POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa

PLAN NACIONAL MULTIMODAL 2024

Positiva Prevención

Sociedad Colombiana de Medicina del Trabajo

COLOMBIA POTENCIA DE LA VIDA

POSITIVA COMPAÑIA DE SEGUROS | suma 5.0 | educa

10

Comunidad Nacional de Conocimiento para la:

PREVENCIÓN DE RIESGOS PÚBLICOS

El cuidado de sí
suma a tu vida

Sociedad Colombiana de Medicina del Trabajo

COLOMBIA POTENCIA DE LA VIDA

SESIÓN 7:
RIESGO PÚBLICO EN REDES INFORMÁTICAS

Experto Líder:

PAOLA ANDREA RAMIREZ AVILA

Perfil Profesional:

Administradora de empresas, especialista en docencia universitaria, y en gestion del talento humano; magister en dirección de personal y en seguridad y salud en el trabajo. Coach ontológico, tutor virtual de diferentes universidades, conferencista de la Cámara Internacional de Conferencistas.

pararamirez@hotmail.com

3142053053

Ruta del conocimiento

Ruta del conocimiento

Evaluémonos

Positiva Prevención

COLOMBIA POTENCIA DE LA VIDA

NO HAY NADA MÁS REAL QUE LO VIRTUAL Y NADA MÁS VIRTUAL QUE LO REAL

Objetivo general

Socializar los posibles casos de materialización de riesgo público en redes sociales y canales informáticos y reconocer las herramientas para prevenir ser víctima.

Objetivos específicos

Socializar los conceptos de riesgo público

Reconocer las modalidades materialización del riesgo público informático

Conocer diferentes herramientas de prevención de riesgo público informático

QUÉ ES EL RIESGO PÚBLICO?

Acto generado por el hombre, con intención de daño.
Situación asociada a condiciones violentas que se pueden vivir en los espacios públicos, poniendo en riesgo las instalaciones o bienes de las empresas y la integridad física de las personas.
Asociado a los accidentes de tránsito

FACTORES DE RIESGO PÚBLICO

- EXTORSIÓN
- ESTAFA

EXTORSIÓN

Esta tipificado por la ley 599 del año 2000, que afecta al Código Penal colombiano y, en su artículo 244, establece que se comete extorsión **cuando un sujeto constriñe a otro a hacer, tolerar u omitir alguna cosa con el propósito de obtener provecho ilícito para sí o para un tercero.**

El fin principal es doblegar la voluntad de la víctima mediante amenazas, intimidaciones o agresiones.

Incurrirá en prisión de ciento noventa y dos (192) a doscientos ochenta y ocho (288) meses y multa de ochocientos (800) a mil ochocientos (1.800) salarios mínimos legales mensuales vigentes.

ESTAFA

Es un delito patrimonial consistente en emplear el engaño con ánimo de lucro para provocar un error en la víctima, induciéndola a realizar un acto de disposición en perjuicio de sí misma o de un tercero.

Este delito puede ser cometido sobre bienes muebles, bienes inmuebles, derechos y servicios.

El principal bien jurídico protegido en el delito de estafa es el patrimonio, considerándose también protegidos la buena fe y las relaciones de confianza.
El tipo básico del delito de estafa se regula en el artículo 248 del Código Penal, y el artículo 249 recoge supuestos específicos de este delito.
El delito de estafa está sancionado con una pena de prisión de 6 meses a 3 años.

CIBERSEGURIDAD

Conocida como cualquier situación en la que se utilicen indebidamente datos y / o información personal a través de la red o el mundo virtual, para cometer delitos, provocando pérdidas a las víctimas, que pueden ser tanto personas como empresas.

Council on Foreign Relations.
https://cnnespanol.cnn.com/2023/10/09/cuantas-guerras-activas-mundo-orix/

PHISHING

(Suplantación de identidad)

Es un método en el cual los delincuentes se hacen pasar por conocidos de las personas, plataformas de e-commerce o instituciones financieras para robar datos personales y bancarios de sus víctimas.

La estafa consiste en crear un sitio web falso extremadamente similar al de algunas empresas legítimas. A través de mensajes vía correo electrónico, Whatsapp o SMS, los delincuentes envían un enlace, solicitando la confirmación de los datos. Al hacer clic en este enlace, las víctimas son redirigidas al sitio web falso, donde terminan cayendo en la trampa y proporcionando sus datos.

SMISHING

(Suplantación de identidad)

Un ataque de smishing es un tipo de ataque de phishing que aprovecha los mensajes de texto como vector de ataque. Puede basarse en ingeniería social, archivos adjuntos maliciosos y sitios web fraudulentos para estafar a la gente.

Una estafa de smishing puede ser fácil de ejecutar, difícil de rastrear y peligrosa en sus efectos. Un ataque de smishing exitoso puede exponer potencialmente sus contraseñas, fotos, vídeos y otros datos sensibles a un estafador y también funcionar como un vector de infección para una caída de malware en su teléfono inteligente.

ENVÍO DE RECIBOS BANCARIOS FALSOS

Este tipo de fraude cibernético consiste en la creación de recibos falsos en nombre de grandes empresas. Al realizar el pago, la víctima deposita el dinero en la cuenta de los estafadores.

Algunas versiones de este tipo de fraude pueden incluso implicar la creación de páginas falsas que simulan el entorno de la empresa, donde se redirige a las víctimas a descargar el documento falso sin levantar sospechas sobre la estafa.

PHARMING

Consiste en redirigirte a una página de internet falsa mediante ventanas emergentes, para robar tu información.

Suelen mostrar leyendas similares a esta: "¡Felicidades, eres el visitante un millón, haz clic aquí para reclamar tu premio!".

Este tipo de estafa digital puede ocurrir al navegar por sitios web sospechosos o incluso al hacer clic en enlaces recibidos de correos electrónicos poco confiables. En estas situaciones, sin darse cuenta, los usuarios pueden terminar instalando programas maliciosos, que darán acceso a terceros a su información privada, así como datos personales y financieros.

SMISHING

En este tipo de fraude, te envían mensajes SMS (mensajes de texto) a tu teléfono móvil con la finalidad de que visites una página web fraudulenta. Esto con el fin de obtener tu información bancaria, para realizar transacciones en tu nombre.

VISHING

Conocido como phishing telefónico, en donde los delincuentes simulan ser empleados de alguna institución y generalmente te convencen al decirte que tus cuentas están registrando cargos irregulares o que requieren alguna información, evita proporcionarles tus datos y llama directamente a la institución financiera para corroborar la información.

SEXTORSIÓN

La extorsión sexual es un tipo de chantaje que se produce cuando alguien amenaza con compartir o publicar material privado y confidencial a menos que la persona amenazada le envíe imágenes sexualmente explícitas, le preste favores sexuales o le dé dinero. La extorsión sexual es un delito grave, que implica a víctimas engañadas o coaccionadas para enviar imágenes o vídeos personales con contenido sexual.

SABOTAJE INFORMÁTICO

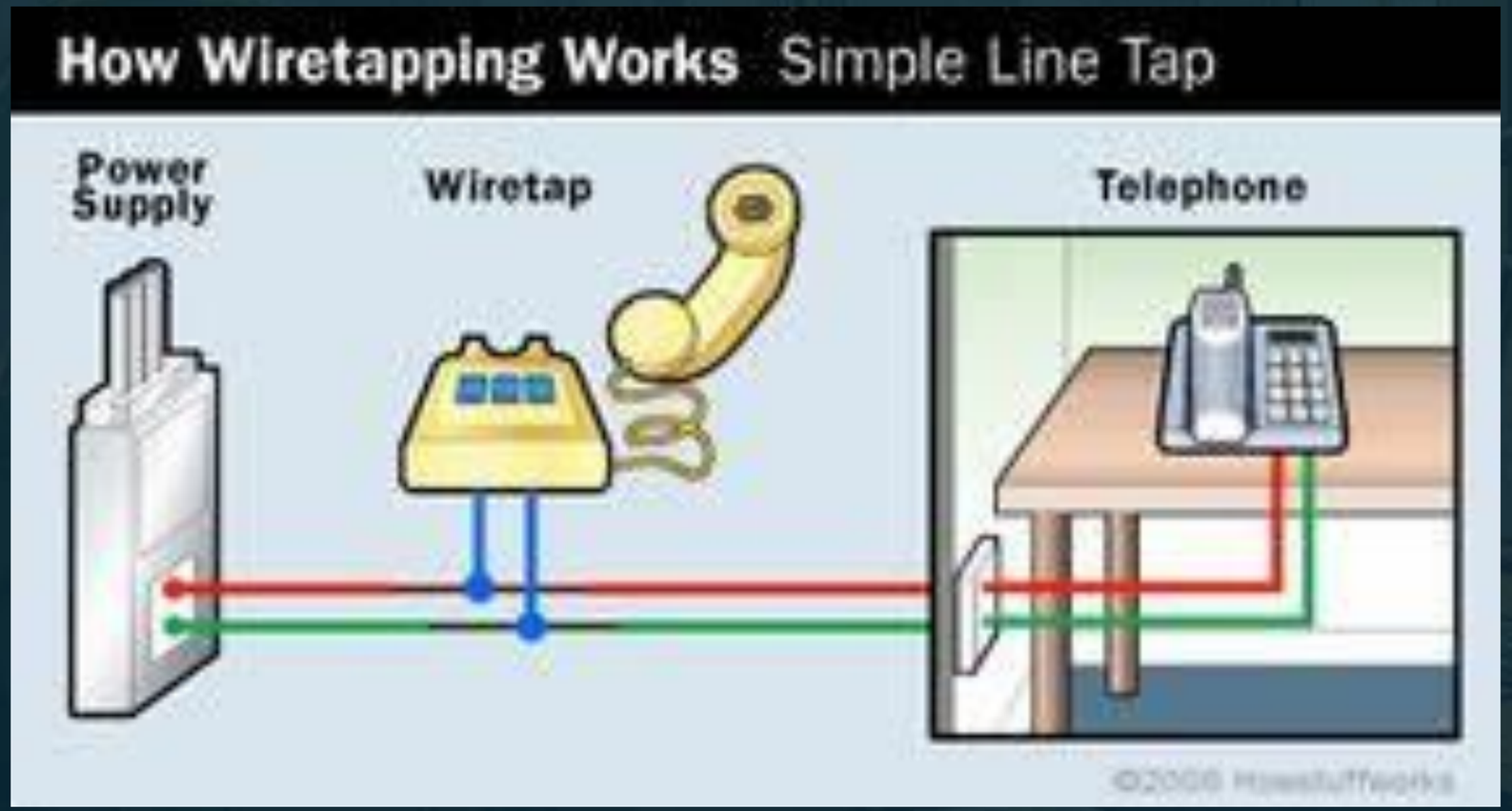
Se trata de aquellos delitos cuyo propósito es alterar, modificar, borrar o suprimir información, programas o archivos de los equipos, a fin de impedir su funcionamiento normal. Se aplican para ello herramientas como los gusanos, las bombas lógicas y malwares.

El sabotaje informático puede incluir delitos tan graves como el ciberterrorismo, que tiene como propósito desestabilizar un país y generar un estado generalizado de conmoción nacional con fines inconfesables..

ESPIONAJE INFORMÁTICO

Este tipo de delito informático tiene como propósito hacer públicos los datos reservados, lo que hace a las empresas y entidades gubernamentales el objetivo ideal de los sujetos activos o delincuentes informáticos.

WIRETAPPING Intercepción de líneas telefónicas



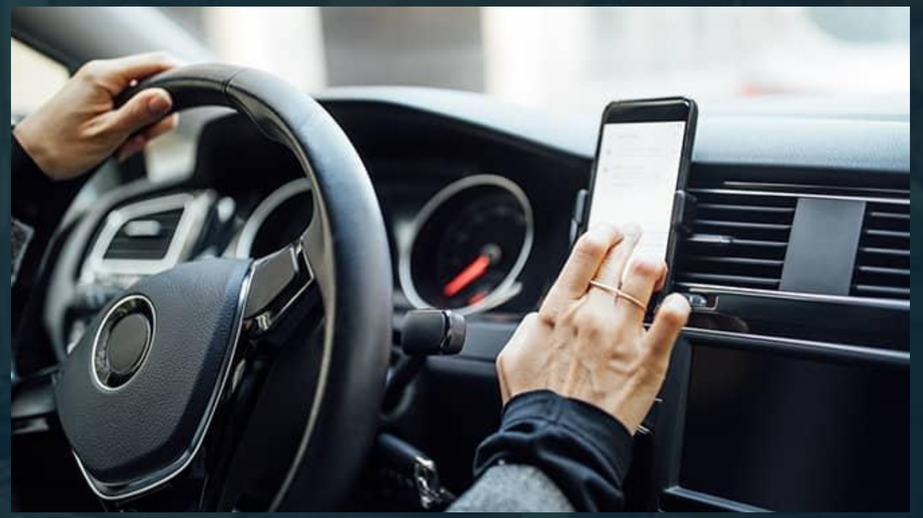
CIBERBULLYING

Acoso virtual, es un acto agresivo e intencionado, llevado a cabo de manera repetida a través del contacto electrónico por parte de un grupo o de un individuo contra una víctima que no puede defenderse fácilmente.

Se trata de un acto reiterativo de acosar, agredir y dañar a otra persona a través de medios telemáticos: internet, telefonía móvil, etc.

WARDRIVING

Tu smartphone a veces te indica que hay una red wireless disponible y te pregunta si deseas conectarte a ella. Esto se debe a que cuando la capacidad inalámbrica de tu smartphone está activada, está constantemente buscando Wi-Fi, por lo que sabe cuándo pasas cerca de una red disponible. En su nivel más básico, eso es wardriving.



Los wardrivers utilizan hardware y software para encontrar señales Wi-Fi en una zona determinada. A menudo, su objetivo es identificar redes vulnerables que puedan explotar.

RANSOMWARE

El ransomware es un tipo de malware que mantiene como rehenes los datos o el dispositivo de la víctima, amenazando con mantenerlos bloqueados, o algo peor, a menos que la víctima pague un rescate al atacante.

SUPLANTACIÓN DE IDENTIDAD

Creación de redes sociales con tu rostro o tu perfil para acceder a información y generar daño.

Creación de cuentas, líneas whatsaap para pedir dinero a familiares o estafar.

IA

Inteligencia artificial que permite crear imágenes, campañas, voz, e información para deteriorar la imagen o crear conflictos amenazantes.

CONSEJOS PARA NAVEGAR SEGUROS POR INTERNET

CÓMO PROTEGERNOS

1. No cliques sobre enlaces sospechosos.
2. Utiliza contraseñas seguras y diferentes para cada uno de tus ámbitos de actividad en internet (cuentas de correo personal, actividades económicas, redes sociales, etc.), cámbialas periódicamente y no las reveles a nadie.
3. No proporciones información confidencial sobre ti a través de ningún canal.
4. Utiliza un único dispositivo para tus transacciones bancarias y comerciales y no introduzcas datos personales o bancarios si tu navegador no reconoce el certificado de la página web que visitas.
5. Aplica la ecuación: solicitud de datos bancarios + datos personales = fraude.
6. Actualiza el sistema operativo, el navegador y el antivirus.
7. No facilites imágenes propias o de otras personas con contenido sexual.
8. Si eres objeto de acoso o abusos a través de las redes sociales pide ayuda a tus familiares y amigos.
9. Si detectas que una persona de tu entorno sufre algún tipo de violencia a través de las redes, ofrécele tu amistad y tu apoyo y anímale a que pida ayuda.
10. Usa el sentido común en tus comunicaciones a través de internet y reflexiona sobre lo que quieres compartir y con quién quieres compartirlo.

CONSEJOS PARA NAVEGAR SEGURO EN INTERNET

1. Utilice únicamente dispositivos de confianza para operaciones bancarias.

2. Verifique que las páginas tengan el símbolo del candado verde para la navegación segura.

3. No responda correos desconocidos que soliciten datos personales.

4. Cambie sus contraseñas periódicamente.

5. Tenga cuidado con los archivos que descarga.

La mejor protección siempre será el sentido común.

¡ALERTA!

CORREO NO DESEADO

La mayoria de estos correos ofrecen dinero de cuentas extranjeras u oportunidades de negocio. Pero su principal objetivo es robar información para suplantar tu identidad.

¡Nunca envies documentos o información personal a este tipo de correos para evitar afectar tu identidad!

¡Cuidado con los archivos adjuntos!

Los cibercriminales pueden ocultar malware en los archivos que recibe por correo electrónico. Tenga en cuenta estas recomendaciones para su seguridad digital:

1. Nunca descargue adjuntos de correos desconocidos.

2. Instale un programa antivirus en los dispositivos que utilice.

3. No ejecute archivos adjuntos con extensión (.exe), suelen traer malware.

Consejos para evitar la suplantación de identidad

1. Denuncie la pérdida de documentos a las autoridades en el menor tiempo posible.

2. Revise las políticas de privacidad de las plataformas digitales que utiliza.

3. Configure contraseñas seguras y active la verificación en dos pasos.

Consejos para mejorar la seguridad de sus contraseñas

1. No utilice las mismas contraseñas en diferentes plataformas.

2. Habilite la autenticación en dos pasos en todas las cuentas.

3. Utilice un gestor de contraseñas para almacenarlas de manera segura.

4. Evite contraseñas de menos de ocho caracteres.

5. Convierta las vocales en números para aumentar la seguridad de las contraseñas.

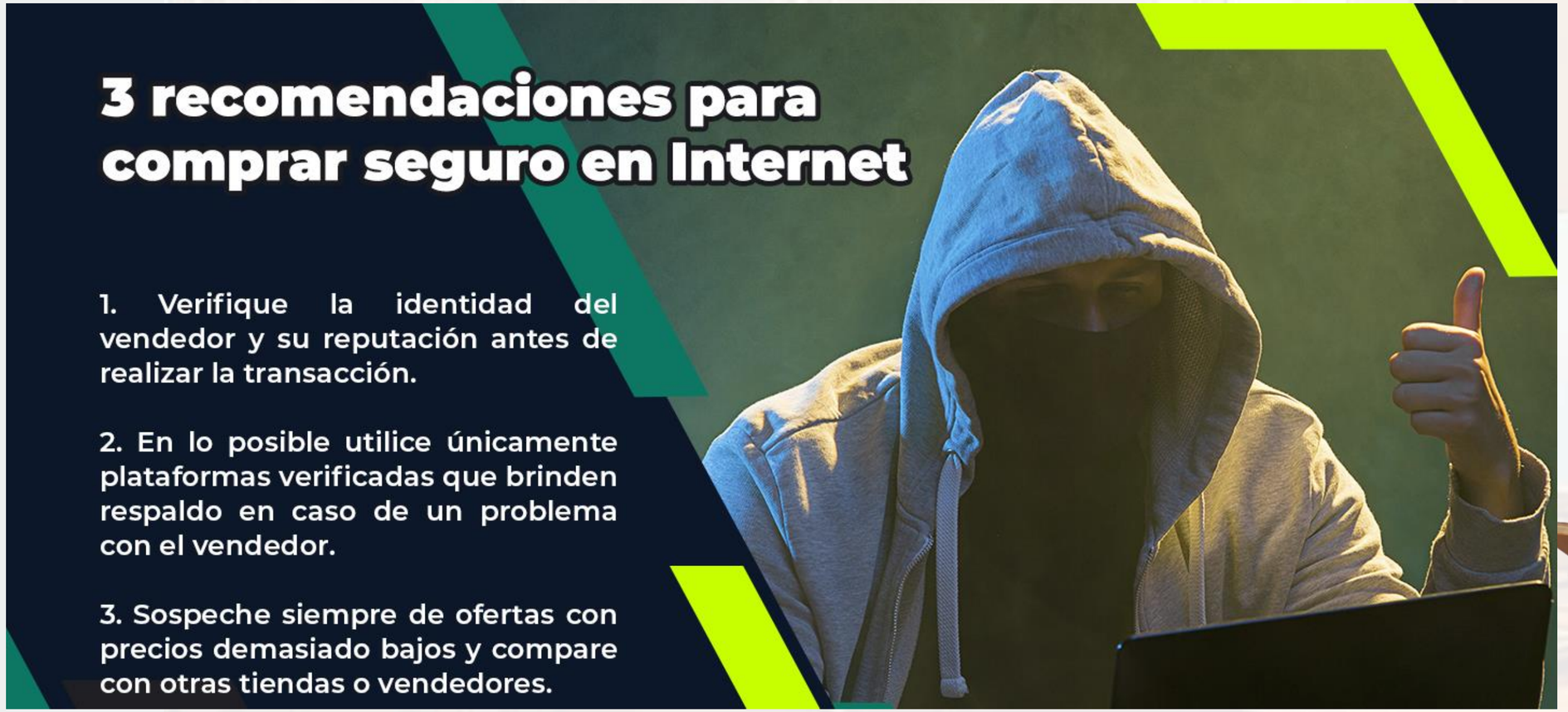
DIOS Y PATRIA
Es un honor ser Policía

3 recomendaciones para comprar seguro en Internet

1. Verifique la identidad del vendedor y su reputación antes de realizar la transacción.

2. En lo posible utilice únicamente plataformas verificadas que brinden respaldo en caso de un problema con el vendedor.

3. Sospeche siempre de ofertas con precios demasiado bajos y compare con otras tiendas o vendedores.



ESTAFAS DE SERVICIO AL CLIENTE
¿CÓMO PROTEGERSE?

¿Cómo funciona?
El cibercriminal crea una cuenta falsa suplantando la imagen de una entidad para atraer víctimas.

¿Cuál es su objetivo?
Que la víctima suministre datos sensibles o descargue alguna aplicación maliciosa en sus dispositivos.

¿Cómo evitarlo?
Siempre verifique que la información de la cuenta, coincida con los datos en otros canales oficiales de la entidad.

DIOS Y PATRIA
Es un honor ser Policía

Su información es valiosa
¿Cómo protegerla?

1. Instale un antivirus en sus dispositivos para detectarlos a tiempo y evitar su ejecución.

2. Mantenga actualizado sus dispositivos y no descargue programas o aplicaciones de páginas desconocidas.

3. Realice una copia de seguridad de su información periódicamente.

4. En lo posible no utilice redes wifi públicas.

¿Qué hacer si recibo amenazas por redes sociales?

1. Si sufre de amenazas, injurias, calumnias, extorsiones o ciberbullying, ¡denuncie!

2. Mantenga la calma y no le siga el juego al ciberdelincuente que quiere intimidarle.

3. Guarde y conserve las conversaciones donde se evidencian las amenazas.

4. Reporte la cuenta en la red social y adjunte todas las evidencias recolectadas.

APRENDE A IDENTIFICAR
EL PHISHING

1. La mayoria de estos correos tienen errores de escritura bastante notables.

2. La pagina web hacia donde lo dirigen para que ingrese sus datos no coincide con la pagina autentica de la entidad.

3. El objetivo de phishing siempre será obtener información, por lo que le pueden pedir:

- Usuarios y contraseñas
- numeros de tarjeta de crédito
- Numeros de cuentas bancarias

Recuerda que ninguna entidad bancaria te solicitara estos datos por correo eléctronico.

Aprenda a identificar el vishing

Las entidades bancarias nunca le solicitarán información sensible sobre sus cuentas. Estas son algunas señales que le deben alertar:

1. Le piden confirmar datos de su tarjeta de crédito, como:
- Número de tarjeta
- Código de seguridad
- Fecha de vencimiento

2. Datos personales que la entidad conoce:
- Dirección de residencia
- Número de cédula
- Correos eletrónicos

ME ESTÁN EXTORSIONANDO CON FOTOS ÍNTIMAS

1. Cuénteselo a alguien de confianza.

2. Evite todo contacto con el cibercriminal.

3. No borre nada y tome evidencias.

4. Realice una denuncia ante las autoridades.

5. Reporte la cuenta del cibercriminal.

Recuerde que la mejor manera de evitar la sextorsión, es no enviando contenido íntimo.


Piense dos veces antes
de hacer clic
Las cadenas de mensajes en WhatsApp pueden ser un peligro para sus datos y la seguridad de su dispositivo. Para evitar ser víctima de estafas:
1. Tenga cuidado con promociones o promesas de regalos que reciba en cadenas.
2. Revise la URL antes de abrirla.
3. No descargue aplicaciones o ingrese datos sensibles si desconoce la procedencia.
4. Evite reenviar estas cadenas con engaños para no viralizarlas.

Consejos para proteger tu cuenta de whatsapp

1. Active la verificación en dos pasos en su cuenta.
2. Proteja su dispositivo con una de las opciones para bloqueo de pantalla.
3. No comparta el código de verificación de su cuenta con nadie.
4. Active las notificaciones de seguridad para mantener su cuenta monitoreada.
5. Configure la copia de seguridad automática de los chats con su cuenta de correo.

UTILIZANDO FACEBOOK DE MANERA SEGURA

1. Nunca divulgue información financiera por chats o publicaciones.

2. No agregue ni acepte solicitudes de amistad de personas que no conoce.

3. Configure factores de recuperación en su cuenta como teléfono y correo.

4. Verifique que solo sus amigos puedan acceder a sus fotografías y publicaciones.

5. Configure las alertas sobre inicios de sesión en dispositivos desconocidos.

CÓMO EVITAR LAS ESTAFAS EN FACEBOOK

Las principales modalidades de estafa que puede encontrarse son:

- Falsos préstamos que solicitan un depósito previo.
- Concursos donde solicitan información bancaria o datos sensibles.
- Falsas donaciones a entidades sin verificar.

Siempre recuerde:

- Nunca envíe dinero por adelantado si no puede comprobar el vendedor y su reputación.
- No comparta documentos o información sensible que pueda comprometer su identidad.

PRINCIPALES PELIGROS EN INSTAGRAM

Sobreexposición

Compartir demasiada información privada como la ubicación en fotografías puede poner en riesgo la integridad física de los usuarios.

Perfiles Falsos

En los entornos digitales es difícil saber quién esta detrás de una fotografía realmente y estas cuentas pueden ser utilizadas para estafas.

Ciberacoso

Los depredadores sexuales están atentos a cualquier víctima, para chantajear o amenazar por este medio a cambio de dinero.

TIPS DE SEGURIDAD PARA SU CUENTA DE INSTAGRAM

Perfil privado

Esta medida permite tener un control total sobre quien puede ver su información.

Opción de "mejores amigos"

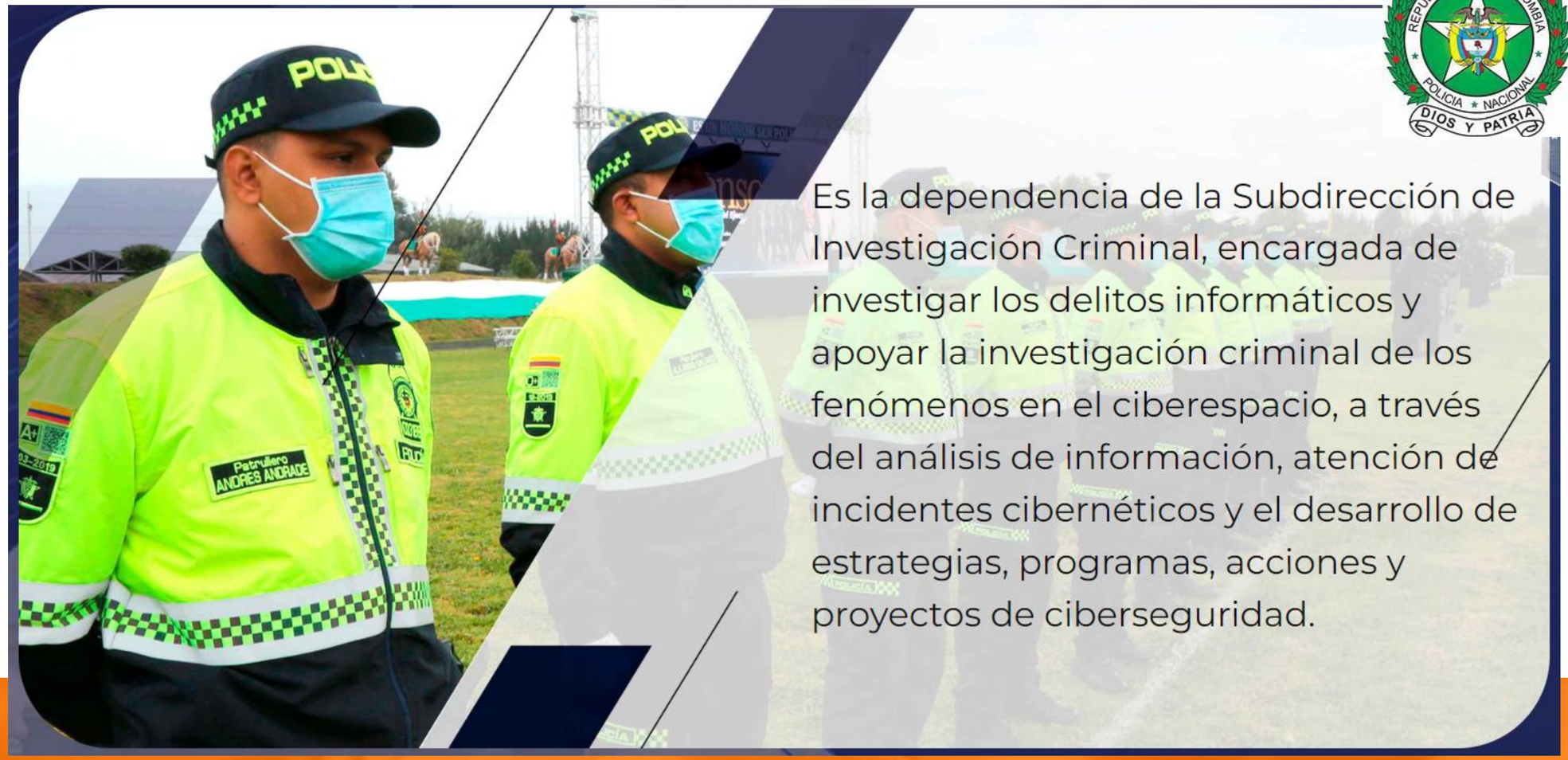
Si tiene el perfil público, esta opción le permite elegir quienes pueden ver sus historias.

Actividad de inicio de sesión

Verifique periódicamente los dispositivos desde donde ha iniciado sesión para evitar accesos no autorizados a su perfil.

Verificación en dos pasos

Evite que terceros tengan acceso a su cuenta, en caso de que cibercriminales obtengan su contraseña.



Es la dependencia de la Subdirección de Investigación Criminal, encargada de investigar los delitos informáticos y apoyar la investigación criminal de los fenómenos en el ciberespacio, a través del análisis de información, atención de incidentes cibernéticos y el desarrollo de estrategias, programas, acciones y proyectos de ciberseguridad.

¿QUIÉN REGULA EL DELITO INFORMATICO?

DIJIN – POLICÍA NACIONAL

RIESGO PÚBLICO EN REDES INFORMÁTICAS

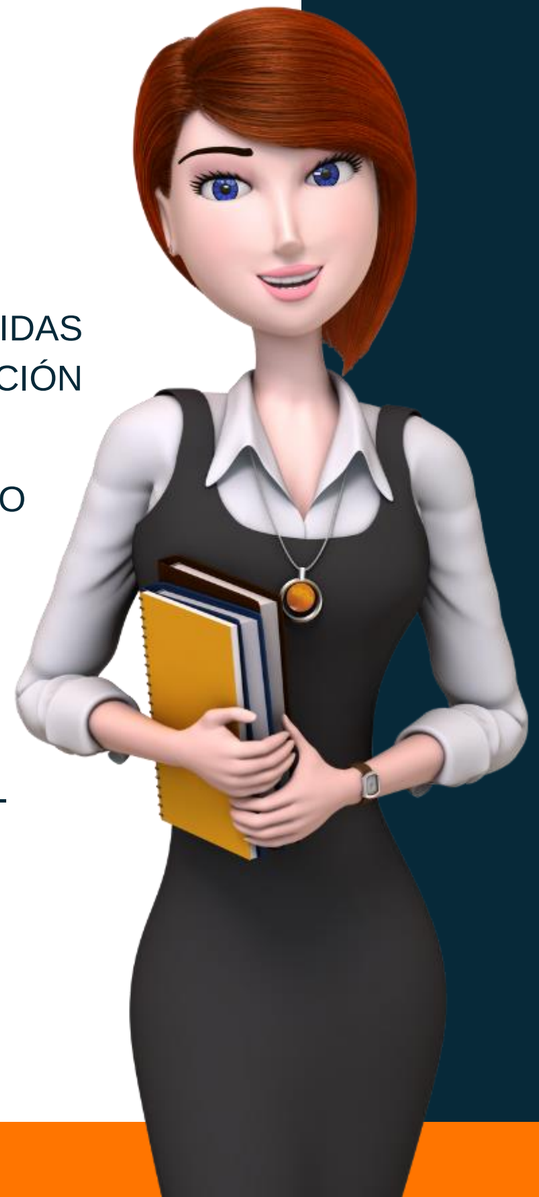
El CAI Virtual, es el primer servicio en Iberoamérica dedicado a la prevención, sensibilización y atención de incidentes cibernéticos, brindando atención policial contra el delito cibernético, el cual ha permitido focalizar la atención al ciudadano, destacando de manera diferencial el servicio online 24/7, orientado a dar respuestas a los diferentes requerimientos reportados por los ciberciudadanos.

¿QUIÉN REGULA EL DELITO INFORMATICO?

https://caivirtual.policia.gov.co/

Bibliografía

- ARL, P. C. (2016). ASISTENCIA TÉCNICA EN EL DISEÑO Y SEGUIMIENTO DE MEDIDAS DE CONTROL PARA EL RIESGO PÚBLICO, SECRETARIA DISTRITAL DE INTEGRACIÓN SOCIAL. Bogotá: Belisario Velasquez SAS.
- MININTERIOR, M. D. (2022). PROTOCOLO PARA EL MANEJO DEL RIESGO PÚBLICO. Bogotá: Ministerio del Interior de Colombia.
- https://expansion.mx/finanzas-personales/2021/11/29/tipos-fraudes-ciberneticos-mexico-como-evitarlos
- https://www.ambitojuridico.com/noticias/penal/penal/estos-cinco-pasos-y-en-este-orden-configuran-el-delito-de-estafa
- https://www.avg.com/es/signal/sextortion
- https://caivirtual.policia.gov.co/



Evaluémonos

Positiva Prevención

COLOMBIA POTENCIA DE LA VIDA

¿Preguntas?

Recuerda que POSITIVA tiene para ti:

Posipedia

https://posipedia.com.co/

- Cursos virtuales
- Artículos
- Audios
- Juegos digitales
- OVAS
- Guías
- Mailings
- Videos

POR MUCHAS CONEXIONES MÁS

Andrés

Despierta todos los días seguro y feliz, porque permanece informado de las noticias y actividades nuevas en SST con su comunidad educativa Positiva Educa en WhatsApp.

1

Escanea el Código QR con tu celular.

2

Síguenos y entérate de todas las actualizaciones de nuestro Plan Nacional de Educación.

3

¡Recuerda!

El canal lo encuentras en la pestaña de Novedades de tu Whatsapp

POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa

¡SÍGUENOS EN NUESTRA COMUNIDAD EDUCATIVA!

Escanea el código QR con tu celular