gmail

¿Sabías que el mejor amigo de Hotmail es Messenger? ¡Conoce las razones!

<http://login.live.com/by117fd.bay117-passport-net-by103fd-bay103-hotmail-msn-com-curml>



Internet | Modo protegido: activado



2023
AÑO DE
**Francisco
VILLA**
EL REVOLUCIONARIO DEL PUEBLO

¿Cómo identificar un correo electrónico fraudulento?



GOBIERNO DE
MÉXICO



Asunto importante

Mediante técnicas de ingeniería social, buscan atraer tu atención para que abras el mensaje.

Múltiples destinatarios

Aunque el correo vaya dirigido a ti, puede dirigirse también a otras personas desconocidas, o marcar copia oculta a miles de direcciones de correo.

Mensajes no personalizados

Al iniciar el mensaje, se dirige a un usuario genérico como "cliente," usuario, tarjetahabiente..."

Solicitud de información

Recuerda que ninguna empresa o institución solicita datos personales o confidenciales mediante correo electrónico.

Vínculos o enlaces

En el mensaje, generalmente se solicita ingresar a enlaces que dirigen a páginas web fraudulentas o infectadas de virus informáticos.

micorreo Juan.dominguez@micorreo.com

Redactar Responder Reenviar Eliminar Archivar Correo no deseado

Buzón (12)
Enviados
Eliminados
Borradores
Archivo
Carpetas
Agenda
Contactos

Asunto Tu tarjeta ha sido cancelada
De soporte.tecnico.mibanco@yahoo.com.mx
Para juan.dominguez@..com, juan01domingues@..com,jdomin....

Archivos adjuntos: solicitud_alta_cta.exe

Mi Banco

Estimado cliente:

Debido a una falla detectada en el sistema, su tarjeta de crédito fue bloqueada y protegida de cualquier robo o fraude de manera exitosa. Realice las siguientes indicaciones para que puede hacer uso de sus servicios en línea:

- 1.- Descargue el archivo solicitud_alta_cta.exe y llene el formulario con los datos que se solicitan.
- 2.- Acceda al siguiente URL: www.mibanco.com
- 3.- Suba el archivo en el apartado que aparece.

En breve un ejecutivo se comunicará para validar su solicitud.

ATENTAMENTE
Saul Torres VeLeZ
Director General

Remite desconocido

Comúnmente utilizan proveedores del servicio de correo electrónico gratuitos (Hotmail, Yahoo, Gmail, etc...), a nombre de empresas o instituciones reconocidas.

Archivos adjuntos

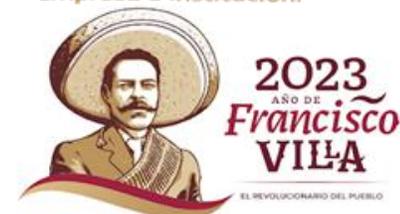
Pueden contener archivos adjuntos que al descargarse pueden ocasionar daños a los dispositivos con los que accedes a internet.

Mala redacción y ortografía

El mensaje generalmente está mal redactado o adaptado con traductores automáticos. Las empresas o instituciones cuidan cada detalle, como la ortografía al dirigirse a sus clientes o socios, con el objetivo de mantener una buena imagen y presentación.

Firma falsa

Puede tratarse de una persona falsa fingiendo un cargo importante en la empresa o institución.



Lista de los sitios web que se han detectado como apócrifos



GOBIERNO DE
MÉXICO



El portal <https://www.sat-mexico.com/vehiculos> es apócrifo
No te dejes engañar

HACIENDA | SAT

¿Cuáles Son Los Beneficios De Adquirir un Vehículo con una Institución Gubernamental?

SITIO APÓCRIFO

¿Que tipo de vehículos te gustaría comprar? Estamos en liquidación

Autos comerciales | Autos deportivos | Camionetas SUV | Camionetas Pick-up

Envío gratis a toda la republica mexicana

Contacto

Intentan suplantar a la SHCP, SAT o Aduanas:

<https://sat-goodyeargob.mx>

<https://sat-bmwgob.mx>

<https://www.sat-ventadirecta.mx>

<https://www.rematetributarios.com>

<https://www.rematetributarios.org>

<https://aduanas-sat.com.mx>

<https://www.remates-tributarios.com>

<https://satgobmx.com>

<https://aduanas-sat.com.mx>



¿Cómo actúa el Pharming?

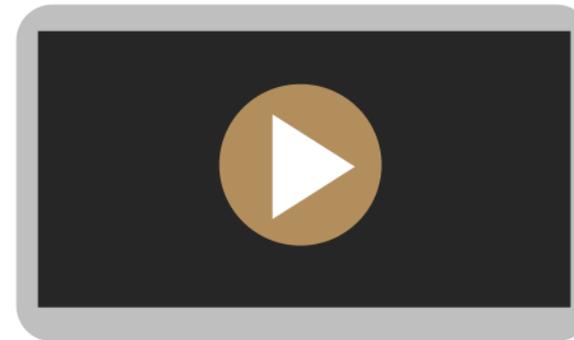


GOBIERNO DE
MÉXICO



GN
GUARDIA
NACIONAL

Es una práctica fraudulenta similar al phishing, que **orillan al usuario a instalar los archivos adjuntos los cuales contienen códigos maliciosos que redireccionan a Sitios Web falsos**, donde se le solicita información para enviarla a terceros.



Doble 2014. "¿Qué es el pharming?"
<https://www.youtube.com/watch?v=k3b5xzB3dds>



Ante una notificación urgente, evita caer el pharming a través de la descarga de archivos maliciosos.



GOBIERNO DE
MÉXICO



GN
GUARDIA
NACIONAL



lunes 11/04/2016 01:33 p. m.

Notificaciones SAT <notificaciones@[REDACTED]>

Anomalías graves en su situación fiscal actual. Último Aviso

To



Último Aviso:

Estimado Contribuyente:

El Servicio de Administración Tributaria se ha percatado que en diversos despachos alrededor del País, Usted ha propuesto esquemas para evadir el pago de impuestos y hemos detectado anomalías en su situación fiscal. Para evitar una sanción en su contra, le recomendamos regularizar su situación fiscal inmediato. A continuación le adjuntamos un documento detallado de su situación fiscal actual.

<http://verasmo.com/word.html?id=1223b8c30a347321299611f873b449a>
Click to follow link

[Descargar Documento](#)

© Derechos Reservados SAT - Servicio de Administración Tributaria



2023
AÑO DE
Francisco
VILLA
EL REVOLUCIONARIO DEL PUEBLO

Ejemplos de smishing.



¡Felicidades!

¡Lo hiciste! ¡Ganaste el Toyota Corolla!
*** LAS NORMAS ***

1. Debes informar a 5 grupos o 20 amigos sobre nuestras promociones.
2. Ingrese su dirección y complete el registro.

OK

Adidas regala 5000 pares de zapatos gratis para celebrar su 93° aniversario. Obtenga sus zapatos gratis en : <http://www.adidas.com/zapatos-gratis/> .

21:21

Reenviado



Regalos del 20 Aniversario de Mercado Libre.

2000 productos gratis! 🛒👉

gentleall.top

http://gentleall.top/MercadoLibre/tb.php?_t=1623778159

01:29:19

12:57

Spoofting Telefónico

Spoofting (falsificación, modificación de los datos) es el acto de suplantación de identidad, ocurre cuando una persona mediante **llamadas telefónicas o mensajes de texto (SMS) falsifica deliberadamente, la información del identificador de llamadas.**

Los estafadores a menudo utilizan la suplantación de identidad de un número local, compañía u organismo gubernamental conocido por la víctima.

Si el objetivo contesta, los defraudadores utilizan guiones o la ingeniería social para obtener información personal, que se puede utilizar en actividades fraudulentas.



GOBIERNO DE
MÉXICO



Actualización de datos

citibanamex



Dic 29, 2021 11:32:00 AM

Como parte del proceso de venta de la banca empresarial y de consumo de Citibanamex, necesitamos verificar tus datos. Recuerda que si en 24 horas no son actualizados, tu cuenta será cancelada.

Actualiza aquí tus datos:

www.citibanamex.com/actualizacion

¿No reconoces esta actualización? Llámamos



Atención Telefónica (Audiomático)

CDMX, Gdl, Mty: 55 1226 2639
Del interior sin costo: 800 021 2345
EUA y Canadá: 1 800 226 2639
Otro país por cobrar a EUA: 1636 722 6799

Ayúdanos a mantener tus cuentas protegidas

Por seguridad nunca compartas con ningún tercero incluyendo ejecutivos, tu número de cliente y/o contraseña, códigos SMS, información confidencial de tus tarjetas, cuentas o claves de NetKey.

www.citibanamex.com/notificaciones

El Banco Nacional de México®



2023
AÑO DE
Francisco
VILLA

EL REVOLUCIONARIO DEL PUEBLO

Nuevas modalidades de Usurpación de Identidad.



GOBIERNO DE
MÉXICO



A través de fotografías obtenidas en redes sociales, estados o fotos de perfil en diversas aplicaciones o plataformas, las **utilizan para crear nuevos perfiles falsos.**

En redes sociales complementan la farsa, replicando el nombre de usuario utilizado por la víctima.

En mensajería instantánea la línea telefónica es de un número nuevo (desconocido por las víctimas).

Aprovechando el factor sorpresa y situaciones de urgencia e incluso de emergencia, mediante mensajes de texto persuaden a los contactos de las víctimas a realizar depósitos o transferencias bancarias como supuestos préstamos.



Usurpación de Identidad a través del robo de cuenta

A través de la ingeniería social obtienen los códigos de verificación, lo que permite instalar la aplicación de mensajería instantánea en un nuevo dispositivo.

Obtienen el control de la cuenta, por lo que tienen acceso a los contactos.

Familiares, amigos y conocidos, reciben mensajes sobre alguna urgencia laboral e incluso de alguna emergencia familiar, con lo que persuaden a los contactos a realizar depósitos o transferencias bancarias.



GOBIERNO DE
MÉXICO



Usurpación de identidad mediante buzón de voz



GOBIERNO DE
MÉXICO



A través de una mala configuración del Buzón de voz de telefonía móvil, los ciberdelicuentes se aprovechan para tomar el control de las cuentas de mensajería instantánea de sus víctimas y cometer fraudes. Ante ello:

Activa el Doble Factor de Autenticación, para brindar una protección adicional a tus cuentas digitales.

Recuerda desactivar el Buzón de voz, si no lo utilizas.

Comunícate con un asesor de tu compañía telefónica para configurar el buzón de voz con un NIP seguro y cámbialo periódicamente.



Ante una retención de tu tarjeta bancaria en el cajero, te recomendamos:



Antes de introducir tu tarjeta, revisa que el cajero no cuente con dispositivos o aditamentos colocados.

Si la tarjeta es retenida, identifica los números oficiales de la entidad financiera, los delincuentes están utilizando engomados con números telefónicos falsos para que llames y hagan contacto contigo.

A través del engaño simulan levantar un reporte para sustituir tu tarjeta y te piden que uses tu banca móvil para asociarla al nuevo número de tarjeta que está bajo su control.

Si fuiste víctima de un delito en el cajero automático puedes reportarlo en el 088 para recibir asesoría técnica y legal.



GOBIERNO DE
MÉXICO



Servicios financieros en línea



GOBIERNO DE
MÉXICO



GN
GUARDIA
NACIONAL

Antes de solicitar préstamos en Internet, considera:

Verificar la autenticidad y condiciones del servicio.

Abstenerse de realizar depósitos a terceros.

Reportar perfiles o números telefónicos que ofertan falsos créditos.



Servicios financieros en línea



GOBIERNO DE
MÉXICO



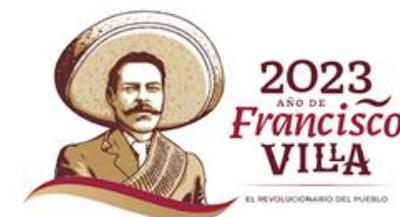
GN
GUARDIA
NACIONAL

Antes de solicitar préstamos a través de plataformas digitales, recuerda:

Verificar que la empresa este registrada ante autoridades competentes y tenga un sitio oficial.

Consultar la reputación de la aplicación o sitio web.

Revisar los permisos de acceso a tu dispositivo que otorgas antes de instalar alguna aplicación.



¿Cómo identificar una página web fraudulenta?



GOBIERNO DE
MÉXICO



Dominio incorrecto

Utilizan el mismo nombre del sitio web oficial con un dominio diferente.

Mala redacción y ortografía,

Algunas veces son producto del uso de traductores, considera que las instituciones o empresas cuidan cada detalle de sus sitios oficiales.

Se requiere para este sitio instalar software en su equipo

https://mitiendaenlínea.uk

Mi tienda en línea



DESCARGA NUESTRA APLICACIÓN

Para realizar tus compras con los mejores descuentos, es por tiempo limitado..

- 1.- **Inztala la App Mi Tienda Premium** en tu compu, table o cel.
- 2.- Regístrate e ingresa los datos de tu tarjeta para agilisar tus compras y nadie te las gane, a través del siguiente link:

www.mitiendaenlinea.com/registro

https://mitienda-enlínea.net/home

Instalación de herramientas adicionales

Argumentando mejorar la navegación, solicita la descarga de programas que resultan dañinos para los dispositivos

Descuentos atractivos

Promociones por debajo de lo normal, demasiado buenos para ser verdad.

Enlaces ocultos o incompletos en su contenido

con la finalidad de ingresar a sitios falsos, los cuales pueden visualizarse al colocar el cursor sobre la liga.



Recomendaciones para evitar un Fraude cibernético.



GOBIERNO DE
MÉXICO



- **Comprar en tiendas oficiales y reconocidas.**
- **Acudir directamente al establecimiento oficial para validar la promoción** sobre el servicio o producto ofertado en internet.
- **Verificar en los sitios oficiales** de las dependencias, los requisitos y formas de pago válidas.
- **Desconfía** de las promociones que sean muy atractivas, recibidas por correo electrónico o como mensajes de texto en tu celular.
- **Utilizar contraseñas seguras y diferentes** para cada servicio, considerando actualizarlas de manera periódica.
- **Activar los sistemas de alerta** de tu banca electrónica para recibir notificaciones de tus movimientos bancarios.
- **Activar el doble factor de autenticación** de las aplicaciones de redes sociales, telefonía móvil y banca en línea.
- Revisar periódicamente los estados de cuenta.



¿Cómo protejo mis dispositivos con acceso a internet?



GOBIERNO DE
MÉXICO



GN
GUARDIA
NACIONAL



Contraseñas seguras



Las contraseñas son la principal defensa contra el acceso no autorizado a los dispositivos de red o los servicios que utilizamos.

Son claves de acceso, difíciles de adivinar por otras personas, aún utilizando aplicaciones para descifrarlas.

Bloqueo de pantalla



Bloquea el uso de aplicaciones y acceso a la información almacenada en los dispositivos informáticos.

- Desbloqueo por patrón
- Huella digital
- Reconocimiento facial
- Contraseñas alfanuméricas



¿Cómo protejo mis dispositivos con acceso a internet?



GOBIERNO DE
MÉXICO



GN
GUARDIA
NACIONAL

Doble Factor de Autenticación

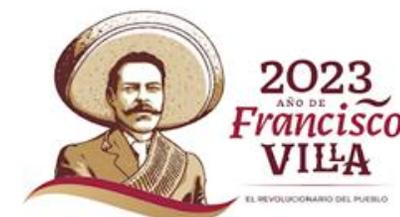


Ayuda a prevenir la suplantación de tu identidad al momento de ingresar a tus cuentas, perfiles o al realizar operaciones financieras.

Antivirus



Ayuda a identificar, bloquear el ingreso y eliminar oportunamente archivos maliciosos que puedan afectar la información que almacenamos o dañar el sistema operativo del dispositivo



¿Cómo crear una contraseña segura?



GOBIERNO DE
MÉXICO



GN
GUARDIA
NACIONAL



1_L0v3+wick3y

Artista Favorito.

v0y*1kRr3r4+

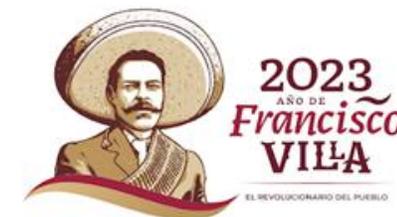
Actividad que mas te gusta.

W4r10_Bn3DtT1

Autor Favorito.

Wy_Pn3r+@_35_536ur@

Oración que más relacione ...



Configuración de seguridad



FACEBOOK



configuración y
privacidad

Seguridad e
inicio de sesión

Autenticación en
dos pasos

TWITTER



Más
opciones

Configuración
y privacidad

Seguridad y
acceso a la
cuenta

Seguridad

Autenticación
en dos fases

TIK TOK



Ajustes y privacidad

Seguridad

Verificación de
2 pasos

INSTAGRAM



Configuración

Seguridad

Autenticación
en dos pasos

HOTMAIL



Configuraciones

Editar
Perfil

Más opciones de
seguridad

Verificación en dos
pasos

GMAIL



Panel de
navegación

Seguridad

Acceso a
Google

Verificación en
dos pasos

TELEGRAM



Ajustes

Privacidad y
seguridad

Verificación en
dos pasos

Al utilizar las redes sociales, considera



GOBIERNO DE
MÉXICO



Terminos y Condiciones de uso



Incluye el tratamiento de la información y el contenido que generen los usuarios para distintos fines e incluso compartirlos con terceros, bajo la protección de los datos personales.

Configuración de la Privacidad



Selección de contenidos (textos, fotos y vídeos) y usuarios pueden interactuar (público, sólo para amistades, sólo un grupo o privado).

Interacciones



Al acceder a una publicación, debemos conocer como las interacciones impactan en nuestro perfil:

- Interactuar

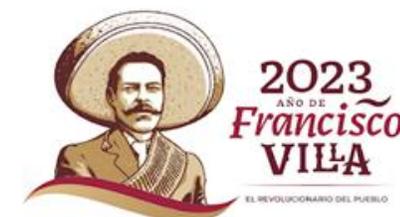


- Comentar
- Compartir

Herramientas de apoyo



Sesiones automáticas
Ubicación de la Publicación
Etiquetado de usuarios y lugares
Datos del sistema operativo o dispositivo de origen de la fotografía o video.



Protege tus dispositivos móviles



GOBIERNO DE
MÉXICO



- **Respalda** de manera periódica la información que almacenas en tus equipos informáticos.
- **Evita** guardar información sensible en el teléfono y si es necesario, utilizar la función para encriptar o cifrar la información.
- **Verifica** qué aplicaciones están instaladas en el celular: desinstalar las aplicaciones que no se usen, porque pueden ser una fuente de vulnerabilidad.



¿Cómo preservar la evidencia digital y presentar tu denuncia?



GOBIERNO DE MÉXICO



La Guardia Nacional te brinda orientación técnica y legal para presentar tu denuncia ante el Ministerio Público ante un delito cibernético.

Ministerio Público
Fiscalía General de la República o
Fiscalías o Procuradurías entidades
federativas



088 | Centro Nacional de Atención Ciudadana



<https://www.facebook.com/XXXXXXX>



CAPTURA DE PANTALLA



Correos electrónicos, mensajes, perfiles, conversaciones, ...

SCREENSHOT



Internet seguro para todas y todos

Consulta las recomendaciones de Ciberseguridad y síguenos a través de las redes sociales de la Guardia Nacional:



Lanzamiento de la Jornada de Ciberseguridad 2022

INTERNET SEGURO PARA TODAS Y TODOS

Únete a las actividades a través de Facebook Live /GUARDIA.NACIONAL.MX

Síguenos #InternetSeguroParaTodasYTodos

La ciudadanía digital es tarea de todas y todos

- Analiza si tus comentarios o publicaciones podrían afectar a alguien.
- Convive y comunícate sin faltar el respeto a los demás.
- Recuerda que tus acciones en el mundo virtual pueden tener consecuencias en la vida real.

¡PONTE EN GUARDIA!

¡Cuidate de los estafadores que intentan engañarte!

- Recuerda que ninguna entidad financiera o página web puede borrar a las personas enlistadas dentro del Buró de Crédito.
- Evita proporcionar datos personales o sensibles, como nombre completo o RFC.
- Descarta realizar depósitos en tiendas de conveniencia como pago para trámites no formales o no reconocidos.

#InternetSeguroParaTodasYTodos

#MexicoContraElCiberFraude

-  @GUARDIA.NACIONAL.MX
-  @GN_MEXICO_
-  @gn_mexico_
-  /GuardiaNacionaldeMexico





GOBIERNO DE
MÉXICO



GN
GUARDIA
NACIONAL

Por su atención
MUCHAS GRACIAS

