PREVENCIÓN DE DELITOS INFORMÁTICOS

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Área Funcional de Ciberdelitos de la Dirección General Científica de la Guardia Nacional

Especializada en la prevención, investigación y persecución de conductas antisociales e ilícitas consumadas por internet y las nuevas tecnologías.

Integrada por elementos con estudios a nivel licenciatura y posgrado, quienes cuentan con entrenamiento y certificaciones internacionales.

Capacidades de la Dirección General Científica en materia de ciberseguridad

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

Delitos contra Niños, Niñas y Adolescentes y Trata de Personas

Prevención e Investigación Pornografía infantil y Trata de Personas en Internet

Alerta AMBER

NCMEC

Operación Ciberguardián

Protección de Infraestructuras críticas de información (CERT-MX)

Ciberseguridad

Protocolo Nacional de Gestión de Incidentes Cibernéticos

Baja de sitios web apócrifos

Análisis de vulnerabilidades

Simulacros Nacionales de ataques Cibernéticos

Asesoría jurídica en gestión de incidentes

Coordinación Nacional de Policías Cibernéticas

Atención de Delitos de alto impacto Ciberinteligencia

Ciberinteligencia I+D

Narcotráfico

Robo de Hidrocarburos

Delincuencia organizada

Inteligencia en Deep y Dark WEB

Tráfico de Armas

Atención a autoridades competentes y Prevención de delitos cibernéticos

Prevención e Investigación Del Cibercrimen

Atención de mandamientos ministeriales y judiciales

Laboratorio de Forense electrónica

Atención ciudadana

Desarrollo de Tecnología en Ciberseguridad

Monitoreo de tendencias en redes sociales

Búsqueda de imágenes

Sistema Chat Cifrado

GUARDIA NACIONAL
JUSTICIA Y PAZ

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Ciberseguridad

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

Riesgos en las TIC

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Ventajas y riesgos en el uso de internet

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL
GN
GUARDIA NACIONAL

Correo electrónico

Búsquedas

Comercio electrónico

Banca electrónica

Descargas

Distribución de SPAM

Información falsa

Fraudes

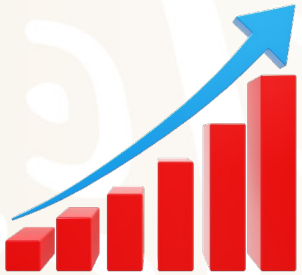
Suplantación de identidad

Códigos maliciosos / Piratería

Las Tecnologías de la Información y Comunicación nos han facilitado y permitido realizar infinidad de actividades instantáneamente, desde cualquier parte mundo. Sin embargo, esta facilidad conlleva responsabilidad para evitar los riesgos asociados a ellas:

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Riesgos en la seguridad de redes sociales



Los riesgos de seguridad en redes sociales no desaparecen, de hecho se incrementan.

Las redes sociales en la actualidad se han convertido en la principal herramienta y plataforma de comunicación a nivel global.

A mayor accesibilidad, mayor riesgo y a mayor riesgo, mayor necesidad de supervisión y control de las redes sociales.

¡Cuidado con lo que compartes!

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

Conductas y ataques en línea facilitados por las TIC.

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Creación, difusión, distribución o intercambio digital de fotografías o videos de naturaleza sexual o íntima sin consentimiento.

Es una forma de violencia que puede ocurrir en una gran variedad de contextos:

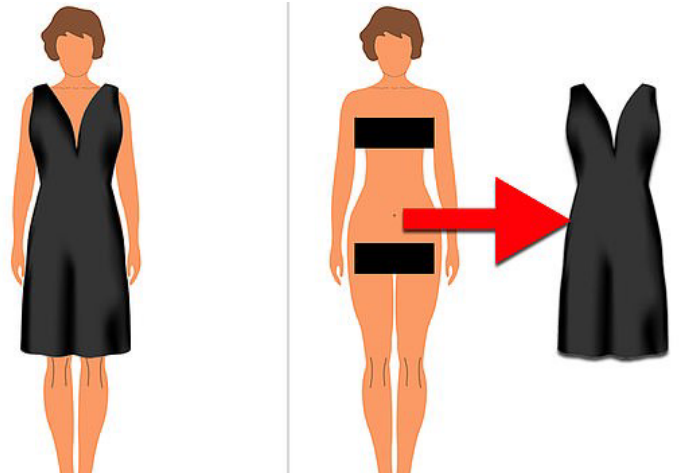
- Sexting: es una práctica que implica la generación e intercambio de material sexualmente explícito y de forma voluntaria por una persona a otra.

Sin embargo, este consentimiento no implica un permiso para almacenar, publicar, reproducir o difundir estos contenidos. Esto es una forma grave de violencia de género.

- Crear imágenes sexualizadas, editadas con fotomontaje, o videos deepfake (falsos).

- Tomar, sin consentimiento, fotografías o videos de partes íntimas del cuerpo de las mujeres en espacios públicos y compartirlos en línea.

- Grabar y distribuir imágenes de abuso sexual.

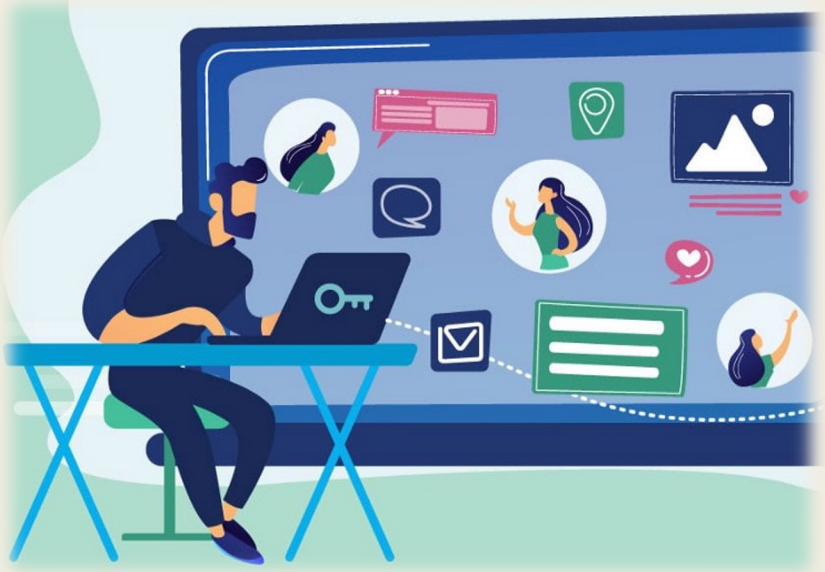


Sextorsión.
Violencia Digital ARTÍCULO 20 Quáter LGAMVLV

Acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta 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.

Doxing o Doxxing

Consiste en la extracción y la publicación no autorizada de información personal, como una forma de intimidación o con la intención de localizar a la persona en “el mundo real” para acosarla, incluso puede ser publicada en sitios pornográficos con el anuncio de que la víctima está ofreciendo servicios sexuales.



Ciberacoso

Es el uso intencional de las TIC para humillar, molestar, atacar, amenazar, alarmar, ofender o insultar a una persona.

Puede estar asociado a otras formas de violencia en línea como por ejemplo el Doxxing.

Puede implicar amenazas.

Suplantación de identidad

Consiste en hacerse pasar por otra persona en línea usando sus datos personales con el fin de amenazarla o intimidarla.

Los datos pueden ser obtenidos mediante la creación de perfiles falsos en redes sociales o la usurpación de cuentas de correo o números de teléfono que puedan ser utilizados para contactar amistades, familiares, colegas o conocidos de la víctima con el propósito de entablar comunicación y tener acceso a información sobre ella.

Grooming

Es una conducta en la cual un adulto se hace pasar por un menor para ponerse en contacto con un niño, niña o adolescente con el fin de ganarse su confianza para luego involucrarle en una actividad sexual.

El adulto suele adaptar el lenguaje a la edad de la víctima con la finalidad de conseguir material íntimo y/o hasta llegar a mantener un encuentro sexual.

Abuso, explotación y/o trata de mujeres y niñas por medio de las tecnologías.

Es el uso de las tecnologías para seleccionar y enganchar mujeres y niñas con fines de abuso sexual o trata.

Técnicas de enganche con fines de explotación:

- Aceptación de amistad a perfiles desconocidos.
- Búsqueda de pareja.
- Enamoramiento.
- Búsqueda de empleo.

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

Técnicas de Ingeniería Social en la economía

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

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

SUSCRIPCIONES GRATUITAS
pueden tener códigos maliciosos

COMUNICADOS FALSOS
solo buscan confundir

CORREOS ALARMANTES
para obtener información personal y financiera

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

SPAM
correos de desconocidos con archivos maliciosos

OFERTAS ATRACTIVAS
suelen ser irreales y pueden derivar robos

PÁGINAS APÓCRIFAS (Phishing)
solicitan donativos o información

Comercio electrónico y banca electrónica

Hoy día, las instituciones bancarias facilitan el acceso a sus servicios a sus clientes, a través de plataformas en línea que permiten realizar operaciones bancarias desde cualquier dispositivo con acceso a internet.

Sin embargo, existen personas que se dedican a suplantar la identidad de las instituciones financieras, con la finalidad de obtener información personal y financiera de los tarjetahabientes, para obtener algún beneficio económico.

Uso seguro de la banca en línea

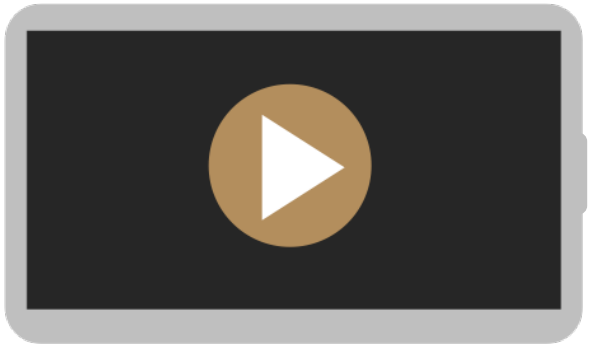
- **Ingresa** desde el sitio oficial de tu banco, no accedas por hipervículos
- **Instala** la aplicación de banca en línea desde tiendas oficiales
- **Desactiva** en el navegador la opción “recordar contraseña”
- **No** abras correos electrónicos o ventanas emergentes (pop up´s)
- **Activa** el servicio de notificaciones vía celular o correo electrónico

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Phishing

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.

¿CÓMO ACTUA EL PHISHING?



Banco General 2014. ¿Qué es el phishing? https://www.youtube.com/watch?v=Z34PbwQtGgk

¿Cómo se visualiza un sitio web apócrifo tipo phishing?

¿Cómo identificar un correo electrónico fraudulento?

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

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.

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

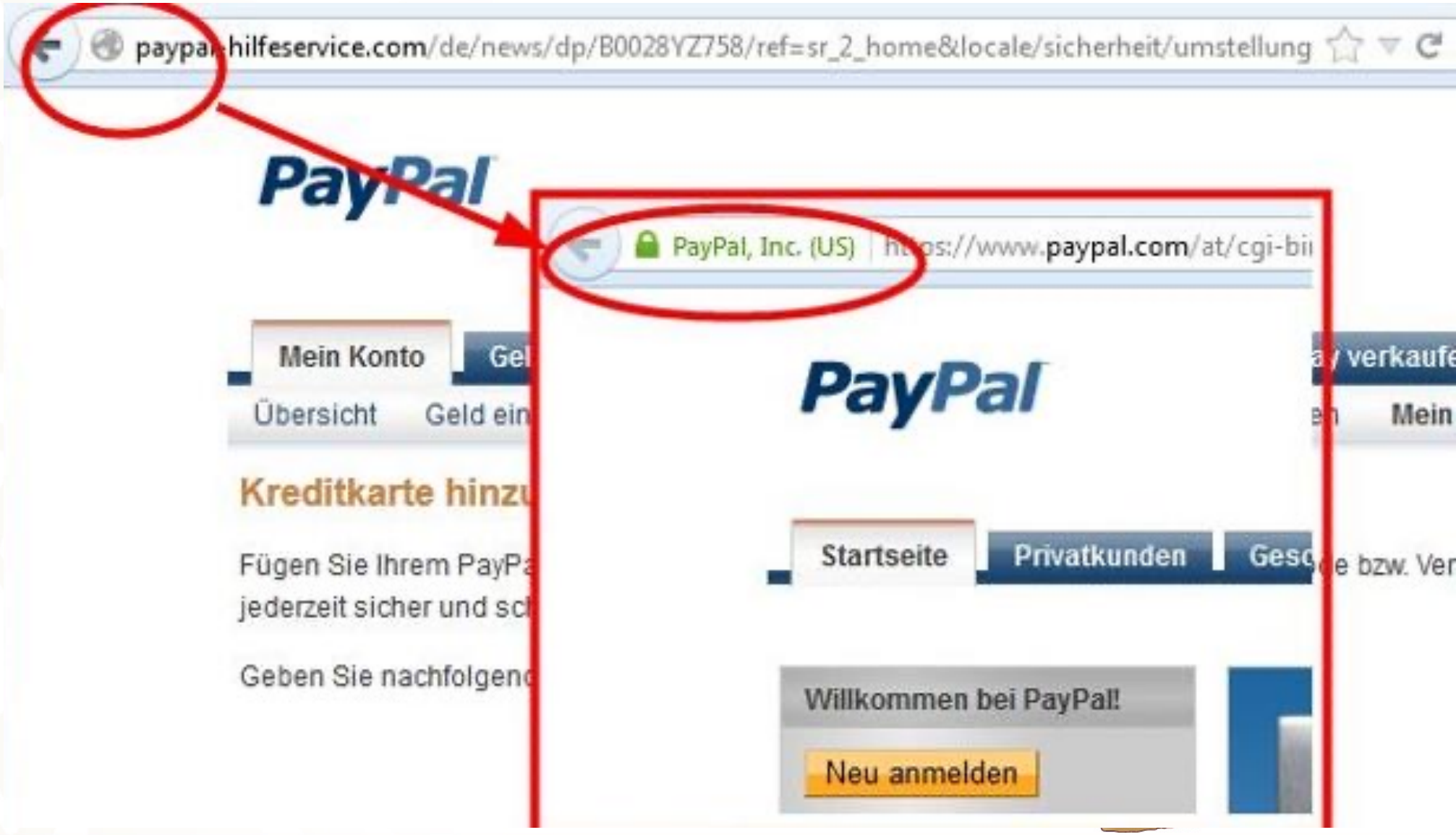
Archivos adjuntos
Pueden contener archivos adjuntos que al descargarse pueden ocasionar daños a los dispositivos con los que accedes a internet.

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.

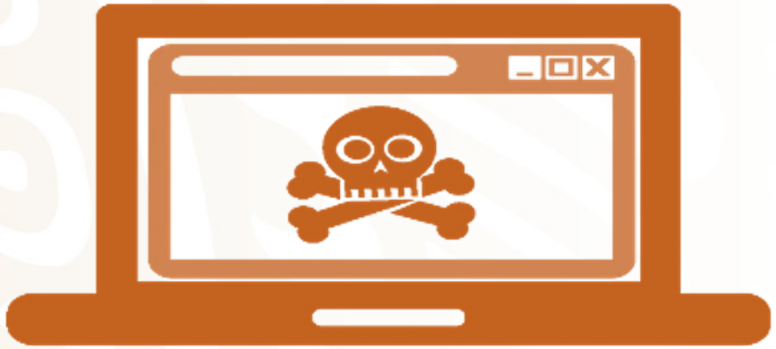
Firma falsa
Puede tratarse de una persona falsa fingiendo un cargo importante en la empresa o institución.

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

¿Cómo se visualiza un sitio web apócrifo tipo phishing?

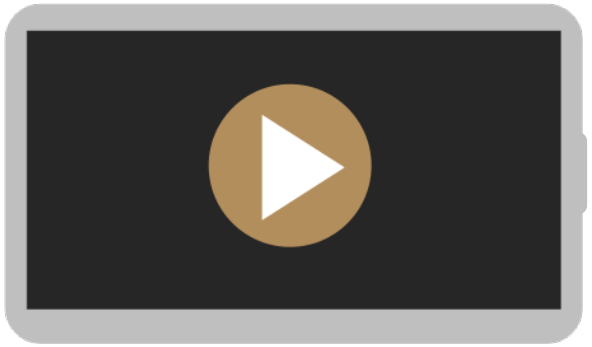


Pharming



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.

¿CÓMO OPERA EL PHARMING?



Doble 2014. “¿Qué es el pharming?” https://www.youtube.com/watch?v=k3b5xzB3dds

¿Cómo se visualiza un correo electrónico fraudulento tipo pharming?

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

Notificaciones SAT <notificaciones@[redacted]>

Anomalías graves en su situación fiscal actual. Último Aviso

To

SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

SAT
Servicio de Administración Tributaria

Último Aviso: 11/04/2016

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 regulariza[illegible]mediato. A continuación le adjuntamos un documento detallad[illegible]al actual.

http://verasmo.com/word.html?d=1223b8c30e3473212996 11f873b449ac
Click to follow link

Descargar Documento

© Derechos Reservados SAT - Servicio de Administración Tributaria

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

¿Cómo identificar una página web fraudulenta?

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.

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.

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

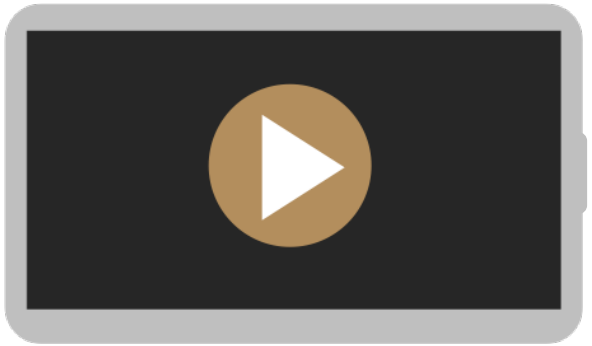
Recomendaciones ante el phishing y pharming

- Mantén actualizado el sistema operativo y antivirus de tus equipos.
- Escribe correctamente la dirección del sitio web que deseas visitar, con ello verificas que la página sea la auténtica, ya que existen páginas falsas con una o dos letras de diferencia.
- Asiste a tu banco para verificar los hechos alarmantes o promociones demasiado atractivas que te llegan por correo electrónico, mensajería instantánea o redes sociales, antes de actuar.
- Evita hacer clic en enlaces que provengan de usuarios desconocidos.
- Nunca entregues tus datos por correo electrónico. Las empresas y bancos jamás solicitarán tus datos financieros o de sus tarjetas de crédito por correo.
- Habilita el doble factor de autenticidad, para reforzar la seguridad de tus cuentas.
- Si crees estar en una situación de riesgo o has sido víctima de algún delito cibernético, asesórate o reporta al 088.

Smishing

Envío de mensajes de texto dirigidos aleatoriamente a los usuarios de telefonía móvil, en los que se difunden ligas electrónicas para acceder a sitios web fraudulentos o números telefónicos reclamar supuestos premios, con la finalidad de solicitar información confidencial a los usuarios, como datos bancarios o contraseñas.

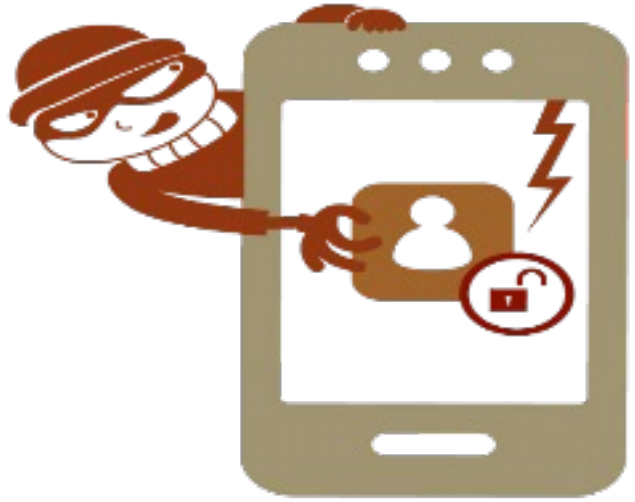
¿Cómo se desarrolla el smishing?



Doble 2014. “CUIDADO CON LA ESTAFA DE "TELCEL" 100 MIL PESOS” https://www.youtube.com/watch?v=_02IaC1RrBI

Vishing

Es una modalidad de estafa a través de llamadas telefónicas, que mediante el uso de grabaciones y la ingeniería social engañan a la personas con la finalidad de obtener su información financiera y robar de identidad.



Los ciberdelincuentes simulan ser empleados de alguna institución financiera y notifican a las personas que situaciones alarmantes como cargos irregulares identificados.

Así mismo, a través de mensajes de texto proporcionan una liga para ingresar a un sitio apócrifo o dirigiéndote a supuesto buzón de voz del sistema financiero con la finalidad de que la víctima proporcione su información financiera, como:

Número telefónico
Nombre y apellidos,
Los 16 dígitos de la tarjeta de crédito,
Fecha de vencimiento,
Clave de seguridad.

Recomendaciones ante el vishing

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL
GN
GUARDIA NACIONAL

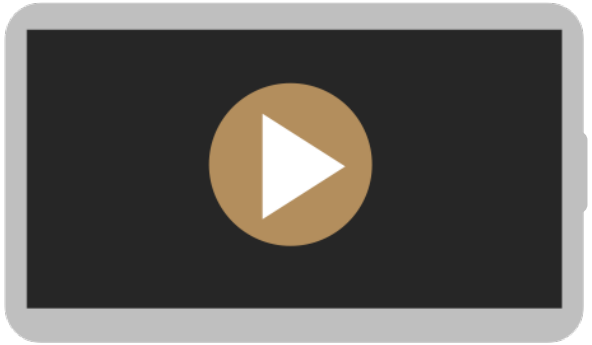
- **Recuerda** siempre verificar por otro medio la información que recibes, antes de actuar.
- **Considera** que ante llamadas alarmantes relativas a tus cuentas o servicios o que adviertan de algún riesgo, contacta a tu banco o proveedor a través de sus números oficiales.
- **Nunca** proporciones datos personales, las instituciones financieras nunca solicitan información financiera mediante llamadas, correos o mensajes.
- **Evita** ingresar a ligas proporcionadas por remitentes desconocidos.
- **Activa** las alertas de movimientos bancarios y revisa periódicamente tus estados de cuenta.
- **Si crees** estar en una situación de riesgo o has sido víctima de algún delito cibernético, asesórate o reporta al 088.

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Fraude nigeriano

Es una modalidad de estafa cibernética a través de correo electrónico, mediante el cual se hacen pasar por personas millonarias argumentando que requieren del apoyo de sus víctimas para compartir su fortuna, a través de un deposito para realizar la gestión de la transacción, debido a las complicaciones políticas para liberar el recurso.

¿Cómo opera el fraude nigeriano?



Animal Político 2020. “Estafa nigeriana: qué es y cómo no ser víctima de este fraude por internet.” https://www.youtube.com/watch?v=75Fq0jMZo0c

Soy la señora Lorena Benzel de Suiza , me casé con difunto Sr. Chresteli Benzel quien fue el principal director ejecutivo de una empresa productora de petróleo y gas en Kuwait durante once años antes de su muerte y desde entonces ningún niño .

Mi difunto marido depositó la suma de $ 4,200,000.00 millones de dólares en una empresa Fimance y Storag en Reino Unido y me aconsejó que él utilizó mi nombre como los familiares ya su amada esposa , y que los funcionarios Fimance y Storag Sociedad no tiene conocimiento de la verdadera contenido de esa caja del tronco porque él depositó como (OBJETOS DE VALOR dE LA FAMILIA y LOS TESOROS) , y sigue siendo con este Fimance y Storag compañía hasta ahora.

Recientemente, mi doctor me dijo que tengo grave enfermedad interna que es el cáncer de riñón , el que más me molesta es mi enfermedad del movimiento . Después de haber conocido mi condición, ahora que tomé esta decisión después de pasado por su perfil ; Oré y decidí compartir con ustedes esta visión . Toma 25 % de la suma total luego distribuir el resto a otras menos privilegios , casas orfanato y algunas iglesias pobres .

Sé que mis aflicciones del tiempo presente no son dignos de ser comparados con la gloria que será revelada a mí en el reino de Dios según el libro de [Romanos 8:18] . Por favor, deje que esto permanezca secreto entre tú y yo.

Tan pronto como recibamos su respuesta en la aceptación de mi donación , te daré la dirección de contacto de este Fimance y Storag Company en Reino Unido con la constancia de depósito de dicho fondo para el reclamo. Rogar por favor siempre a lo largo de su vida y también me recuerden en sus oraciones. Permanezca bendito !

Con la esperanza de recibir su respuesta urgente.

Atentamente en el Señor ,

La señora Lorena Benzel .

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

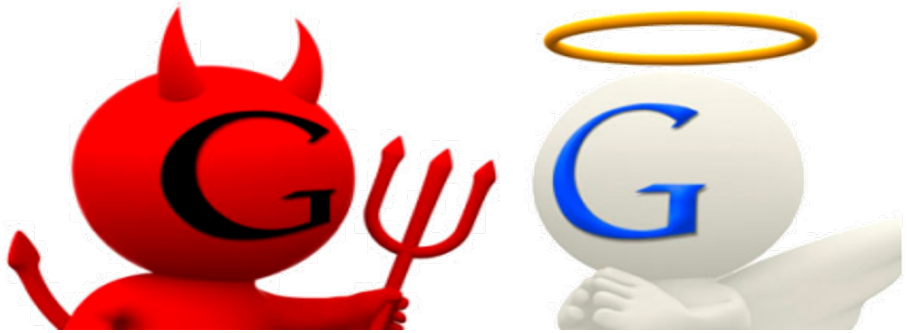
GN
GUARDIA NACIONAL

Ejemplos de correo tipo fraude nigeriano

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Estafa BEC (Business Email Compromise)

Correo electrónico de negocios comprometido



Consiste en tener acceso los correos empresariales y posteriormente cambiarlos por uno muy similar para indicar que los pagos de empresa a proveedores se harán cuentas bancarias distintas.

rickrudolph@germanytools.com

rickrudolph@geermanytools.com

Ejemplos de bec

ING DIRECT

Estimado/a Cliente :

Asunto : Fallo de Identidad,
Remitente : Servicio al cliente

Lamentamos informarle que su cuenta ha sido bloqueada temporalmente en la cartera de ING en linea.
Por su seguridad le rogamos que complete inmediatamente la siguiente verificación de la cuenta.

Para evitar que el acceso se bloquee para siempre.
Haga clic aqui y verifique su identidad bancaria

Así que por su seguridad le pedimos termine la sesión de inmediato.
Para evitar que su acceso sea manejado por personas ajenas a usted

Atentamente,

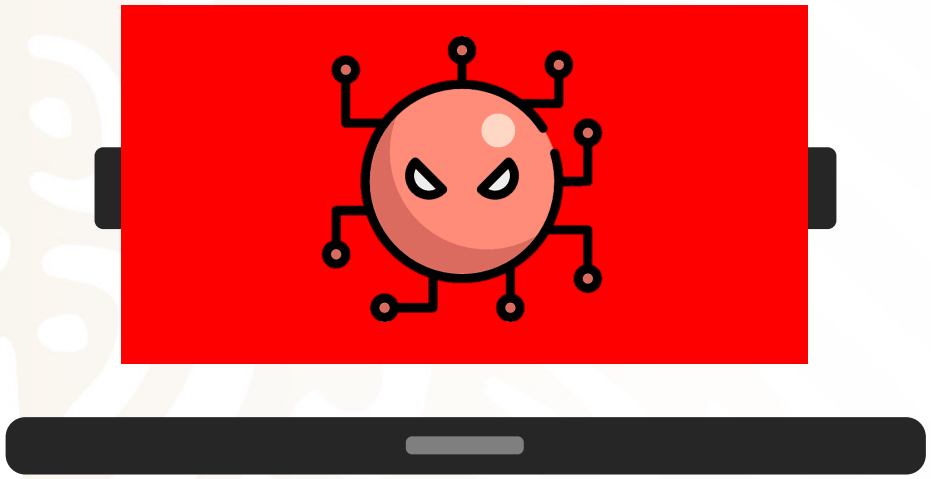
Atención al Cliente de GRUPO ING

Recomendaciones ante el bec

- **Confirmar** con los proveedores todo cambio de cuenta bancaria para realizar sus pagos.
- **Revisar** los códigos fuente de sus correos corporativos.
- **Desconfiar** las solicitudes de pago de proveedores urgentes y con promociones.

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

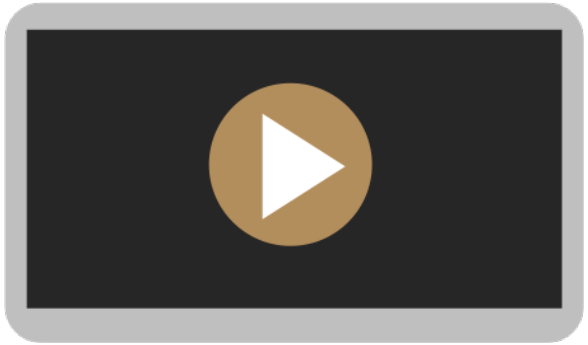
7.3. Ransomware



Son códigos maliciosos diseñados para bloquear el acceso a los dispositivos electrónicos o codificar los archivos contenidos en ellos, para después solicitar a sus víctimas un pago a cambio del "rescate" de su información.

Es una técnica para la comisión de delitos como fraude y extorsión.

¿Cómo opera el ransomware?



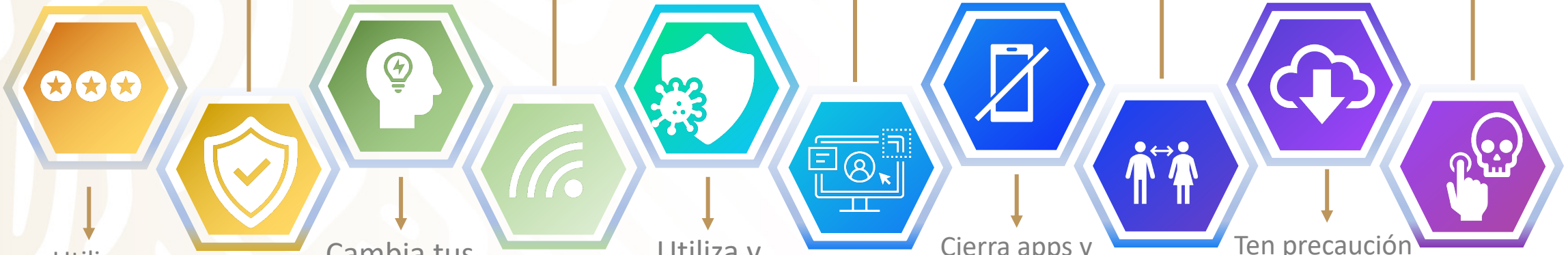
ESET Latinoamérica 2015. "Conoce qué es el ransomware y cómo puedes protegerte!" https://www.youtube.com/watch?v=xpFU4n2iHN8

Recomendaciones

¿ Como proteger tus redes sociales?

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL



Utiliza contraseñas robustas

Activa la verificación de dos pasos

Cambia tus contraseñas de forma periódica

No te conectes a Wifi públicas

Utiliza y actualiza un antivirus para tus dispositivos

Activa la alerta de inicio de sesión

Cierra apps y bloquea las sesiones en tus dispositivos

Cuida tus datos personales

Ten precaución con lo que descargas

Elimina tus cuentas de redes sociales que no utilizas

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

¿Cómo tener una identidad digital responsable?

- **Perfiles responsables.**
  Asegura tus cuentas en los dispositivos y en las redes sociales

- **Adoptar una actitud cívica digital.**
  Participa adecuadamente en la red y genera una convivencia digital sana.

- **Configuración de privacidad.**
  Revisa detenidamente la política de privacidad de cada sitio, ya que en algunos casos el hecho de que borres un contenido no significa que este se elimina de los servidores.

- **Llevar a cabo medidas en la navegación.**
  Actualiza el software regularmente, usa conexiones Wifi protegidas y navega en sitios web seguros

Ejemplo de configuración de seguridad

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

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 dos pasos

INSTAGRAM

Configuración → Seguridad → Autenticación en dos pasos

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Ejemplo de configuración de seguridad

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

TELEGRAM

Ajustes → Privacidad y seguridad → Verificación en dos pasos

GMAIL

Panel de navegación → Seguridad → Acceso a Google → Verificación en dos pasos

HOTMAIL

Configuraciones → Editar Perfil → Más opciones de seguridad → Verificación en dos pasos

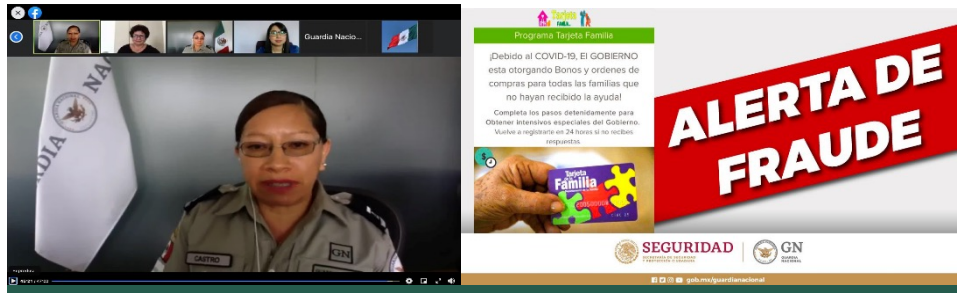
2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Ejemplo de configuración de seguridad.

https://twitter.com/GN_MEXICO_/status/1513167093989998593?t=d__ZoWy0fllRvrydqThkfw&s=08

Síguenos a través de las redes sociales de la Guardia Nacional:

#InternetSeguroParaTodasYTodos



#MexicoContraElCiberFraude

@GUARDIA.NACIONAL.MX

@GN_MEXICO_

@gn_mexico_

/GuardiaNacionaldeMexico

088 | Centro Nacional de Atención Ciudadana

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

Por su atención
MUCHAS GRACIAS

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

GN
GUARDIA NACIONAL

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA