UNIVERSIDAD
NACIONAL
DE COLOMBIA

PROYECTO **CULTURAL, CIENTÍFICO Y COLECTIVO** DE NACIÓN

Sistema de Gestión de Seguridad de la Información - SGSI

Diciembre de 2023
Dirección Nacional de Estrategia Digital - DNED

Universidad Nacional de Colombia
PROYECTO **CULTURAL, CIENTÍFICO Y COLECTIVO** DE NACIÓN

INGENIERÍA SOCIAL

La Ingeniería social es una técnica que emplean los delincuentes para ganarse la confianza del usuario y conseguir así que haga algo bajo su manipulación y engaño, como puede ser una llamada, un seguimiento a los comportamientos, o o enviar mensajes con el ejecutar un programa malicioso para conseguirsus claves privadas o comprar en sitios web fraudulentos.

¿Qué es el Vishing?

https://www.bing.com/videos/riverview/relatedvideo?q=QUE+ES+EL+VISHING&mid=3A422B1C3B85FB8410AE3A422B1C3B85FB8410AE&FORM=VIRE

Vídeo de Vishing

"C:\Users\User\Downloads\Video_Vishing.jpeg“

TIPS DE SEGURIDAD

- ***¡La era digital llegó para quedarse! ¡No fue sólo en pandemia, ahora es parte nuestra realidad!***
- Según un estudio realizado por la consultora **Gartner**, en 2023, el 25% de la fuerza laboral mundial trabaja de forma remota al menos una parte del tiempo. Esto equivale a **850** millones de personas.

TIPS DE SEGURIDAD

- En Colombia, según el **DANE**, el 5,54% de las personas en Colombia trabajan de forma remota, esto equivale a **2.160.000** personas.
- En Colombia tenemos acceso a internet y redes sociales **38.5 millones**, de las cuales les dedicamos en promedio ***NUEVE HORAS DIARIAS***. Según la ***OCDE***.
- La Policía Nacional, en lo que va de este año ha recibido más de **45.000 denuncias por ataques cibernéticos** y entre las modalidades más comunes **están hurto por medios informáticos y semejantes, acceso abusivo a un siste informático y violación de datos personales**.

¡TODOS SOMOS CIBERSEGURIDAD!

- A mayor número de personas en la red, mayor será el riesgo de exposición de nuestra información.
- Al mismo tiempo somos el eslabón más débil de la cadena.
- De nada servirá tomar las medidas más avanzadas en tecnología sí no hay la consciencia.

¿PARA USTEDES CUÁLES SON LAS EMPRESAS QUE MÁS INVIERTEN EN TECNOLOGIA PARA LA SEGURIDAD DE LA INFORMACIÓN?

TIPS DE SEGURIDAD

Diez síntomas de un posible hackeo de las cuentas

1- Pagos desconocidos: Una primera señal es comenzar a notar cargos adicionales, inapropiados, no autorizados o exagerados en las tarjetas de crédito y débito.

2- Mensajes extraños: Préstele mucha atención a la información que recibe a través de las redes sociales, el correo electrónico o los mensajes de texto que incluyen información sensible o fotos no reveladas públicamente.

3- Acciones que nunca hizo: Llamadas salientes incluyendo voz, facetime y chat.

Diez síntomas de un posible hackeo de las cuentas

4- Usted no lo publicó: Cuando empieza a notar publicaciones en las redes sociales desde su cuenta solicitando un sitio web, nuevas conexiones o amistades, o revelando material inapropiado.

5- Aparición de programas: Cuando ve nuevos dispositivos añadidos a las cuentas de Apple, iCloud, Google o Microsoft Live, Office 365 o en línea.

6- Navegación sospechosa: Redirección en línea a sitios potencialmente maliciosos al especificar sitios web comunes o visitados con frecuencia.

Diez síntomas de un posible hackeo de las cuentas

7- El celular muy lento: Cuando comienza a sentir que es más lento de lo normal el sistema operativo del celular o el computador.

8- Permisos que jamás dio: Intentos de autenticación de dos factores por SMS o de otro tipo que no hayan sido iniciados por usted en ese momento.

9- Batería se agota rápido: El malware y las aplicaciones fraudulentas a veces usan códigos maliciosos que tienden a consumir mucha energía.

10- La cámara: Entra a la galería y se encuentra con fotos y videos que no recuerda haber hecho, o el flash se enciende aparente explicación

PHISHING

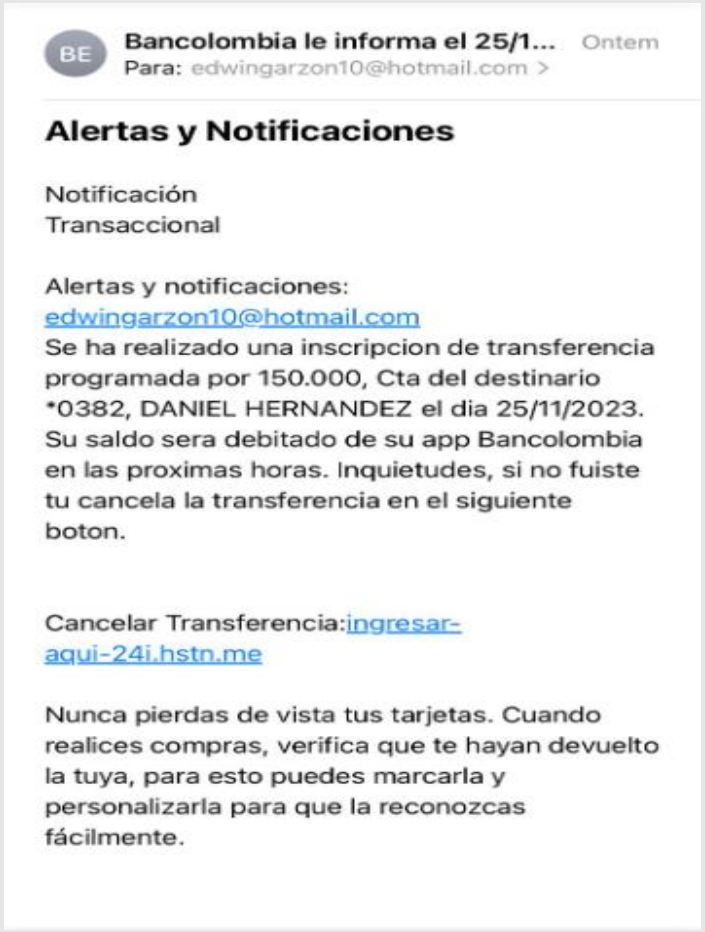
PHISHING

- Se rige por el verbo en ingles ***FISHING***, entendido por **PESCAR**.

- El phishing es una de las técnicas más comunes de ciberataques. ***Consiste en engañar a las víctimas para que revelen información personal o confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios.***

- **Los ataques de phishing pueden realizarse a través de diferentes canales, como correo electrónico, SMS, redes sociales o aplicaciones de mensajería.** Los atacantes suelen utilizar técnicas de ***ingeniería social*** para engañar a las víctimas, como crear correos electrónicos o mensajes que ***parezcan*** legítimos.

NO CAIGA



BE **Bancolombia le informa el 25/1...** Ontem
Para: edwingarzon10@hotmail.com >

Alertas y Notificaciones

Notificación
Transaccional

Alertas y notificaciones:
edwingarzon10@hotmail.com
Se ha realizado una inscripcion de transferencia programada por 150.000, Cta del destinario *0382, DANIEL HERNANDEZ el dia 25/11/2023. Su saldo sera debitado de su app Bancolombia en las proximas horas. Inquietudes, si no fuiste tu cancela la transferencia en el siguiente boton.

Cancelar Transferencia:ingresar-aqui-24i.hstn.me

Nunca pierdas de vista tus tarjetas. Cuando realices compras, verifica que te hayan devuelto la tuya, para esto puedes marcarla y personalizarla para que la reconozcas fácilmente.

NO CAIGA

VD **Validar Clave Dinamica-bancol...** Ontem
Para: edwingarzon10@hotmail.com >

Validar Clave Dinamica

Importante

Bancolombia

Registro de Dispositivo
Estimado; edwingarzon10@hotmail.com

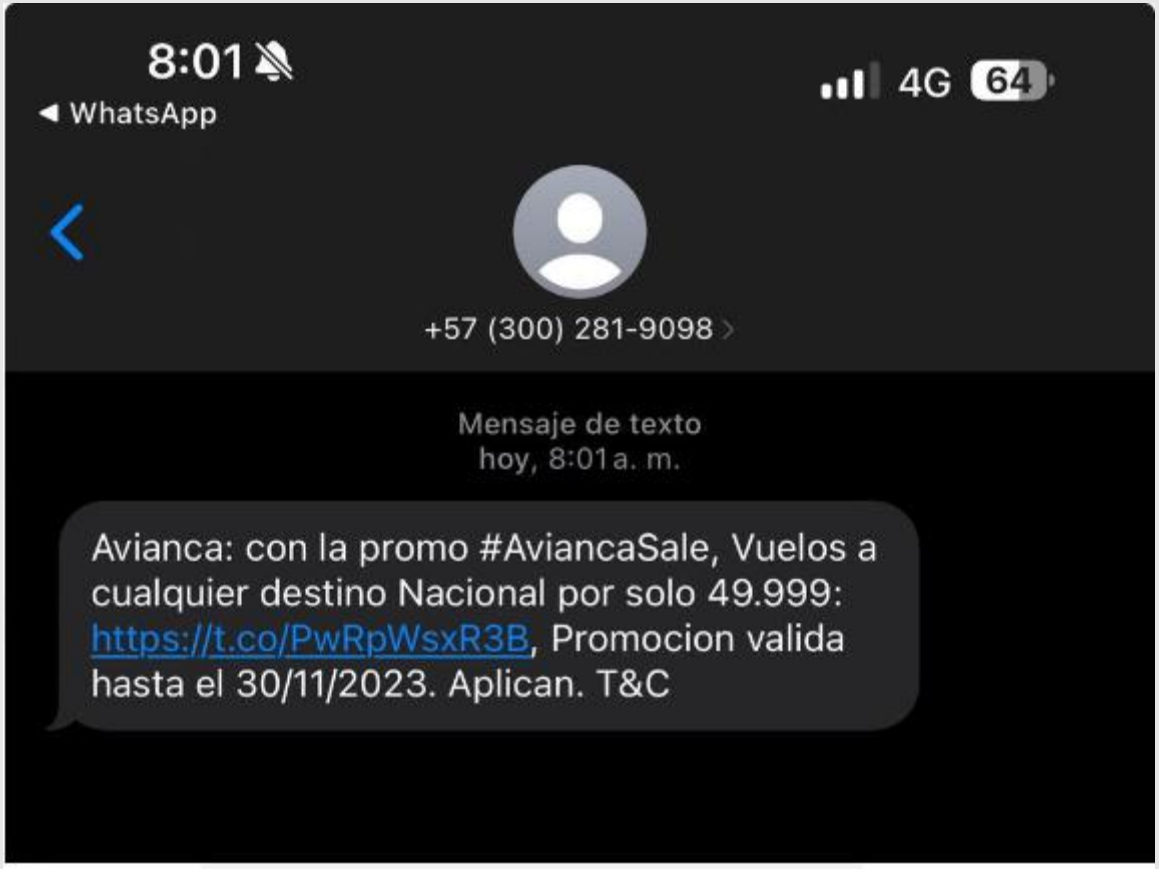
Estimado(a) Cliente: Bancolombia: Notamos un movimiento sospechoso realizado en nuestros canales digitales de otro dispositivo no registrado. Dispositivo (iPhone 13 pro) -Navegador safari Dirección IP: 181.59.3.100 debido a dicho acceso, bloqueamos tu Clave Dinámica el 25/11/2023. si no a sido usted dirijase al siguiente enlace virtual.

Si no fue usted proteja su cuenta en el siguiente enlace de:

(cancelaestacompra.0hi.me)

Recuerde el cuidado especial de tu información de acceso, misma que por ningún motivo debe ser

NO CAIGA


8:01
WhatsApp
4G
64
+57 (300) 281-9098
Mensaje de texto
hoy, 8:01 a. m.
Avianca: con la promo #AviancaSale, Vuelos a cualquier destino Nacional por solo 49.999: https://t.co/PwRpWsxR3B, Promocion valida hasta el 30/11/2023. Aplican. T&C

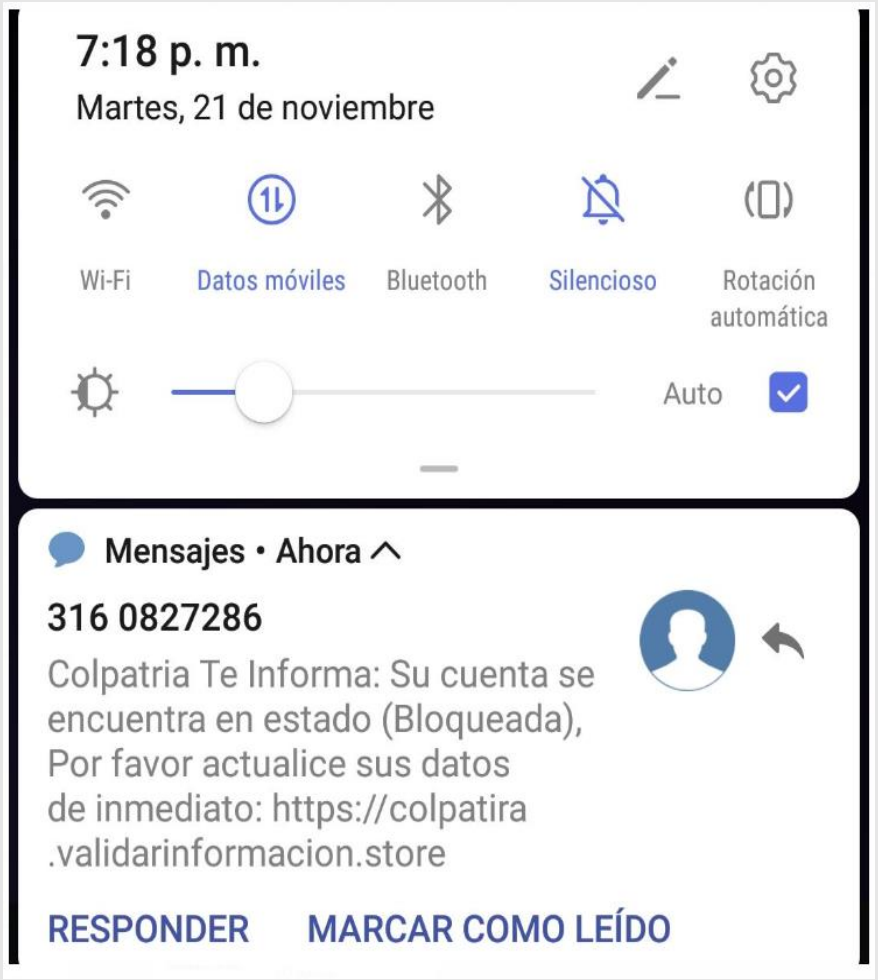
NO CAIGA


6:01
+57 (316) 064-6469
Mensaje de texto
hoy, 2:04 p. m.
Apreciado(a) CLIENTE Colpatria notifica se ha generado un bloqueo preventivo, siga instruciones para su desbloqueo https://colpatira.validarinformacion.info/

NO CAIGA


3182050843
Añadir a contactos
Bloquear número
miércoles, 22 de noviembre de 2023
Paola te envio $85000 por TRANSFIYA acepta aqui:https://yep.pt/iYGPP
9:00 p. m.

NO CAIGA


7:18 p. m.
Martes, 21 de noviembre
Wi-Fi
Datos móviles
Bluetooth
Silencioso
Rotación automática
Auto
Mensajes • Ahora
316 0827286
Colpatria Te Informa: Su cuenta se encuentra en estado (Bloqueada), Por favor actualice sus datos de inmediato: https://colpatira .validarinformacion.store
RESPONDER
MARCAR COMO LEÍDO

NO CAIGA


Entra a tu Nequi
Podrás bloquear tu nequi, consultar tus datos
+57
Número de celular
Contraseña
No soy un robot
reCAPTCHA
Privacidad - Términos
Enviar

Consejos para evitar se utilice correo corporativo en redes sociales

- **Conoce las políticas de uso:** Familiarícese con las políticas de la universidad sobre el uso del correo corporativo y las redes sociales.
- **Utiliza una cuenta de correo personal:** Configura una cuenta de correo electrónico personal para sus actividades en redes sociales u otros asuntos personales.
- **No mezcles información personal y profesional:** Evita utilizar el correo corporativo para registrarse en redes sociales o cuentas personales.
- **Mantenga la seguridad de sus contraseñas:** Utiliza contraseñas fuertes y únicas para tus cuentas personales en redes sociales.

Consejos para evitar se utilice correo corporativo en redes sociales

- **Sea consciente de los riesgos de seguridad:** Comprenda los riesgos asociados con el uso del correo corporativo para actividades personales en línea.
- **Evite el acceso desde dispositivos de trabajo:** Utilice sus propios dispositivos personales para acceder a las cuentas de redes sociales.
- **Protege su privacidad en redes sociales:** Configure adecuadamente las opciones de privacidad en tus cuentas de redes sociales para mantener la información personal segura.
- **Mantenga la confidencialidad de la información corporativa:** Recuerde que el correo corporativo es propiedad de la institución y puede ser monitoreado por razones de seguridad y cumplimiento.
- **Consulta las dudas con la Mesa de Servicio**: Si tienes dudas o preguntas sobre las políticas de uso del correo corporativo o las redes sociales, contacta a gestionti_nal@unal.edu.co.

TIPS PARA NO CAER EN CORREOS INTERNOS ILEGÍTIMOS DE LA INSTITUCIÓN

- **Verifica el remitente.**
- **Examina la redacción y el estilo.**
- **No reveles información confidencial.**
- **Confirma la solicitud por otros medios.**
- **No hagas clic en enlaces o descargues archivos adjuntos sospechosos.**

¿CÓMO PUEDO PROTEGER MI CUENTA DE WHATSAPP?

VERIFICACIÓN EN DOS PASOS

La verificación en dos pasos es una función opcional que añade seguridad a tu cuenta de WhatsApp. Verás la pantalla de verificación en dos pasos después de registrar correctamente tu número de teléfono en WhatsApp.

Información acerca de la verificación en dos pasos | Servicio de ayuda de WhatsApp

Gracias

Universidad Nacional de Colombia

PROYECTO **CULTURAL, CIENTÍFICO Y COLECTIVO** DE NACIÓN

UNIVERSIDAD
NACIONAL
DE COLOMBIA

PROYECTO **CULTURAL, CIENTÍFICO Y COLECTIVO** DE NACIÓN

Sistema de Gestión de Seguridad de la Información - SGSI

Diciembre de 2023
Dirección Nacional de Estrategia Digital - DNED

Universidad Nacional de Colombia
PROYECTO **CULTURAL, CIENTÍFICO Y COLECTIVO** DE NACIÓN

MAL-WARE

La palabra malware viene del inglés y es el resultado de la unión de las palabras **MAL**icious soft**WARE** o software malicioso.

TIPOS DE MALWARE

TIPOS DE MALWARE

- **Ransomware**: Un malware que secuestra los datos de su computador bloqueándolo, y pidiendo un rescate económico a cambio de recuperarlos.
- **Spyware**: Un malware que también se instala en tu equipo por sí sólo o mediante la interacción de una segunda aplicación que lo lanza sin que te des cuenta. Ejemplo: **Keylogger** (registrador de teclas): capta las pulsaciones de teclas mientras el usuario escribe y se usa frecuentemente para robar credenciales, como nombres de usuario y contraseñas

TIPOS DE MALWARE

- **Adware**: Una aplicación en la frontera del malware, porque no siempre es dañino para el ordenador. Su única misión es la de meterse en el computador y empezar a mostrar publicidad, ya sea mientras estás navegando por internet, a forma de **popup.**

- **Gusano informático**: Este malware no necesita de la intervención del usuario ni modificar ningún archivo existente, y también puede replicarse a sí mismo y enviar copias a otros equipos conectados a ese en el que están o que estén en su lista de contactos.

- **Troyano**: Es un malware que va dentro de un programa legítimo o disfrazado de él para introducirse en tu equipo como si usara un Caballo de Troya, de ahí su nombre.

- **Las redes de robots o botnets se apodera de un computador y lo agrega a una red de** otros sistemas secuestrados para enviar campañas de spam a gran escala.

¿CÓMO PUEDO EVITAR EL MALWARE?

Mantener actualizado el sistema operativo

Uno de los principales consejos para prevenir las infecciones de malware es mantener su sistema operativo siempre actualizado.

No abra archivos adjuntos provenientes de fuentes desconocidas o sospechosas

Los archivos adjuntos a los mensajes de correo electrónico son una de las vías favoritas de infección de muchos tipos de virus.

Evita realizar descargas desde redes P2P o de uso compartido de archivos

Las redes de bots utilizan redes P2P y servicios de uso compartido de archivos para infectar equipos.

No hagas clic en enlaces sospechosos

Los enlaces a sitios web maliciosos son una vía frecuente de infección. Así que evita hacer clic sobre ellos a menos que los inspecciones cuidadosamente.

TIPS PARA RECONOCER URL SOSPECHOSAS CON EL FIN DE NO CAER EN CORREOS MALICIOSOS

- **Verifica la autenticidad del dominio:** Observa cuidadosamente el dominio en la URL. Los dominios legítimos suelen ser reconocibles y estar relacionados con la empresa o la organización.
- **Examina la estructura de la dirección de la URL:** Presta atención a la estructura de la URL. Los dominios legítimos suelen tener una estructura coherente, mientras que las URL sospechosas pueden tener segmentos aleatorios, cadenas de caracteres sin sentido o subdominios desconocidos.
- **Comprueba la presencia de "https":** Verifica si la URL comienza con "https://" en lugar de solo "http://". El "https" indica una conexión segura y encriptada, lo cual es importante para proteger la información confidencial.

TIPS PARA RECONOCER URL SOSPECHOSAS CON EL FIN DE NO CAER EN CORREOS MALICIOSOS

- **Ten cuidado con las direcciones cortadas**: Las URL acortadas pueden ocultar la dirección real del sitio web. Si recibes una URL acortada en un correo electrónico o mensaje.
- **No confíes en enlaces incrustados en correos electrónicos no solicitados:** Evita hacer clic en enlaces directamente desde correos electrónicos no solicitados o sospechosos.
- **Busca indicios de phishing en la dirección:** Examina la URL en busca de posibles indicios de phishing, como palabras clave engañosas, errores de ortografía o adiciones sospechosas.
- **Confirma la autenticidad del sitio web de forma independiente:** Si tienes dudas sobre la autenticidad de una URL, verifica la legitimidad del sitio web de forma independiente.
- Sucursal Virtual Empresas (bancolombia.com)
- }}

CÓMO ACTIVAR EL FIREWALL PARA PONER MÁS SEGURIDAD A MI COMPUTADOR

- Un firewall es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada.
- Los firewalls pueden considerarse fronteras o puertas que administran el flujo de la actividad web que se permite o prohíbe en una red privada. El término proviene del concepto de **paredes físicas que actúan como barreras para ralentizar la propagación del fuego hasta que los servicios de emergencia pueden extinguirlo**. En comparación, los firewalls de seguridad de red sirven para la administración del tráfico web y normalmente están destinados a ralentizar la propagación de las amenazas web.

CÓMO ACTIVAR EL FIREWALL PARA PONER MÁS SEGURIDAD A MI COMPUTADOR

- Confirma que el firewall de Windows está activado.
- Consulta Activar o desactivar el Firewall de Microsoft Defender para obtener instrucciones sobre cómo hacerlo en las versiones modernas de Windows
- https://support.microsoft.com/es-es/windows/activar-o-desactivar-el-firewall-de-microsoft-defender-ec0844f7-aebd-0583-67fe-601ecf5d774f

Gracias

Universidad Nacional de Colombia

PROYECTO **CULTURAL, CIENTÍFICO Y COLECTIVO** DE NACIÓN