2FA

DOBLE FACTOR DE AUTENTICACION

VERIFICACION EN DOS PASOS.

Validar el acceso de forma segura a dispositivos y aplicaciones.

¿ COMO FUNCIONA EL 2FA PARA MITIGAR ATAQUES?

1. Usuario ingresa contraseña de acceso.
2. Sistema valida credencial y envía un 2FA (TOKEN)
3. Usuario valida el token en su dispositivo móvil
4. Usuario ingresa el token en el sistema se permite el acceso.

Para mitigar que tu cuenta sea interceptada:

Emplea una contraseña preterminada y un código de seguridad. I CONOCIMIENTO I

Conecta tu dispositivo móvil con la cuenta para generar un token. I POSESIÓN I

Utilice su huella dactilar o reconocimiento facial . I DISTINCIÓN I

Use preguntas y respuesta de seguridad. I CONOCIMIENTO I

II INTENTO DE ACCESO POR UN CIBERDELICUENTE II

Ciberdelicuente roba contraseña utilizando una amaneza informatica. → Ingresa la credencial hackeada e intenta acceder al sistema. → El sistema solicita el segundo factor de autenticación. → Atacante no tiene acceso al segundo código y se prohíbe el acceso. → **SEGURO**

ICS Instituto de Ciberseguridad

Capacitación y entrenamiento real

#ICS #InstitutoDeCiberseguridad

"Mi hijo me comentó que, cuando estaba jugando en su ordenador, alguien le había enviado un mensaje al móvil amenazándolo con publicar en Internet unas fotos comprometedoras suyas si no pagaba una cantidad de dinero en menos de 24 horas.

En dicho mensaje se detallaba cómo habían obtenido sus fotos y cómo pensaban extorsionarle si no accedía a las peticiones."

¿Cómo nos afectaría?

Este tipo de extorsión **consiste en chantajearnos con la publicación de fotos, vídeos** o información íntima de nosotros, si no pagamos. En la mayoría de casos, **no tienen nada, pero se sirven del miedo y el desconocimiento** para engañarnos.

No revelar información

Seremos cuidadosos con quién compartimos nuestra información personal, como fotos o vídeos.

Mantener la calma

Lo primero es no alarmarnos ya que puede tratarse de un engaño, y que no tengan los archivos que dicen tener.

Recomendaciones "Buenas prácticas del cibernauta"

Desconectar webcam y micrófono

Si no estamos utilizando la cámara u otros dispositivos de audio como el micrófono, es mejor desconectarlos. Tampoco es recomendable que permitamos que cualquier app tengan acceso a la cámara del dispositivo.

OFF

No abrir archivos adjuntos

Si recibimos correos dudosos, no abriremos los archivos adjuntos, ya que podrán contener algún tipo de malware.

$ No enviar dinero

Realizar un pago no garantiza que no sigan extorsionándonos. Es más, estaremos favoreciendo este tipo de prácticas.

Enlaces relacionados

- ¿Buscas pareja por Internet? ¡Ten cuidado!
- Detectada una estafa a través de correo electrónico extorsionando con supuestas imágenes de contenido sexual
- Cuidado con las sesiones de fotos

OSI Oficina de Seguridad del Internauta

EUROPOL

Ciberseguridad con niños

CÓMO HACER DE TU HOGAR UN CIBER LUGAR SEGURO

Cambia la **contraseña** predeterminada de fábrica y mantén el software actualizado

Revisa la **seguridad** y la **privacidad** de los juguetes inteligentes

Habla con tus hijos sobre ciberseguridad. **Escucha** sus experiencias online y **explícales** la importancia de estar tan seguros online como offline

Usa el **control parental** para salvaguardar la actividad online de tus hijos

RECUERDA

Sigue fuentes oficiales para obtener información actualizada. Si llegas a ser víctima de un ciberdelito, comunícalo siempre a la Guardia Civil o la Policía Nacional.

¿Cómo evitar que mis cuentas sean hackeadas?

Activación en dos pasos

facebook

- Ingresa en tu página conectado como administrador.
- Da click en Configuración General.
- Verificación de la página.

twitter

- En el menú lateral, dar clic en Más.
- Configuración y privacidad.
- Configuración de cuenta y haz clic en Seguridad.
- Pulsa Autenticación de dos factores.

whatsapp

- Ingresa a Ajustes.
- Configuración.
- Cuenta.
- Verificación en dos pasos.
- Activar.

gmail

- Ve a tu cuenta de Google.
- En el panel de navegación de la izq; haz clic en Seguridad.
- Haz clic en Verificación en dos pasos.
- Haz clic en Empezar.

instagram

- Accede a la pestaña de perfil.
- Entra en Configuración, Autenticación en dos pasos.
- Selecciona Aplicación de autenticación.
- Añade el código en la app de verificación. Cópialo y vuelve a Instagram.
- Pulsa sobre siguiente, introduce el código y acéptalo.
- Guarda tus códigos de seguridad para emergencias.

outlook

- Haz click en "Más opciones de seguridad".
- Elige verificación en dos pasos.
- Selecciona Activar verificación en dos pasos.
- Configura la autenticación con tu teléfono móvil.

fiscalia.chihuahua.gob.mx

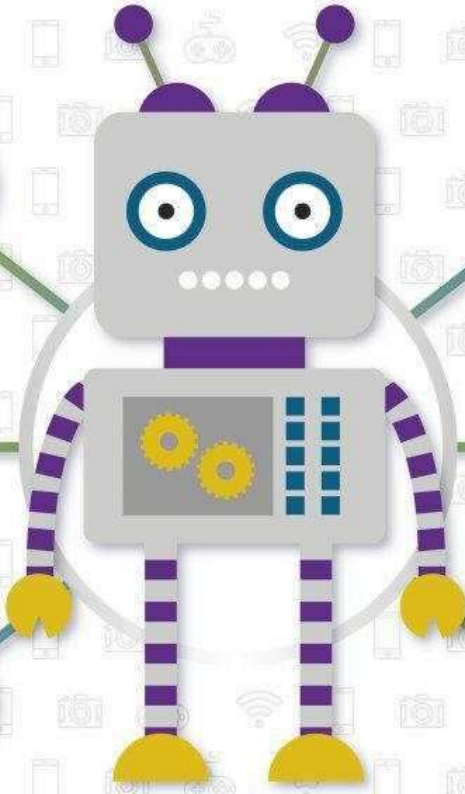
Chihuahua

FISCALÍA GENERAL DEL ESTADO

DIRECCIÓN DE ANÁLISIS DE EVIDENCIA DIGITAL E INFORMÁTICA FORENSE

UNIDOS conVALOR

JUGUETES CONECTADOS, PERO SEGUROS



MICRÓFONO, CÁMARA

APAGAR O DESACTIVAR CUANDO NO SE ESTÉN USANDO PARA EVITAR QUE REGISTREN DATOS CONTINUAMENTE.

WIFI, BLUETOOTH, NFC

CAMBIAR LAS CONTRASEÑAS POR DEFECTO DE LAS CONEXIONES INALÁMBRICAS PARA EVITAR QUE OTRAS PERSONAS SE PUEDAN CONECTAR PARA ESPIARNOS.

SEGURIDAD DE DATOS

EL NIVEL DE CIFRADO DE LOS SERVIDORES ES ADECUADO.

VINCULACIÓN CON APPS

ASEGURARSE DE QUE DESCARGAMOS LA APP AUTÉNTICA DESDE EL MERCADO OFICIAL Y SUS PERMISOS SON APROPIADOS.

USO DE LOS DATOS

LA POLÍTICA DE PRIVACIDAD ES CLARA Y NO PERMITE EL USO COMERCIAL DE LOS DATOS, NI SU CESIÓN A TERCEROS.

¿MÁS INFORMACIÓN?

GUÍA DE JUGUETES CONECTADOS DE IS4K: **www.is4k.es**

SOLICITA AYUDA EN:
www.is4k.es y **900 116 117**
Servicio gratuito y confidencial

GOBIERNO DE ESPAÑA · MINISTERIO DE ECONOMÍA Y EMPRESA · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · is4k INTERNET SEGURA FORKiDS · Cofinanciado por la Unión Europea Mecanismo «Conectar Europa» · Asociación Española de Fabricantes de Juguetes

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017
TU AYUDA EN CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

Consejos para identificar las llamadas del falso soporte técnico de Microsoft

- La llamada puede realizarse desde cualquier número de teléfono: fijo, móvil, desde España o el extranjero.
- El operador suele hablar en castellano, pero no es nativo.
- Podría solicitar que instales un programa en tu ordenador y así tomar el control del mismo.
- En ocasiones, solicitan una cuantía económica por el servicio prestado.

CÓMO HACER DE TU HOGAR UN CIBER LUGAR SEGURO

Durante la pandemia

Mantente alerta y no:

EUROPOL

- ⊗ Respondas a mensajes o llamadas sospechosas
- ⊗ Abras enlaces y archivos adjuntos no solicitados
- ⊗ Compres cosas online que parezcan estar agotadas en cualquier otro lugar

- ⊗ Compartas detalles de tu tarjeta bancaria o información financiera personal

- ⊗ Compartas noticias que no vengan de fuentes oficiales
- ⊗ Hagas donaciones benéficas sin verificar su autenticidad
- ⊗ Envíes dinero por adelantado a alguien que no conoces

CCN
centro criptológico nacional

¿Estás mostrando tu día a día en redes sociales?

Reflexiona sobre el contenido que compartes. Evita dar demasiada información sobre ti. También te aconsejamos desactivar la geolocalización por defecto en el menú de configuración de tu perfil.

#CiberCOVID19
#NoTeInfectesConElMail

CCN
centro criptológico nacional

¿Quieres adquirir conocimientos básicos de ciberseguridad?

Entra en www.ccn-cert.cni.es/cibercovid19 y haz el nuevo curso online sobre principios y recomendaciones básicas del CCN.

#CiberCOVID19
#NoTeInfectesConElMail

PHISHING

Es una técnica que utilizan los ciberdelincuentes para engañar y conseguir información sensible (*contraseñas, número de cuentas bancarias, datos de tarjetas de crédito, información de la organización...*)

Se considera un tipo de ataque de **ingeniería social** porque se basa en errores humanos.

CÓMO FUNCIONA

- Los ciberdelincuentes intentan suplantar a una entidad legítima (*organismo público, entidad financiera, servicio técnico...)*

- La mayoría de los ataques comienzan con la recepción de un correo electrónico o un mensaje directo.

- Los correos incluyen enlaces a sitios web preparados por los atacantes en los que se pide la información.

- Otros medios de propagación son: *mensajería instantánea, redes sociales, SMS, teléfono.*

EJEMPLO

COVID-19

Usuarios no habituados a teletrabajar tienen que adaptarse a una nueva situación.

Los ciberdelincuentes pueden realizar campañas de "phishing" en las que haciéndose pasar por personal de la organización, en especial de atención a usuarios, pretendan obtener credenciales de acceso a los sistemas.

PREVENCIÓN

- Comprueba que la dirección del correo remitente coincide con quien dice ser. *Presta atención a la sintaxis, una letra puede marcar la diferencia.*
- Cuidado con las urgencias que fuerzan a tomar decisiones rápidas para evitar supuestas consecuencias negativas:
  - *Tu cuenta ha sido o va a ser bloqueada.*
  - *Notificaciones de sanciones.*
  - *Confirmación de la identidad.*
  - *Mejoras en medidas de seguridad.*

- Desconfía de textos mal redactados o con faltas de ortografía.
- Desconfía de ofertas, loterías o premios de gran valor.
- Las webs seguras empiezan por **https://** y aparece en el navegador el icono de un pequeño candado cerrado.
- Presta atención a la sintaxis de los enlaces a páginas web, en muchos casos la dirección web parece legítima, pero tiene algún cambio.
- Evita introducir datos en web cuyos enlaces lleguen acortados (**cort.as, bit.ly**)
- Si sospechas ser víctima de un phishing ponte en contacto con el soporte informático a usuarios de tu organización.

CORREO ELECTRÓNICO

El correo electrónico es una herramienta de comunicación que además se sigue utilizando para el intercambio de información. Es frecuente que los ciberdelincuentes traten de utilizar tus cuentas de correo para fraudes y estafas, así como para infectar y comprometer los equipos de trabajo.

BUENAS PRÁCTICAS

Identifica al remitente.

Comprueba que el dominio es de confianza (parte a la derecha de @).

Si el contacto es conocido pero solicita información inusual comunica con él por otra vía para comprobar la legitimidad.

Inspecciona los enlaces.

Desconfía de los link en los correos:

- Links a páginas web dañinas.
- Links a páginas web que simulan ser la página oficial de un organismo o institución.

Revisa la URL (sitúate sobre el texto del enlace para visualizar la dirección).

Evita responder a correos electrónicos no solicitados con fines publicitarios o comerciales..

No reenvíes rumores, noticias falsas, ofertas o regalos, propagandas...

Identifica correos sospechosos.

- Mal redactados, faltas de ortografía.
- Cambio de aspecto (logotipos, firma...)
- Solicita o urge a hacer algo no habitual.
- Genéricos con contenidos llamativos.

Uso adecuado del correo corporativo.

Sé consciente de dónde utilizas tu correo profesional.

No facilites tu dirección de correo profesional para asuntos personales o en webs públicas o de dudosa reputación.

Utiliza copia oculta.

Impide que los destinatarios de un correo vean a quién más ha sido enviado .

CCO...

Analiza los ficheros adjuntos.

Evita abrir ficheros:

- de remitentes desconocidos.
- que incitan a su descarga.
- con extensiones desconocidas.
- que piden habilitar el uso de macros.

Si detectas algo sospechoso, comunícalo.

Contacta directamente con los medios de atención a usuarios, preferentemente mediante el sistema **CRU**.

Protege la información sensible.

Evita enviar información sensible por correo electrónico.

PROTEGE TUS CUENTAS

EUROPOL

LA NUEVA NORMALIDAD

TRAS EL COVID-19

CONSEJOS DE SEGURIDAD

¡Atención a los mensajes demasiado buenos para ser verdad!

- Gangas en inversiones y préstamos
- Ofertas baratas de bienes y servicios
- Oportunidades de trabajo sospechosas

Adiós 'dinero en metálico' Hola 'pagos online'

- Utiliza conexiones seguras para las transacciones por internet
- Emplea únicamente sitios web seguros
- Utiliza tarjetas de crédito para las compras por internet

¿Adquieres criptomoneda?

- Cómprala directamente y evita sistemas de inversión
- Escoge un intercambiador fiable
- Considera almacenarla en una 'cartera virtual'