PÍLDORAS FORMATIVAS DE CIBERSEGURIDAD

CIBER SEGURIDAD

CURSO: INGENIERÍA SOCIAL

1. Introducción

La ingeniería social es una de las técnicas más empleadas por los atacantes para engañar a las personas y obtener acceso, información o privilegios. Este curso te ayudará a identificar, prevenir y responder ante estas amenazas, fortaleciendo la seguridad de la Junta de Comunidades de Castilla-La Mancha.

1.1 OBJETIVOS DEL CURSO

- Comprender cómo piensa y actúa un ciberdelincuente.
- Conocer las principales técnicas de manipulación utilizadas por los atacantes.
- Entender qué es un *phishing*, el ataque más común.
- Identificar otros ataques frecuentes: *vishing*, *smishing*,*clickfix*, etc.
- Adoptar buenas prácticas y saber cómo actuar ante posibles amenazas.

2. El ser humano como eslabón más débil

Se dice que el ser humano es el eslabón más débil en la cadena de la seguridad de la información, pero ¿por qué?

01/ Las personas no pueden programarse ni actuar siempre de forma predecible.

02/ Sus decisiones pueden introducir riesgos involuntarios.

03/ Incluso con sistemas seguros, no debemos olvidar que toda tecnología depende siempre de un usuario.

2.1 ¿QUÉ ES LA INGENIERÍA SOCIAL?

CONCEPTOS PREVIOS:

- **Vulnerabilidad:** Debilidad o fallo en un sistema, aplicación o proceso que puede ser explotado por un atacante para comprometer su confidencialidad, integridad o disponibilidad.
- **Amenaza:** Cualquier evento, acción o agente (intencional o accidental) que puede explotar una vulnerabilidad para causar daño a un sistema o a la información que contiene.
- **Incidente:** Evento que compromete o intenta comprometer la confidencialidad, integridad o disponibilidad de sistemas o datos, alterando su funcionamiento normal.
- **Impacto:** Consecuencia o nivel de daño que un incidente provoca en una organización, afectando sus operaciones, activos, servicios o reputación.
- **Riesgo:** Probabilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo sobre los sistemas, datos u operaciones de una organización.

2.1 ¿QUÉ ES LA INGENIERÍA SOCIAL?

CONCEPTO DE INGENIERÍA SOCIAL

La Ingeniería Social engloba un conjunto de técnicas maliciosas basadas en la manipulación psicológica. Los ciberdelincuentes las emplean para engañar a los usuarios y lograr que comentan errores de seguridad o compartan información sensible.

¿CÓMO LOGRAN MANIPULAR A LAS PERSONAS?

- El engaño y la persuasión.
- La explotación de las emociones: curiosidad, miedo, urgencia, confianza…
- La suplantación de identidades legítimas.
- La creación de situaciones de necesidad o emergencia.
- El aprovechamiento de la falta de atención del usuario.

2.1 ¿QUÉ ES LA INGENIERÍA SOCIAL?

MOTIVOS Y OBJETIVOS DE LOS CIBERDELINCUENTES

¿A QUÉ SE DEBE LA POPULARIDAD DE LOS ATAQUES QUE UTILIZAN LA INGENIERÍA SOCIAL?

- La ingeniería social es más fácil que tratar de *hackear* un sistema mediante códigos y algoritmos.
- No es necesario violar o burlar sistemas de detección de intrusos o *firewalls*.
- Las herramientas que utilizan los ciberdelincuentes son gratuitas o de muy bajo coste.
- Este tipo de ataques tienen una efectividad muy alta.
- Las personas son la vulnerabilidad más grande en cualquier organización.

¿QUÉ PERSIGUE UN CIBERDELINCUENTE?

- Acceder a los sistemas.
- Alterar los sistemas objetivo para que no puedan continuar con su funcionamiento habitual.
- Obtener información para cometer fraudes posteriores.
- Divulgar, alterar, destruir o robar información crítica o confidencial.
- Espionaje industrial.
- Controlar el sistema de información a través de los privilegios administrativos podrá conseguir el control total de los sistemas de información.
- Persistencia: lograr permanecer dentro del sistema hasta conseguir todos los objetivos.
- Explotar el sistema.

2.2 CICLO DE VIDA DE LA INGENIERÍA SOCIAL

2.3 MÉTODOS DE OBTENCIÓN DE INFORMACIÓN: OSINT Y HUELLA DIGITAL

La Inteligencia de fuentes abiertas (OSINT) es el conjunto de técnicas y herramientas que permiten recopilar y analizar información pública sobre personas u organizaciones. Los ciberdelincuentes la emplean para transformar datos accesibles en inteligencia útil para preparar ataques.

¿CUÁNTA INFORMACIÓN HAY SOBRE TI EN INTERNET?

Prueba a buscar tu nombre y apellidos entre comillas en un buscador.

Gran parte de esta información procede de **tu huella digital**, es decir, del rastro de datos que dejas cuando navegas por internet. Este registro es rastreable, persistente y permite perfilar el comportamiento del usuario, siendo utilizado para seguridad, *marketing* o evaluación de antecedentes. Tu huella digital se construye en base a:

Los sitios web que visitas.

Las redes sociales en las que participas.

Los correos electrónicos y la información que compartes o envías en línea.

A través de técnicas OSINT, los ciberdelincuentes pueden recopilar y correlacionar estos datos para rastrear tus actividades, identificar tus dispositivos o incluso descubrir tus hábitos y relaciones personales.

2.3 MÉTODOS DE OBTENCIÓN DE INFORMACIÓN: OSINT Y HUELLA DIGITAL

¿QUIERES REDUCIR TU HUELLA DIGITAL? ¡SIGUE ESTOS CONSEJOS!

01/ Comparte lo mínimo: evita publicar datos personales (dirección, teléfono, ubicación en tiempo real) en internet y en tus redes sociales.

02/ Revisa la configuración de privacidad: limita quién puede ver tu información en redes y servicios *online*.

03/ Usa contraseñas únicas y fuertes: distintas para cada servicio y difíciles de adivinar.

04/ Elimina cuentas que no uses para reducir los puntos de exposición innecesarios.

05/ Piensa antes de aceptar: desconfía de *apps*, permisos y enlaces sospechosos.

TODO LO QUE HACEMOS EN INTERNET DEJA UNA HUELLA DIGITAL, CUIDA LA INFORMACIÓN QUE COMPARTES PORQUE TODO LO QUE PUBLICAS PUEDE SER UTILIZADO EN TU CONTRA.

2.3 MÉTODOS DE OBTENCIÓN DE INFORMACIÓN: OSINT Y HUELLA DIGITAL

FUENTES DE INFORMACIÓN

FUENTES	TIPOLOGÍA
DE INFORMACIÓN WEB	Web corporativa, buscadores, redes sociales, páginas de búsqueda de empleo, prensa *online*, Google Maps, metadatos, webs de la Administración Pública, blogs y publicaciones científicas o académicas.
PÚBLICAS	Archivos municipales, catastros, cámaras de comercio, BOE, publicaciones de Administraciones Públicas, Registro Mercantil…
VIGILANCIA TRADICIONAL	*Dumpster diving* (buscar en la basura), escucha de conversaciones de trabajo en zonas comunes, *shoulder surfing* (situarse detrás de la víctima cuando está ingresando información confidencial).

3. El arte del engaño: Herramientas y tipos de ataques

3.1 HERRAMIENTAS DE MANIPULACIÓN

Los ciberdelincuentes se sirven de factores cognitivos y, sobre todo, emocionales para manipularnos y engañarnos.

FACTORES EMOCIONALES

¿Sabías que nuestras emociones se generan en las áreas más primitivas del cerebro? Esto nos lleva, en muchas ocasiones, a reaccionar por impulso, sin analizar completamente toda la información que recibimos. Estas "vulnerabilidades" de nuestro "*hardware*" son bien conocidas por los ingenieros sociales, quienes las utilizan para manipularnos.

ATRACCIÓN	**SIMPATÍA**	**CURIOSIDAD**	**NECESIDAD**
ESCASEZ	**URGENCIA**	**MIEDO**	**AUTORIDAD**

3.1 HERRAMIENTAS DE MANIPULACIÓN

FACTORES COGNITIVOS: SESGOS COGNITIVOS

Los sesgos cognitivos son atajos mentales que usa nuestro cerebro para simplificar el procesamiento de datos, pero pueden llevarnos a conclusiones incorrectas o poco racionales.

¿Cuál es el riesgo de los sesgos cognitivos?

El problema surge cuando nos dejamos llevar por estos atajos mentales y no interpretamos correctamente lo que recibimos. Si no prestamos atención, los sesgos cognitivos pueden conducirnos a cometer errores, tomar decisiones impulsivas o incluso generarnos malestar emocional o psicológico.

3.1 HERRAMIENTAS DE MANIPULACIÓN

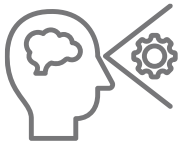
FACTORES COGNITIVOS: SESGOS COGNITIVOS

Ejemplos de sesgos cognitivos

SESGO	DEFINICIÓN
EFECTO ARRASTRE	Adoptamos comportamientos o decisiones por influencia de la mayoría.
EFECTO ANCLAJE	Tomamos decisiones basándonos excesivamente en la primera información recibida: “La primera impresión es la que cuenta”.
SESGO DE ENCUADRE	Tomamos una decisión motivada por la forma en que se presenta la información (p.ej.: comprar algo porque se nos presenta como una oferta atractiva).
SESGO DE CONFIRMACIÓN	Solemos buscar, interpretar y recordar mejor la información que confirma nuestras creencias previas.

3.1 HERRAMIENTAS DE MANIPULACIÓN

FACTORES FÍSICOS Y FISIOLÓGICOS



Limitaciones en la percepción	Cada vez usamos más los dispositivos móviles para navegar, comprar, etc. El tamaño de las pantallas puede dificultar en muchas ocasiones ver la letra pequeña, las direcciones de los sitios web o las URLs por las que navegamos.
Cansancio mental	Cuando estamos cansados, nuestros niveles de atención disminuyen y la capacidad de procesar la información también. Esto nos vuelve más vulnerables frente a ataques de ingeniería social.
Sobrecarga de información	Cuando estamos expuestos a demasiada información o estímulos, nuestro cerebro no es capaz de procesarlo todo, siendo más proclive a cometer fallos.

3.2 TÉCNICAS DE MANIPULACIÓN COGNITIVA Y EMOCIONAL

En los ataques de ingeniería social, el ciberdelincuente utiliza las siguientes estrategias para engañar y manipular a sus víctimas.

Pretexting:
Suplantar a un perfil legítimo para obtener acceso (ej. “soy el mensajero”).

Halago:
Usar elogios para generar cercanía y que la víctima colabore.

Afirmación falsa:
Dar un dato incorrecto para provocar que la víctima lo corrija.

Bracketing:
Sugerir una cifra aproximada para que el objetivo dé el dato real.

Ignorancia artificial:
Fingir desconocimiento para que la víctima facilite información.

Caja de resonancia:
Escuchar y validar quejas para crear afinidad y obtener datos.

Confidential baiting:
Compartir “información confidencial” para que la víctima haga lo mismo.

Quid pro quo:
Prometer un beneficio o solución a cambio de información.

3.3 TIPOS DE ATAQUES DE INGENIERÍA SOCIAL

Según el medio utilizado

TIPOLOGÍA	DEFINICIÓN	EJEMPLOS
DIGITALES	Manipulación a través **de medios digitales** para engañar a la víctima y obtener información, acceso o dinero.	*Phishing*, *vishing*, *smishing*, *clickfix*, *QRishing*…
FÍSICOS	Manipulación en **entornos presenciales** para obtener información o acceso mediante observación o interacción directa.	*Shoulder surfing, dumpster diving*, ingeniería social inversa….

Según la relación con el objetivo

TIPOLOGÍA	DEFINICIÓN
HUNTING	Técnica en la que los atacantes buscan, investigan y seleccionan cuidadosamente a sus víctimas antes de lanzar un ataque. A diferencia de los ataques masivos y automatizados, el *hunting* implica un **enfoque personalizado**, donde el ciberdelincuente recopila información sobre su objetivo para aumentar las probabilidades de éxito.
FARMING	Algunos tipos de ataques de ingeniería social implican **entablar una relación con la persona objetivo para extraerle información** en el transcurso de un período más dilatado. Esta táctica se conoce como *farming* y es más arriesgada para el atacante, porque tiene más probabilidades de ser descubierto. Sin embargo, si la infiltración es fructífera, puede sustraer mucha más información.

4. *Phishing*, el ataque por excelencia

4.1 *Malware*

Antes de adentrarnos en el *phishing*, es importante entender qué es el *malware*, ya que ambos conceptos están estrechamente relacionados.

El *malware* es un *software* malicioso diseñado para dañar, interrumpir o acceder sin autorización a un sistema informático, red o dispositivo. Su objetivo puede ser:

- **Robar información.**
- **Espiar al usuario.**
- **Bloquear el acceso a los datos.**
- **Tomar el control del equipo.**

En muchos casos, el *phishing* actúa como la "puerta de entrada" del *software* malicioso, ya que los ciberdelincuentes utilizan estos correos fraudulentos para incitar al usuario a descargar o ejecutar un *malware* sin darse cuenta.

4.1 *Malware*

Tipos comunes de *malware*:

Virus:
Se adjunta a archivos legítimos y se activa al ejecutarlos.

Troyanos:
Se presentan como programas fiables para engañar al usuario.

***Ransomware*:**
Bloquea o cifra los datos y exige un pago para recuperarlos.

***Spyware*:**
Recopila información sin conocimiento ni consentimiento del usuario.

***Adware*:**
Muestra publicidad invasiva y puede instalar más *software* malicioso.

Gusanos:
Se replican y se propagan automáticamente sin intervención del usuario.

4.2 ¿Qué es el *phishing*?

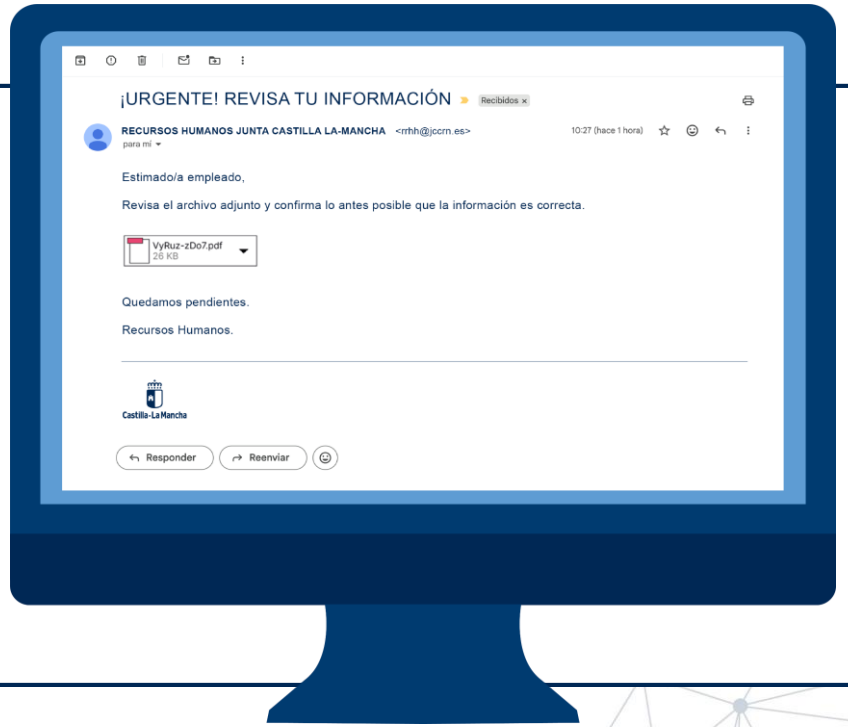
INTRODUCCIÓN Y EJEMPLO DE PHISHING

El *phishing* es una de las amenazas más comunes y peligrosas del mundo digital. Reconocerlo a tiempo es fundamental para prevenir fraudes y pérdidas de información. A continuación, exploraremos sus fundamentos y te enseñaremos a identificar y prevenir correos sospechosos, pero antes vamos a ver un ejemplo:

Beatriz recibe un correo inesperado con un archivo adjunto. Lo descarga y, de repente, **¡se bloquea el ordenador y sale un mensaje de alerta en la pantalla!**

Beatriz se asusta, apaga rápidamente el ordenador, pero al reiniciarlo sigue apareciendo el mismo mensaje. Es entonces cuando duda entre hacer clic para intentar recuperar su información o notificar lo sucedido a su responsable.

Beatriz ha sido víctima de un *phishing*. Vamos a descubrir qué es.



4.2 ¿Qué es el *phishing?*

CONCEPTO DE PHISHING

El *phishing* es un tipo de fraude por correo electrónico que busca robar información confidencial y credenciales.

Los ciberdelincuentes suplantan organizaciones legítimas o personas de confianza, creando mensajes que parecen auténticos para engañar al usuario.

¿Cómo funciona?

- El ataque se activa mediante un enlace o archivo malicioso incluido en un correo electrónico.
- Puede dirigir a una página fraudulenta o instalar *malware*.

4.2 ¿Qué es el *phishing?*

IMPACTO PARA LA JCCM

Ser víctimas de un ataque de *phishing* puede generar consecuencias relevantes para la organización, como:

Perjuicio en la confidencialidad de la información	Los atacantes pueden acceder a credenciales (usuario y contraseña), exponer información sensible o provocar filtraciones y robo de datos.
Perjuicio en la integridad de la información	El ataque puede provocar la pérdida, alteración o destrucción de datos personales o corporativos.
Perjuicio en la disponibilidad	La información o los sistemas pueden quedar inaccesibles, impidiendo el normal funcionamiento de la actividad.
Control de dispositivos y redes	A partir de un único equipo comprometido, los atacantes pueden extender el ataque a otros dispositivos o a toda la red.
Suplantación de identidad	Los ciberdelincuentes pueden hacerse pasar por la víctima para realizar nuevas acciones maliciosas.
Pérdidas financieras	Pueden producirse pagos fraudulentos, robos directos o costes derivados de la recuperación del incidente.
Daños morales y reputacionales	Tanto personas como organizaciones pueden sufrir pérdida de confianza, credibilidad o impacto en su imagen pública.
Pérdida de privacidad	La información personal o profesional puede quedar expuesta o ser utilizada de forma indebida.

4.2 ¿Qué es el *phishing?*

PAUTAS DE IDENTIFICACIÓN DEL PHISHING

Asunto: Suele usar llamadas de atención, miedo o urgencia para que actúes sin pensar.

Remitente: Verifica si lo conoces y revisa su dirección real. Desconfía de dominios extraños o imitaciones.

Adjuntos: Cuidado con archivos comprimidos, ejecutables o con doble extensión. Suelen contener *malware*.

Mensaje genérico: Saludos como *"Estimado cliente"* indican que se envió a muchas personas. Señal de alerta.

Ortografía y gramática: Errores o redacción pobre pueden indicar fraude, aunque los ataques actuales son muy convincentes.

Contenido del mensaje: Argumentos alarmistas que piden datos o acciones urgentes (premios, bloqueos, multas, etc.).

Enlaces: Comprueba la URL real antes de hacer clic. Desconfía si tiene caracteres raros, homógrafos o usa *http* en lugar de *https*.

4.2 ¿Qué es el *phishing?*

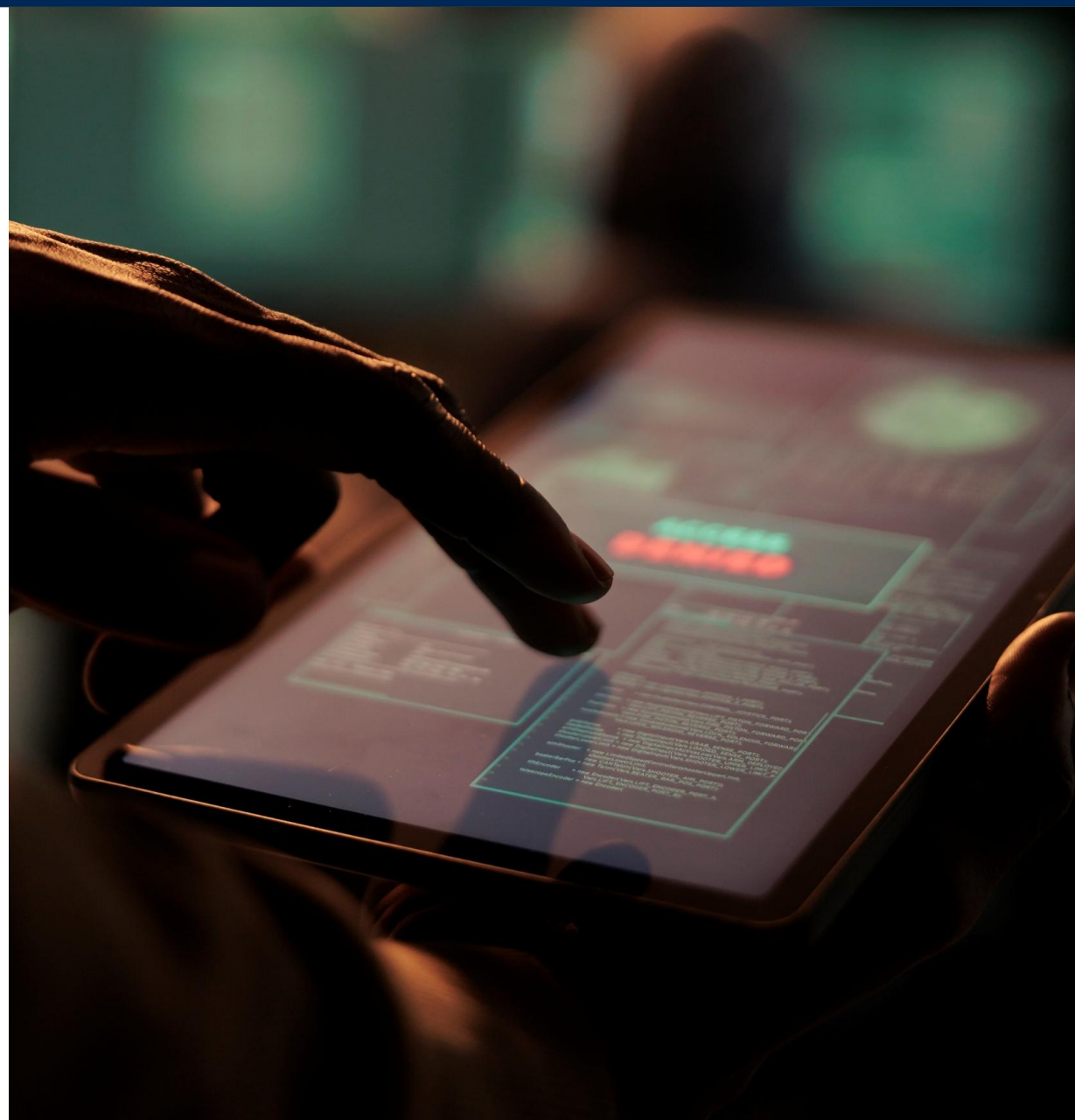
PAUTAS DE IDENTIFICACIÓN DEL PHISHING

¿Cómo prevenirlo?

- Desconfía de mensajes urgentes que pidan datos personales o credenciales.
- Verifica el remitente y la URL antes de hacer clic en enlaces o descargar archivos.
- No compartas contraseñas ni códigos por correo, SMS o mensajería instantánea (WhatsApp/Telegram).
- Activa la autenticación en dos pasos (2FA) siempre que sea posible.
- Mantén sistemas y aplicaciones actualizados para evitar vulnerabilidades.

5. Otros ataques frecuentes de ingeniería social

Los ciberdelincuentes no solo usan el *phishing* para manipular y engañar a sus víctimas, sino que explotan otras vías de ataque como llamadas telefónicas (*vishing*), mensajes de texto (*smishing*) y códigos Qrs (*QRishing*) para engañar a sus víctimas, robar información y/o estafarlas.



5.1 *VISHING* (FRAUDE TELEFÓNICO)

El *vishing* es un tipo de ataque que busca obtener datos personales o bancarios mediante una **llamada telefónica**, suplantando a una entidad de confianza.

Modalidades comunes:

- **Llamada directa:** el atacante contacta a la víctima para obtener credenciales, instalar *software* o realizar operaciones.
- **Doble llamada:** inducen a la víctima a llamar a un número fraudulento para clonar su SIM o generar costes.

¿Cómo prevenirlo?

- Desconfía de llamadas inesperadas que pidan datos.
- No des información confidencial por teléfono.
- Verifica la identidad llamando tú al número oficial.
- Cuidado con la urgencia o amenazas.
- Bloquea números sospechosos y usa identificador de llamadas.
- No sigas instrucciones extrañas (marcar códigos, instalar apps, etc.).
- Denuncia el intento de fraude.

5.2 *SMISHING* (FRAUDE A TRAVÉS DE SMS)

El *smishing* es un tipo de ataque a través de **un SMS**, en el que el atacante suplanta a una entidad legítima para robar datos, credenciales o dinero.

El mensaje suele incluir un enlace malicioso o un número de tarificación especial para que la víctima haga clic o llame.

¿Cómo prevenirlo?

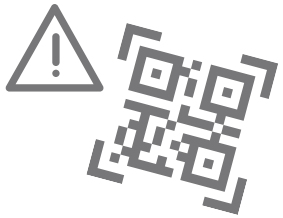
- No hagas clic en enlaces sospechosos o inesperados.
- No compartas datos personales o bancarios por SMS.
- Verifica la fuente llamando al número oficial de la entidad.
- No respondas al SMS.
- Desconfía de mensajes urgentes (cuentas bloqueadas, premios…).
- Activa la verificación en dos pasos y usa apps de seguridad.
- Denuncia el intento de fraude.

5.3 *QRISHING* (FRAUDE A TRAVÉS DE CÓDIGOS QR)

El *QRishing* es una técnica de ingeniería social que utiliza **códigos QR falsificados** para dirigir al usuario a páginas fraudulentas y robar datos sensibles.

¿Cómo funciona?

- **Creación del QR malicioso:** redirige a una web falsa que imita a una legítima.
- **Distribución:** se coloca en lugares públicos, eventos o se envía por email.
- **Escaneo:** la víctima accede al sitio fraudulento.
- **Robo de datos:** el usuario introduce credenciales o información sensible que los atacantes capturan.



¿Cómo prevenirlo?

- Verifica la fuente antes de escanear.
- Previsualiza el enlace con la app del lector QR.
- No introduzcas datos sensibles sin revisar la URL.
- Activa MFA para mitigar accesos no autorizados

Recuerda: un QR pegado en cualquier sitio no siempre es seguro.

5.4 *CLICKFIX* (VENTANAS EMERGENTES)

El *clickfix* es una técnica de ingeniería social que oculta virus y fraudes tras notificaciones, actualizaciones de *software* o alertas de seguridad.

¿Cómo funciona?

- Aparece **un mensaje de error o alerta falsa que genera urgencia**.
- Solicitan **la descarga de un supuesto *software*** (p.ej.: actualizaciones del navegador, antivirus) que contiene *malware* o la **ejecución de comandos** en una consola.
- En un segundo plano (de forma no visible), **te conectan con sitios comprometidos** que descargan *software* malicioso automáticamente en el dispositivo o te redirigen a páginas falsas de inicio de sesión para robar credenciales.

¿Cómo prevenirlo?

- No copies o ejecutes comandos que aparezcan en pop-ups o páginas web.
- No pulses “Fix/Arreglar” ante mensajes inesperados o sospechosos.
- Desconfía de la urgencia.
- Verifica siempre la fuente.

5.5 *BAITING* (CEBO)

El *baiting* utiliza un "cebo" (normalmente físico o digital) para explotar la curiosidad o el interés de la víctima y lograr que ejecute una acción que comprometa su seguridad.

¿Cómo funciona?

- **Creación del cebo:** suele ser un USB infectado u otro elemento atractivo.
- **Distribución:** el atacante lo deja en lugares visibles como oficinas, pasillos o cafeterías.
- **Interacción de la víctima**: la persona conecta el dispositivo o accede al contenido.
- **Compromiso del sistema:** se instala *malware* que permite robar datos, cifrar archivos o espiar la actividad.

¿Cómo prevenirlo?

- No conectes dispositivos desconocidos encontrados en lugares públicos o comunes.
- Descarga solo desde fuentes oficiales y evita *software* "gratuito" sospechoso.
- Mantén antivirus y sistemas actualizados para bloquear amenazas.
- Reporta cualquier cebo sospechoso (USB, enlaces tentadores, "regalos" inesperados).

5.6 ATAQUES COMBINADOS

COMBINACIÓN DE ATAQUES: PHISHING + VISHING

Los ciberdelincuentes suelen combinar varios tipos de fraude para ganar credibilidad y aumentar sus posibilidades de éxito.

¿Cómo funciona este ataque combinado?

- ***Phishing:*** envían un correo fraudulento (por ejemplo, “actividad sospechosa en tu cuenta bancaria”).
- ***Vishing:*** llaman por teléfono para “confirmar” que recibiste el email y guiarte durante el supuesto proceso de solución.
- ***Objetivo final***: que hagas clic en el enlace malicioso del email o proporciones tus credenciales.

Recuerda: Ninguna organización legítima te pedirá tus credenciales (usuario y contraseña) por correo, SMS o teléfono. Si tienes dudas, verifica siempre por otro medio: contacta tú directamente con la entidad usando su web, app o número oficial.

5.7 OTROS ATAQUES

ATAQUES	DESCRIPCIÓN
Post en redes sociales	Los atacantes usan posts y concursos falsos para insertar enlaces maliciosos y robar datos de los usuarios.
Spin o mensajería instantánea	Se ejecuta a través de aplicaciones de mensajería instantánea (*WhatsApp* o *Telegram*) y tiene como objetivo que cliques en un enlace malicioso.
Scareware	Muestra alertas falsas de infección o fallos del sistema para que el usuario instale un *software* malicioso, difundido mediante *pop-ups*, *banners* o correos electrónicos.
Spam en el correo electrónico	Consiste en el envío de correos masivos no solicitados que pueden ser simples molestias, pero también estafas diseñadas para robar credenciales.

6. El auge de la IA en la ingeniería social

La inteligencia artificial generativa está transformando el panorama digital, permitiendo crear textos, imágenes, audios y vídeos hiperrealistas. Esta capacidad también ha sido adoptada por ciberdelincuentes, que ahora desarrollan ataques de ingeniería social mucho más sofisticados y difíciles de detectar.

¡Ha llegado el momento de adelantarse a los ciberdelincuentes!

6.1 *DEEPFAKE*

Los *deepfakes* son imágenes o vídeos creados con IA que suplantan a una persona real con gran realismo. Se generan mediante técnicas de *deep learning*, capaces de imitar expresiones, voz y movimientos. Los ciberdelincuentes los utilizan para engañar, manipular y realizar ataques de ingeniería social.

¿Cómo detectarlos?

- **Desincronización facial:** labios y voz no coinciden perfectamente.
- **Parpadeo anormal:** demasiado poco, demasiado frecuente o poco natural.
- **Luces y sombras incoherentes:** reflejos, brillos y sombras mal integrados.
- **Audio artificial:** voz robótica, sin variaciones naturales o con microcortes.
- **Movimientos extraños:** cabezas “flotantes”, giros rígidos o poco fluidos.

¿Cómo evitar caer en el engaño?

- **Verifica por otro canal:** correo, llamada, mensaje o reunión presencial.
- **Haz preguntas improvisadas:** obligan a respuestas espontáneas difíciles de falsificar.
- **Usa herramientas de detección:** *Deepware Scanner*, Microsoft Video Authenticator.

6.2 *DEEPVOICE*

Un *deep voice* es una técnica de IA generativa que clona voces humanas con gran precisión. Se utiliza para ataques de *vishing*, haciendo solicitudes falsas mediante llamadas o audios manipulados.

¿Cómo detectarlos?

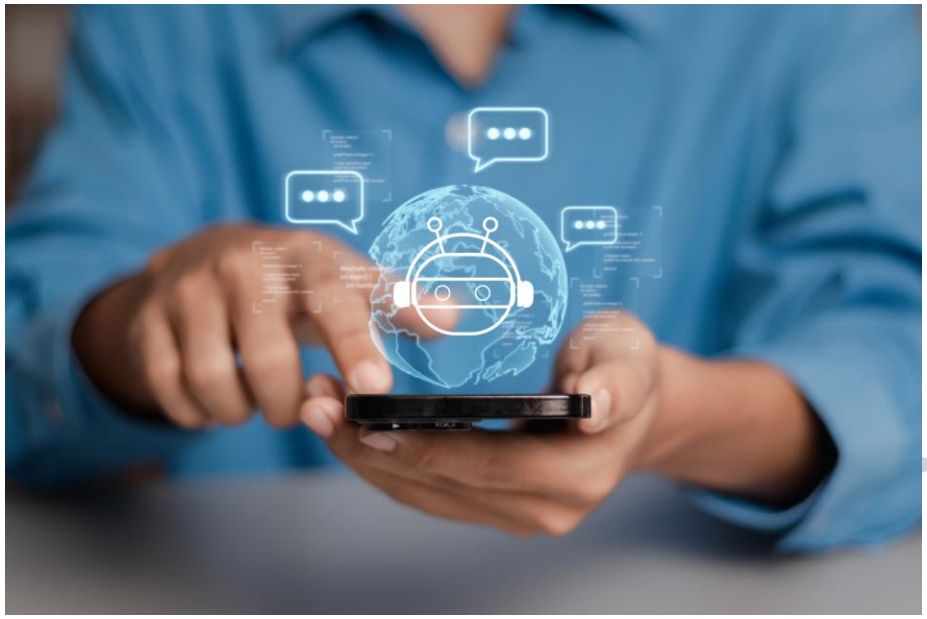
- Voz con poca emoción o cambios poco naturales en la entonación.
- Pausas o silencios inusuales en medio del discurso.
- Errores en pronunciación o acentos inconsistentes.
- Incoherencias contextuales: horarios extraños, solicitudes inusuales o urgentes…
- Voz excesivamente perfecta o uniforme.

¿Cómo evitar caer en el engaño?

- **Verificación en dos pasos:** confirma por otro canal cualquier petición sensible**.**
- **Herramientas de verificación:** *Resemble AI, Deeptrace.*
- **Formación y concienciación:** la mejor defensa ante la ingeniería social.

6.1 *CHATBOTS* MALICIOSOS

Los *chatbots* maliciosos son programas basados en IA diseñados para engañar, manipular o dañar a los usuarios. A diferencia de los *chatbots* legítimos que ayudan en tareas de soporte o automatización, estos se utilizan **con fines fraudulentos**, principalmente para ingeniería social.



Ejemplo: Un *chatbot* malicioso que se hace pasar por el servicio de atención al cliente de *Netflix* y que, a través de *WhatsApp*, te solicita la "verificación de tu cuenta" con el objetivo de robar tus credenciales.

6.1 *CHATBOTS* MALICIOSOS

¿Cómo detectarlos?

- Mensajes urgentes o alarmistas.
- Errores gramaticales o traducciones poco naturales.
- Solicitudes de datos sensibles (contraseñas, información financiera, documentos).
- Respuestas incoherentes, demasiado genéricas o poco naturales.
- Enlaces o archivos sospechosos.

¿Cómo evitar caer en el engaño?

- **Verifica la fuente:** confirma la información por otro canal oficial.
- **No hagas clic en enlaces desconocidos:** utiliza herramientas de análisis de enlaces.
- **Activa la autenticación en dos pasos**: añade una capa de seguridad adicional.
- **No compartas información personal** en chats no verificados.
- **Usa soluciones de ciberseguridad:** extensiones y antivirus que bloquean contenidos maliciosos.
- **Reporta y bloquea** cualquier *chatbot* sospechoso en la plataforma donde lo encuentres.

7. Prevención de los ataques de ingeniería social

Eliminar por completo la ingeniería social es imposible, pero sí podemos mantenernos alerta y aplicar buenas prácticas en nuestro día a día para prevenir este tipo de ataques.

BUENAS PRÁCTICAS

- **Desconfía de mensajes urgentes** o que generen presión para actuar rápido.
- **Verifica la identidad del remitente** por un canal alternativo.
- **No compartas datos sensibles** (contraseñas, códigos, documentos) por correo, chat o teléfono.
- **Revisa enlaces y archivos antes de abrirlos**; evita hacer clic si la fuente te resulta sospechosa.
- **Usa contraseñas seguras** y diferenciadas en cada aplicación.
- Activa **la autenticación en dos pasos** (2FA).
- Mantén tus **dispositivos actualizados** y con herramientas de seguridad activas.
- **Sospecha** de solicitudes inusuales, incluso si parecen venir de alguien conocido.
- **Fórmate** y mantente al día sobre nuevas técnicas de fraude.
- **Reporta** cualquier intento sospechoso a tu equipo de seguridad o soporte TI.

CIBER SEGURIDAD

Y RECUERDA:
LA MEJOR DEFENSA ERES TÚ