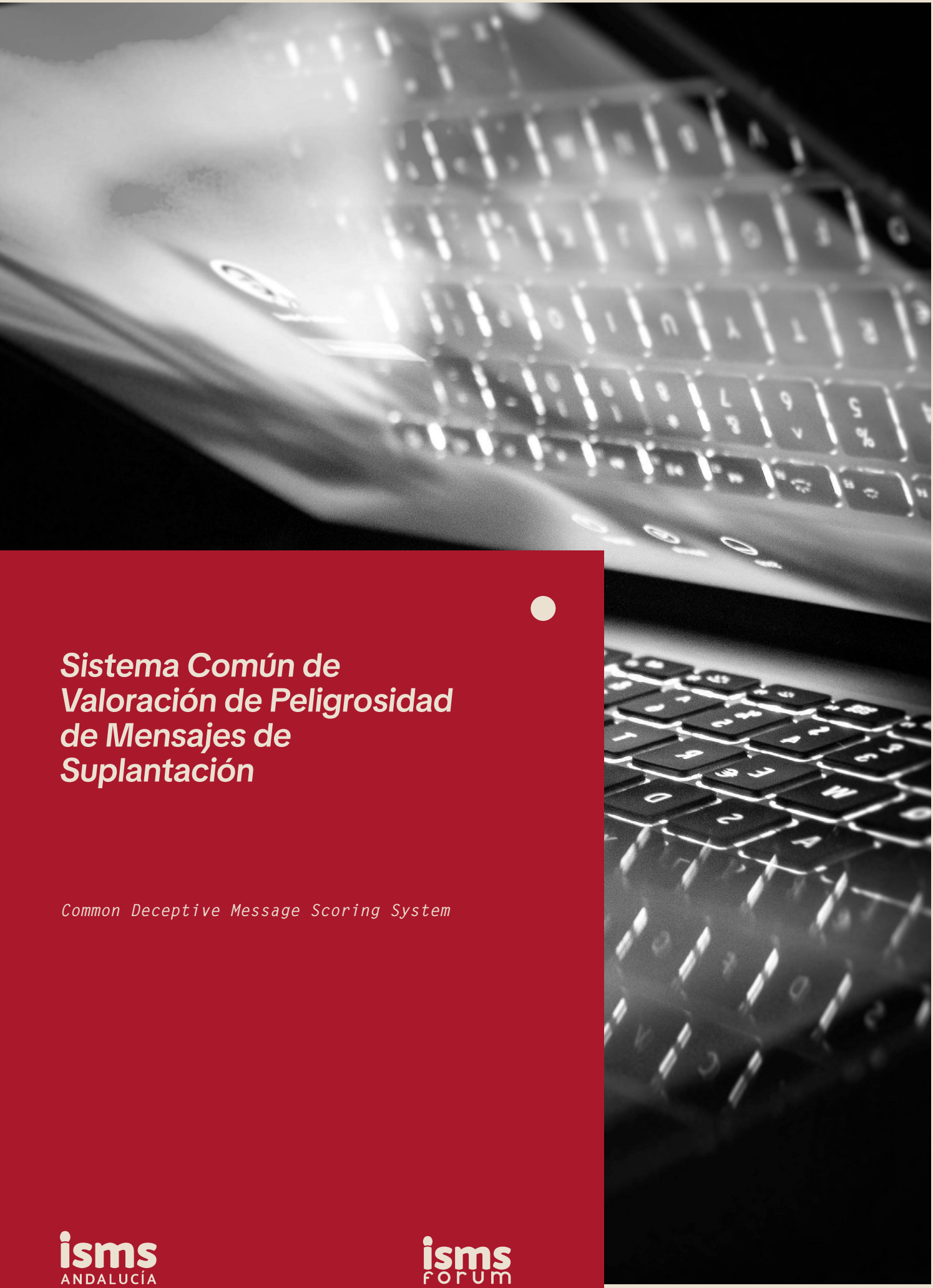


Sistema Común de Valoración de Peligrosidad de Mensajes de Suplantación

Common Deceptive Message Scoring System

isms ANDALUCÍA

isms forum

INTRODUCCIÓN

1.

El “Sistema Común de Valoración de Peligrosidad de Mensajes de Suplantación” (en inglés “Common Deceptive Message Scoring System” o, por sus siglas, “CDMSS”) permite evaluar la peligrosidad de distintos tipos de mensajes fraudulentos como phishing (correo electrónico), smishing (SMS), vishing (llamadas de suplantación mediante voz) y Qrishing (códigos QR maliciosos). El sistema asigna una puntuación de 0 a 10 considerando criterios relevantes como verosimilitud y capacidad para el engaño, el impacto potencial y el medio empleado para el engaño.

Este marco ayuda a priorizar respuestas, mejorar la concienciación de las personas, realizar ejercicios prácticos de simulación (tabletops) y facilitar la comparación entre campañas internas de una misma entidad o en relación con los resultados obtenidos por otras entidades externas.

El sistema de valoración CDMSS ha sido desarrollado por el Capítulo Andaluz del ISMS Forum, asociación sin ánimo de lucro creada en 2007, con el objetivo de promover la cultura de la seguridad de la información y la protección de datos en España, reuniendo a empresas, profesionales y organismos públicos y privados.

El CDMSS tiene un carácter abierto, estructurado, formativo y estandarizable. Se trata de una iniciativa singular y pionera que aspira a posicionarse como un referente exportable.


SYSTEM HACKED

CATEGORÍAS Y VALORACIÓN

La valoración del mensaje sospechoso se realiza mediante cuatro grandes categorías:

Verosimilitud

hasta 3 puntos

Evalúa en qué medida el mensaje resulta convincente para el receptor.

Características Técnicas del Ataque

hasta 2 puntos

Evalúa los elementos técnicos y operativos utilizados en el ataque.

Impacto Potencial

hasta 3 puntos

Mide la capacidad del mensaje de ejecutar una acción maliciosa que genere daño real.

Medio de Comunicación

hasta 2 puntos

Evalúa el canal utilizado, en función de su capacidad de generar confianza o respuesta rápida.

2.

La siguiente tabla resume las categorías, los diferentes aspectos que se evalúan para cada una de ellas, y las puntuaciones previstas:

Categoría	Subcategoría	Descripción	Puntuación subcategoría
Verosimilitud (Pto. máx.= 3)	Calidad Lingüística y Redacción	Uso correcto del idioma, estilo profesional y personalización del mensaje.	1
	Contexto y Relevancia	Relación con la actividad o entorno del destinatario.	1
	Suplantación del Remitente	Uso de dominios engañosos, nombres conocidos y firmas realistas.	1
Características Técnicas del Ataque (Pto. máx.= 2)	Técnicas de Ingeniería Social	Empleo de urgencia, miedo, recompensas o curiosidad para incitar a la acción.	1
	Técnicas Avanzadas de Evasión y Engaño	Uso de acortadores, redirecciones, ofuscación, web de suplantación, simulación de reenvío, HTML/CSS avanzado, etc.	1
Impacto Potencial (Pto. máx.= 3)	Enlace activo	Contiene enlace funcional que lleva a un recurso malicioso activo.	1
	Fichero adjunto	El mensaje incluye archivo adjunto con malware: -Detectable antivirus: 0,5 pts. -Indetectable antivirus (Día cero): 1,5 pts.	1,5
	Solicitud de acción crítica	Solicita ejecución de transferencia, entrega de credenciales, información sensible o instalación de software.	0,5
Medio de comunicación (Pto. máx.= 2)	Phishing	Mensaje enviado por email	0
	Smishing	Mensaje SMS	0,5
	Qrishing	Código QR	0,5
	Vishing	Llamada telefónica de suplantación	1
	Multicanal	Uso combinado de al menos dos canales	2

1.

Verosimilitud

(0 - 1 puntos)

Calidad Lingüística y Redacción

Ortografía y gramática
(0,25 puntos)

El mensaje está libre de errores que puedan despertar sospechas.

Estilo profesional y coherente
(0,25 puntos)

Se mantiene un tono adecuado al contexto empresarial o del remitente.

Personalización básica
(0,5 puntos)

Se utiliza información básica identificativa del receptor, como nombre, dirección de correo o puesto

(0 - 1 puntos)

Contexto y relevancia del contenido

Temática:
(0,25 puntos)

El asunto y contenido tienen sentido para la víctima y está relacionado con la actividad o función del destinatario.

Urgencia
(0,25 puntos)

Se transmite presión o necesidad de actuación inmediata de forma convincente y creíble.

Referencias
(0,5 puntos)

Se mencionan elementos de actualidad relevantes para la organización, como eventos reales o internos recientes

(0 - 1 puntos)

Suplantación del remitente

Dominio:
(0,5 puntos)

Se utiliza un dominio similar o visualmente engañoso, con pequeños cambios para parecer legítimo (typosquatting).

Remitente
(0,25 puntos)

utiliza un nombre coincidente con alguien conocido o con autoridad que inspira confianza por familiaridad o prestigio.

Firma
(0,25 puntos)

Pie de correo bien construido que simula el estilo de la organización suplantada

2.

Características Técnicas del Ataque

(0 - 1 puntos)

Técnicas de Ingeniería Social

Genera urgencia o miedo
(0,5 puntos)

El mensaje presiona al destinatario para actuar de inmediato bajo amenaza de una consecuencia negativa, como suspensión de cuenta o incumplimiento detectado. ***Ej. 'cuenta suspendida', 'incumplimiento detectado'.***

Ofrece recompensas o incentivos
(0,25 puntos)

El mensaje promete un beneficio atractivo —descuentos, premios, bonificaciones— para motivar al usuario a hacer clic o compartir datos. ***Ej. descuentos, premios, bonificaciones.***

Apela a la curiosidad o intriga
(0,25 puntos)

El mensaje despierta interés con frases ambiguas o llamativas, incitando a la acción por simple curiosidad. ***Ej. 'Haz clic para ver algo importante'***

(0 - 1 puntos)

Técnicas Avanzadas de Evasión y/o Engaño

Uso de acortadores, redirecciones u ofuscación
(0,25 puntos)

El enlace está disfrazado mediante servicios de acortamiento, cadenas largas con parámetros irrelevantes o caracteres que simulan direcciones legítimas. ***Ej. enlaces bit.ly, caracteres unicode engañosos.***

Simulación de reenvío o respuesta
(0,25 puntos)

El mensaje se presenta como parte de una conversación previa, incluyendo prefijos o un formato de hilo que genera confianza en el destinatario. ***Ej. Asunto con 'Re:' o estilo de hilo anterior.***

HTML/CSS avanzado o logos imitados
(0,25 puntos)

Se utilizan diseños elaborados, gráficos corporativos o plantillas que imitan con precisión la imagen visual de una organización.

Presencia de datos personales del destinatario
(0,25 puntos)

incluye varios datos personales de difícil localización para reforzar la credibilidad. Por ejemplo, identificador de usuarios, contraseña, fecha de nacimiento, etc. obtenidas de base de datos de fugas de credenciales.

3.

Impacto Potencial

(0 - 1 puntos)

Enlace activo

El mensaje contiene un enlace funcional que dirige a un recurso malicioso activo. (1 punto).

(0 - 1.5 puntos)

Fichero adjunto

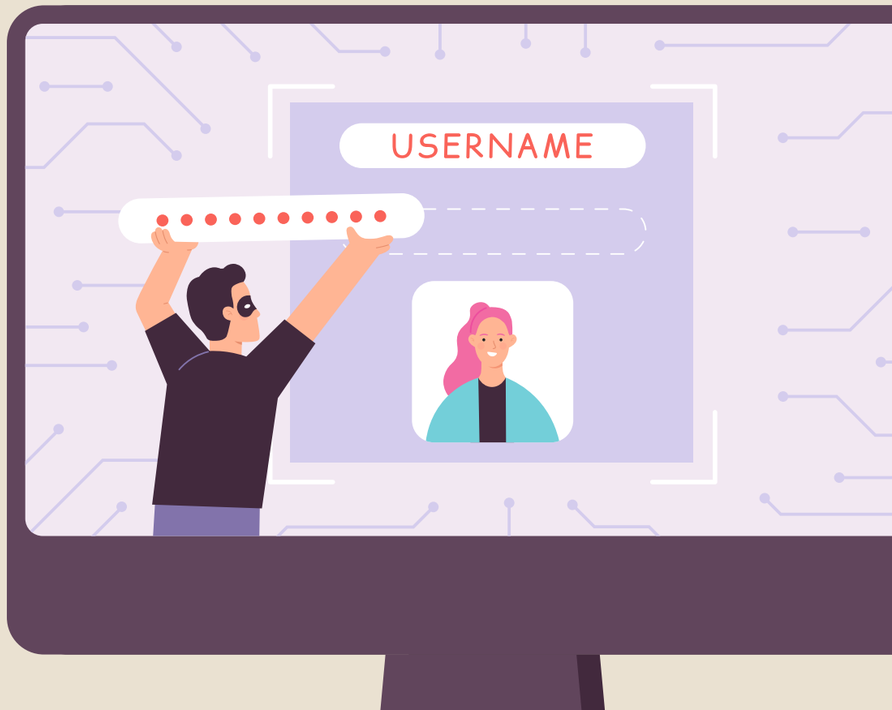
Se adjunta archivo identificado como malware. (0,5 puntos)

El fichero malicioso se corresponde con una amenaza avanzada ***(ej. 0-day)*** o no es detectado por antivirus. (1,5 puntos)

(0 - 0.5 puntos)

Solicitud de acción crítica

El mensaje solicita al usuario realizar acciones como transferencias económicas, entrega de credenciales, información personal, instalación de software o envío de datos sensibles. (0,5 puntos)



4.

Medio de comunicación

Phishing (correo electrónico)

Medio clásico, con alta exposición y usuarios más habituados y concienciados. Es el valor de base de referencia. ***(0 puntos)***

Smishing (SMS)

Medio más inmediato y breve, que genera urgencia. ***(0,5 puntos)***

Qrishing (código QR)

Medio indirecto, difícil de verificar visualmente, especialmente en impresos o pantallas. ***(0,5 puntos)***

Vishing (llamada telefónica)

Medio directo, con interacción social que potencia la manipulación. ***(1 punto)***

Multicanal

Uso combinado de dos o más medios, lo que refuerza la credibilidad y capacidad para persuadir al usuario (ej. email seguido de llamada de voz o SMS con QR). ***(2 puntos)***

5.

Interpretación de la Puntuación Total

Puntuación Total	Nivel de Peligrosidad	Acción Recomendada
0 - 2	Baja	Monitoreo básico.
2.1 - 5	Moderada	Precaución. Análisis adicional.
5.1 - 8	Alta	Respuesta interna y alerta a usuarios.
8.1 - 10	Muy Alta	Bloqueo inmediato e investigación del incidente.

Guía de Evaluación Paso a Paso del *CDMSS*

6.

Esta guía describe el proceso recomendado para evaluar la peligrosidad de mensajes de suplantación utilizando el "Sistema Común de Valoración de Peligrosidad de Mensajes de Suplantación" (CDMSS).

1 *Cómo Iniciar la Evaluación*

1. Recepción y Aislamiento del Mensaje:

- Al recibir un mensaje sospechoso (correo, SMS, llamada, QR), aíslelo de inmediato. No interactúe con enlaces, archivos adjuntos ni responda. Si es una llamada, intente registrar la mayor cantidad de detalles posible.
- Para correos electrónicos o SMS, reenvíe el mensaje como archivo adjunto (no como reenvío normal) a una dirección de análisis segura o a su equipo de seguridad.
- Para códigos QR, tome una foto clara del código y, si es posible, anote el contexto físico donde lo encontró.

2. Preparación del Entorno de Análisis:

- Utilice un entorno seguro y aislado (ej. máquina virtual, sandbox) para abrir enlaces o analizar archivos adjuntos. Nunca realice estas acciones en su equipo de trabajo o personal.
- Asegúrese de tener acceso a herramientas de análisis de URL y de archivos (ej. VirusTotal, urlscan.io) y, si es necesario, herramientas de desofuscación de código.

2 *Orden Recomendado para Evaluar las Categorías y Subcategorías*

Para una evaluación sistemática y eficiente, se recomienda seguir el siguiente orden:

1. Medio de Comunicación (Puntuación de Base):

- Identifique el canal principal de comunicación del mensaje (correo, SMS, QR, llamada, multicanal).
- Asigne la puntuación base según la tabla del CDMSS. Este será su punto de partida.

2. Verosimilitud:

- **Calidad Lingüística y Redacción:** Analice la gramática, ortografía, estilo y nivel de personalización del mensaje.
- **Contexto y Relevancia del Contenido: E**valúe si el mensaje tiene sentido para el destinatario, si transmite urgencia creíble y si hace referencia a elementos reales o recientes.
- **Suplantación del Remitente:** Verifique el dominio, el nombre del remitente y la firma para identificar intentos de engaño o similitud con entidades legítimas.

3. Características Técnicas del Ataque:

- **Técnicas de Ingeniería Social:** Identifique el tipo de manipulación psicológica utilizada (miedo, urgencia, recompensa, curiosidad).
- **Técnicas Avanzadas de Evasión y Engaño:** Busque indicios de ofuscación de enlaces, redirecciones, simulación de hilos de correo, o la presencia de datos personales del destinatario que aumenten la credibilidad.

4. Impacto Potencial:

- **Enlace Activo:** Si hay un enlace, analícelo en el entorno seguro. Determine si es funcional y si dirige a un recurso malicioso (ej. página de phishing, descarga de malware).
- **Fichero Adjunto:** Si hay un archivo, analícelo en el entorno seguro. Determine si contiene malware y evalúe su nivel de sofisticación (detectado por AV vs. amenaza avanzada/0-day).
- **Solicitud de Acción Crítica:** Identifique si el mensaje insta al usuario a realizar acciones de alto riesgo (transferencias, entrega de credenciales, instalación de software).

3 *Consideraciones al asignar puntuaciones*

Para una evaluación sistemática y eficiente, se recomienda seguir el siguiente orden:

◊ **Sea Objetivo:** Basen su evaluación únicamente en la información contenida en el mensaje y en los resultados de su análisis técnico.

◊ **Utilice los Ejemplos:** Consulte los ejemplos detallados para cada subcategoría para guiar la asignación de puntos y asegurar consistencia.

◊ **En Caso de Duda»:** Si se encuentra en el límite entre dos puntuaciones, opte por la puntuación más conservadora (la que mejor refleje el riesgo o la que tenga menos evidencia de sofisticación).

◊ **Sume los Componentes:** Para cada categoría, sume las puntuaciones de las subcategorías. Asegúrese de no exceder el máximo de puntos permitido por cada categoría, tal como se indica en la tabla del CDMSS.

◊ **Puntuación Cero:** Si un elemento no está presente o no aplica, su puntuación es cero para esa subcategoría (ej. si no hay adjunto, el «Fichero adjunto» puntúa 0).

4 *Herramientas o Técnicas que Pueden Ayudar en la Evaluación*

Análisis de Encabezados de Correo: Para verificar el origen real del mensaje, los registros SPF, DKIM, DMARC.

Herramientas de Análisis de URL:

- ***urlscan.io:*** Para ver capturas de pantalla de sitios web, redirecciones y peticiones de red.
- ***VirusTotal (URL):*** Para verificar si una URL ha sido reportada como maliciosa.
- ***PhishTank:*** Base de datos de sitios de phishing reportados.

Sandboxes de Archivos:

- ***VirusTotal (Archivo):*** Para análisis de archivos adjuntos con múltiples motores antivirus.
- ***Any.Run, Hybrid Analysis:*** Sandboxes online para ejecutar archivos de forma segura y observar su comportamiento.

Herramientas de Desofuscación: Para analizar código JavaScript ofuscado en páginas web o macros en documentos.

Búsqueda en Fuentes Abiertas (OSINT): Para verificar la legitimidad de empresas, nombres de personas o eventos mencionados en el mensaje.

Máquinas Virtuales: Para abrir enlaces o archivos adjuntos en un entorno controlado y aislado de su red principal.

Al finalizar la evaluación, sume todas las puntuaciones obtenidas para determinar la puntuación total del CDMSS y consulte la sección de «Interpretación de la Puntuación Total» para la acción recomendada.

7.

Ejemplos prácticos de valoración

Verosimilitud

(0 - 1 puntos)

Calidad Lingüística y Redacción

0.25 «Mensaje con errores gramaticales obvios y faltas de acentuación.»

0.50 «Mensaje con redacción formal pero sin personalización.»

1.00 «Mensaje impecable en gramática y estilo, con el nombre del destinatario.»

(0 - 1 puntos)

Contexto y Relevancia del Contenido

0.25 «Mensaje de un supuesto servicio de streaming con un aviso de pago pendiente, enviado a un usuario que no tiene suscripción a dicho servicio.»

0.50 «Correo electrónico que simula ser de una empresa de paquetería, indicando que hay un envío retenido y que debe actuarse en '24 horas' para evitar cargos, pero el usuario no espera ningún paquete.»

1.00 «Email que se presenta como una comunicación interna, haciendo referencia a una 'reunión de equipo sobre el nuevo proyecto X' que realmente existe y ha sido anunciada, solicitando confirmar asistencia a través de un enlace.»

(0 - 1 puntos)

Suplantación del Remitente

«Correo de 'Soporte Técnico' con una dirección de email genérica como 'soporte@gmail.com', pero el nombre del remitente es 'Microsoft'.» **0.25**

Mensaje de 'PayPal' con el dominio 'payppal.com' (con doble 'p'), muy similar al legítimo 'paypal.com'.» **0.50**

«Email de 'tu banco' con el dominio correcto, pero con una firma que incluye el logo oficial, dirección completa y números de contacto reales del banco.» **1.00**

Características técnicas del ataque

(0 - 1 puntos)

Técnicas de Ingeniería Social

0.25	«Mensaje SMS que dice ‘Mira estas fotos comprometedoras tuyas, haz clic aquí para verlas’, sin más contexto.»
0.50	«Correo electrónico que anuncia un premio de lotería inesperado y solicita datos personales para reclamarlo.»
1.00	«Email que advierte sobre una supuesta brecha de seguridad en su cuenta bancaria y exige la verificación inmediata de credenciales para evitar el bloqueo de la cuenta.»

(0 - 1 puntos)

Técnicas Avanzadas de Evasión y/o Engaño

«Mensaje con un enlace bit.ly que redirige a una página de phishing.»	0.25
«Correo con el asunto ‘Re: Factura pendiente’ que imita un hilo de correo previo, aunque el usuario no recuerda haber tenido interacción previa.»	0.50
«Página de inicio de sesión falsa de Office 365, visualmente idéntica a la legítima, con todos los logos y estilos CSS correctos.»	0.75
«Mensaje de restablecimiento de contraseña que incluye el nombre completo del destinatario, su número de identificación fiscal y su dirección de correo electrónico personal, obtenidos de una fuga de datos.»	1.00

Impacto Potencial

(0 - 1 puntos)

Enlace Activo

1.00

«Un correo de phishing bancario cuyo enlace lleva directamente a una página de inicio de sesión falsa, activa y diseñada para capturar credenciales.»

(0 - 1.5 puntos)

Fichero adjunto

0.50

«Un email que incluye un archivo 'Factura.zip' que, al ser analizado por un antivirus, es detectado como un troyano conocido.»

1.50

«Un correo que adjunta un documento PDF que, al ser abierto, explota una vulnerabilidad 0-day en el lector de PDF e instala un ransomware que no es detectado por los antivirus convencionales.»

(0 - 0.5 puntos)

Solicitud de acción crítica

«Un email que solicita al usuario que instale un 'parche de seguridad urgente' descargando un ejecutable de un enlace externo, o que realice una transferencia a una cuenta bancaria desconocida para 'verificar su identidad'.»

0.25

Medio de comunicación

Phishing

0.00

«Un correo electrónico simple que solicita credenciales de una cuenta de red social, enviado de forma masiva.»

Smishing (SMS)

0.50

«Un SMS que notifica un supuesto cargo no reconocido en la tarjeta de crédito y solicita al usuario que llame a un número de teléfono fraudulento para cancelarlo.»

Qrishing (código QR)

0.50

«Un cartel físico en un lugar público con un código QR que promete un descuento, pero al escanearlo, redirige a una página de phishing que solicita datos personales.

Vishing (llamada telefónica)

«Una llamada telefónica de una persona que se hace pasar por un técnico de soporte de Microsoft, intentando convencer al usuario de que ha detectado un virus en su ordenador y que necesita acceso remoto para 'solucionarlo'.»

1.00

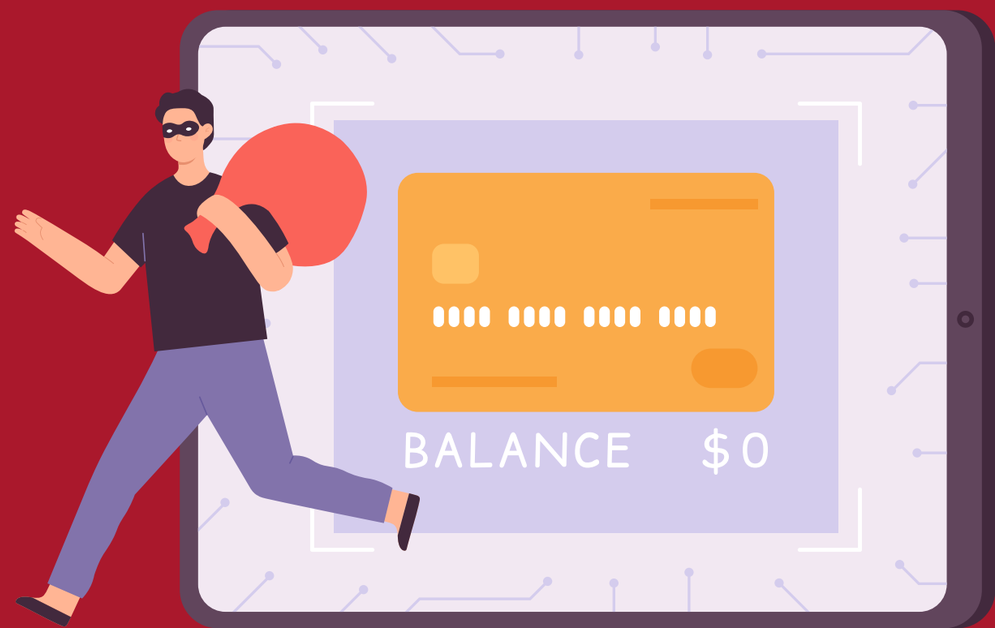
Multicanal

«Un usuario recibe un correo electrónico (phishing) con un enlace. Poco después, recibe una llamada telefónica (vishing) de alguien que dice ser del 'soporte técnico' del servicio suplantado en el email, presionándolo para que haga clic en el enlace del correo y verifique sus datos 'por seguridad'.»

1.00

8.

Ejemplos prácticos aplicados



Correo electrónico
Moderado

3
puntos

Mensaje (correo electrónico de phishing):

Asunto: Importante: su cuenta
De: Soporte Tecnico <soporte@gmail.com>

Estimado usuario,
Su cuenta a sido suspendida. Para activar su cuenta, por favor, haga clic aquí http://s25hy&44.link.zn/12x8htyy258.

Gracias.

CATEGORÍA	SUBCATEGORÍA	OBSERVACIONES	PUNTUACIÓN´ SUBCATEGORÍA
Verosimilitud	Calidad Lingüística y Redacción	Errores ortográficos (“a sido” en vez de “ha sido”)	0.25
	Contexto y Relevancia	Asunto de mensaje plausible en un entorno labora	0.25
	Suplantación del Remitente	Correo desde Gmail genérico, poco realista.	0.25
	Puntuación categoría		**0.75**
Características Técnicas del Ataque	Técnicas de Ingeniería Social	Empleo de urgencia/miedo	1
	Técnicas Avanzadas de Evasión y Engaño	N/A	0
	Puntuación categoría		**1**
Impacto Potencial	Enlace activo	Contiene un enlace fraudulento.	1
	Fichero adjunto	N/A	0
	Solicitud de acción crítica	Solicitud de acción crítica (“activar su cuenta” → credenciales)	0.25
	Puntuación categoría		**1,25**
Medio de comunicación	Phishing	Mensaje enviado por email	0
	Puntuación categoría		**0**
PUNTUACIÓN TOTAL FINAL			**3**

Correo electrónico
Alto

6
puntos

Mensaje (correo electrónico de phishing):

Asunto: Re: Factura pendiente
De: PayPal <servicio@payppal.com>

Estimado cliente,
Le escribimos en referencia a su factura pendiente. Haga clic en el siguiente enlace para revisar el estado de su pago y evitar cargos adicionales: http://payppal.com/soporte/ft.

Atentamente,
El equipo de PayPal.

1 archivo adjunto

CATEGORÍA	SUBCATEGORÍA	OBSERVACIONES	PUNTUACIÓN´ SUBCATEGORÍA
Verosimilitud	Calidad Lingüística y Redacción	Redacción formal (sin personalización)	0.5
	Contexto y Relevancia	Contexto + Urgencia (“evitar cargos”)	0.75
	Suplantación del Remitente	Uso de nombre de dominio similar payppal.com para inducir a engaño	0.75
	Puntuación categoría		**2**
Características Técnicas del Ataque	Técnicas de Ingeniería Social	Empleo de urgencia/miedo	1
	Técnicas Avanzadas de Evasión y Engaño	Utilización de “RE:” para simular cadena o respuesta de mensaje legitimo	0.5
	Puntuación categoría		**1.5**
Impacto Potencial	Enlace activo	Contiene un enlace fraudulento.	1
	Fichero adjunto	Fichero adjunto “factura.pdf” no detectable por antivirus	1,5
	Solicitud de acción crítica	Solicitud de acción crítica (“activar su cuenta” → credenciales)	0.5
	Puntuación categoría		**2.5**
Medio de comunicación	Phishing	Mensaje enviado por email	0
	Puntuación categoría		**0**
PUNTUACIÓN TOTAL FINAL			**6.5**

Correo electrónico + SMS

Muy alto

8 puntos

Mensaje (correo electrónico de phishing + mensaje de texto SMS):

Mensaje por correo electrónico:

Asunto: Alerta de Seguridad: Acceso No Autorizado Detectado - Verifique su Cuenta

De: TuBanco <seguridad@tubanco.com>

Estimado/a Javier Sanchez,

Hemos detectado actividad sospechosa en su cuenta bancaria (No. de Identificación Fiscal: **51547801A**). Para proteger sus fondos y su información personal, hemos bloqueado temporalmente el acceso.

Para restaurar su cuenta de inmediato y verificar su identidad, le solicitamos que haga clic en el siguiente enlace seguro y complete el proceso de verificación: https://tubanco.com/personal.

Si no completa esta verificación en las próximas 24 horas, su cuenta podría ser permanentemente suspendida.

Lamentamos cualquier inconveniente que esto pueda causarle.

Atentamente,

Departamento de Seguridad

TuBanco

https://tubanco.com
Plaza Callao 1, 28001 Madrid
+34 91 456 87 87 / 900 487 487

Mensaje por SMS:

Correo electrónico + SMS

Muy alto

8 puntos

CATEGORÍA	SUBCATEGORÍA	OBSERVACIONES	PUNTUACIÓN´ SUBCATEGORÍA
Verosimilitud	Calidad Lingüística y Redacción	Redacción formal y personalización	1
	Contexto y Relevancia	Entidad bancaria e información personal	1
	Suplantación del Remitente	Suplantación del dominio real, incluye logo y datos reales de la entidad bancaria	1
	Puntuación categoría		**3**
Características Técnicas del Ataque	Técnicas de Ingeniería Social	Empleo de urgencia/miedo	1
	Técnicas Avanzadas de Evasión y Engaño	Utiliza técnicas de email spoofing y cloaking para enmascarar la dirección de correo y la URL maliciosa	1
	Puntuación categoría		**2**
Impacto Potencial	Enlace activo	Contiene un enlace fraudulento.	1
	Fichero adjunto	N/A	0
	Solicitud de acción crítica	Solicitud de acción crítica	0,5
	Puntuación categoría		**2.5**
Medio de comunicación	Multicanal	Mensaje enviado por email y SMS	2
	Puntuación categoría		**2**
PUNTUACIÓN TOTAL FINAL			**8.5**

Sistema Común de Valoración de Peligrosidad de Mensajes de Suplantación

Common Deceptive Message Scoring System

Coordinadores del proyecto

Alfonso López-Escobar Beares

Eudin Mercedes

Beatriz García

Diseño y maquetación

Susana Marín

isms ANDALUCÍA

isms forum