

El anzuelo

Cómo nos engañan y cómo dejar de picar



Webinar · Phishing y fraude por engaño



Viernes, 19:40

Cierras el portátil. Vibra el móvil:

«DGT: último aviso. Dispone de 24 horas para pagar su multa antes del recargo.»

Y durante un segundo piensas: **¿y si es verdad?**

Ese segundo es exactamente lo que buscan.

Nadie fuerza la puerta. Se la abren.

- Antes: había que romper sistemas técnicos
- Hoy: basta con engañar a quien tiene la llave
- El pescador no necesita fuerza, necesita un buen cebo

El ataque más sofisticado del mundo empieza con un mensaje de texto.



EL CONTEXTO

El tamaño del problema, en cristiano

Cada 4 min

se gestiona un incidente de ciberseguridad en España: **122.223 en 2025**, un 26 % más que el año anterior.

INCIBE · Balance 2025

6 de cada 10

pymes españolas sufrieron un ciberataque en el último año.



Hiscox · Informe de Ciberpreparación 2025

99 de cada 100

pymes atacadas tuvieron consecuencias. **Solo el 1 % se libró** de cualquier impacto.



Hiscox · Informe de Ciberpreparación 2025

Más de la mitad

de las pymes atacadas sufrió **fraude por desvío de pagos** (53 %). Como nuestro caso 1.



Hiscox · Informe de Ciberpreparación 2025

4 de cada 10

incidentes en España son **fraude online** (45.445). El phishing suma 25.133 casos.



INCIBE · Balance 2025

6 de cada 10

brechas de seguridad tienen detrás a **una persona**: un clic, un error o un engaño.



Verizon · Data Breach Investigations Report 2025

70 Y en una sola simulación nuestra, **70 personas hicieron clic** en un enlace falso. No es una estadística: son compañeros con nombre y apellidos.

El mapa de los anzuelos

Cambia el agua, pero el truco es el mismo

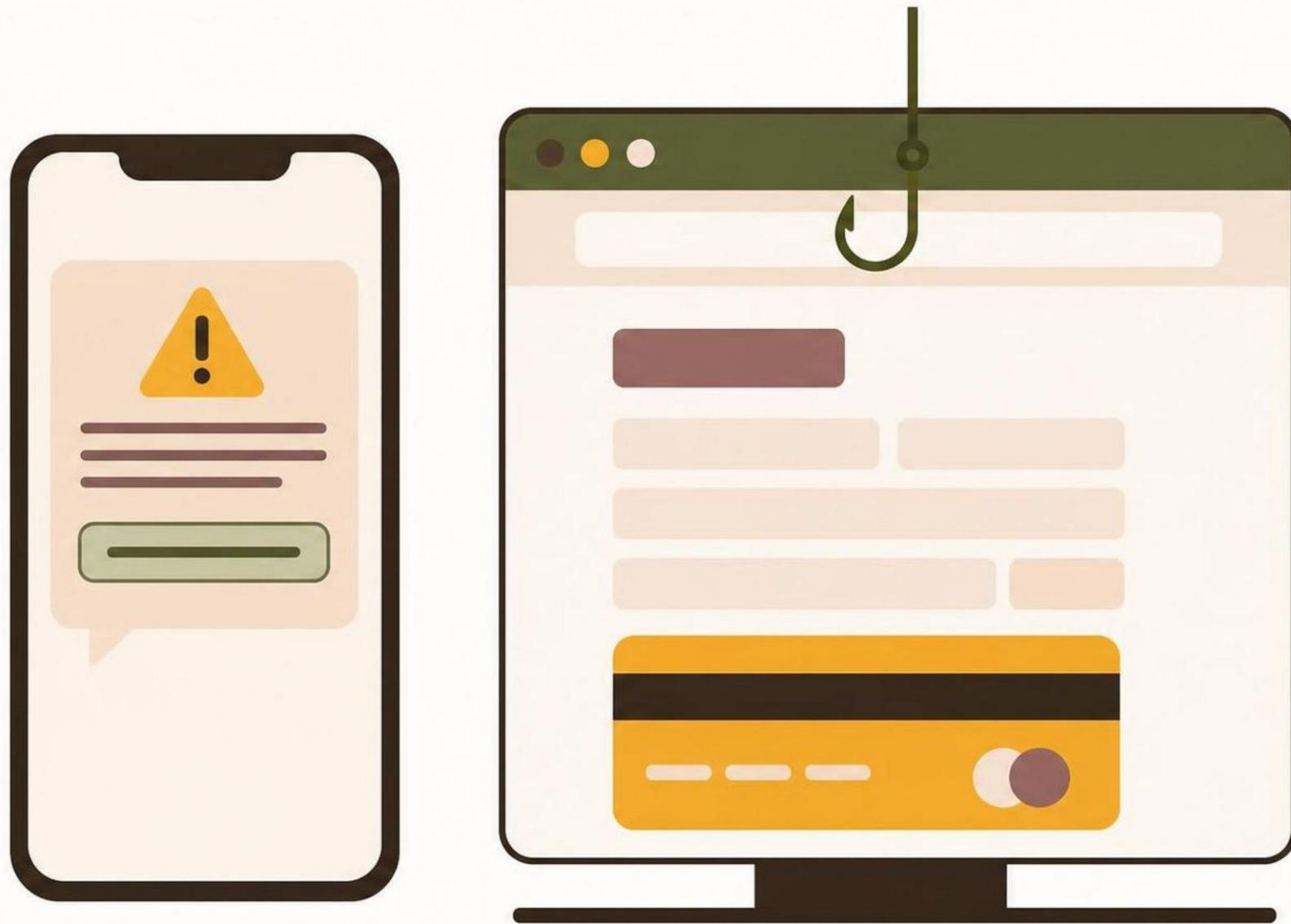


- **Smishing:** SMS
- **Vishing:** llamada de voz
- **Phishing:** correo electrónico
- **Quishing:** código QR
- **Fraude del CEO:** correo corporativo



Smishing: la falsa multa de la DGT

- SMS con 24 horas para pagar antes del recargo
- Enlace a una web clonada que solicita los datos de la tarjeta
- La urgencia artificial impide que te pares a verificar
- **La DGT no cobra multas por SMS**



Vishing: llama «tu banco»

- En pantalla aparece el número real de la entidad (spoofing)
- Avisan de un cargo sospechoso para generar alarma
- Piden el código del SMS «para anularlo» — y así vacían la cuenta
- **Tu banco nunca necesita ese código para bloquear nada**



«Mamá, este es mi número nuevo»

- Mensaje por WhatsApp desde un número desconocido
- Una urgencia inmediata y una petición de transferencia — 2.900 € en un caso real
- Si propones llamar, el «hijo» siempre tiene una excusa para esquivarlo
- **El afecto familiar es el cebo más eficaz que existe**

Fuente: Policía Nacional



Quishing: el QR del parquímetro

- Pegatinas con un QR falso pegadas encima del código real
- Detectado en parquímetros de Alicante y en bicicletas de BiciMAD en Madrid
- El QR redirige a una web de pago fraudulenta
- **Un QR en la calle merece la misma desconfianza que un correo extraño**

Fuente: Policía Nacional, Ayuntamiento de Alicante



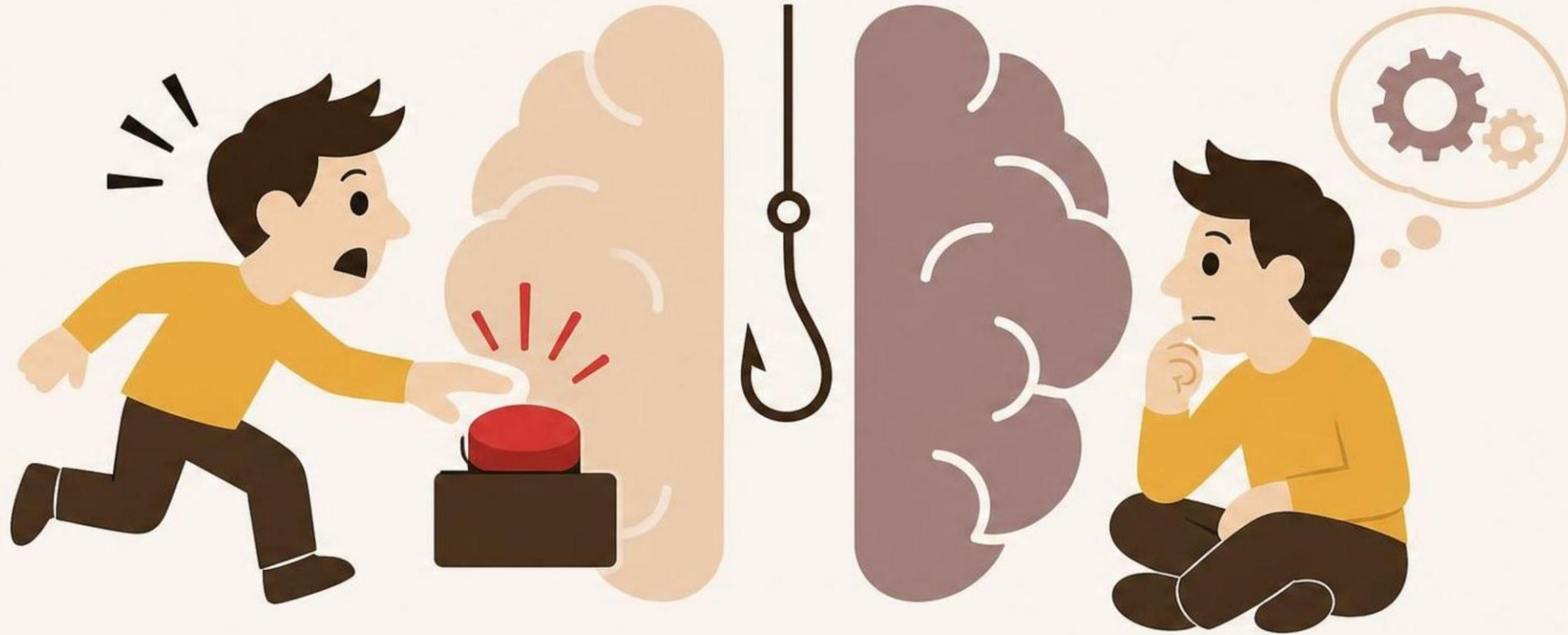
Fraude del CEO

- Los atacantes se infiltran en el correo entre empresa y cliente
- Cambian el número de cuenta justo antes de que llegue la factura
- La víctima paga convencida de que todo es legítimo
- **61 M€ defraudados en España en 2024 por una sola red desarticulada**

Fuente: Ministerio del Interior



¿Por qué picamos?



Nuestro cerebro tiene dos marchas: una rápida y automática que resuelve al instante, y otra lenta que analiza, contrasta y duda.

Los ingenieros del engaño saben cuál prefieren que uses.

El anzuelo está diseñado para que actúes antes de pensar.

Los cuatro cebos



Urgencia: «Tienes 24 horas o perderás el acceso»



Autoridad: «Soy el director financiero, es confidencial»



Miedo: «Han entrado en tu cuenta ahora mismo»



Afecto o recompensa: «Mamá, necesito ayuda» · «Te devolvemos 200 €»



Reconocer el cebo es el primer paso para no morder.

Caer no es de tontos

Estos cebos usan lo mejor de nosotros: queremos cumplir, respetamos a quien manda, protegemos lo que hemos construido y ayudamos a quien queremos.

La ingeniería social no explota debilidades — explota virtudes.

La clave no es desconfiar de todo, sino reconocer cuándo lo usan contra nosotros.

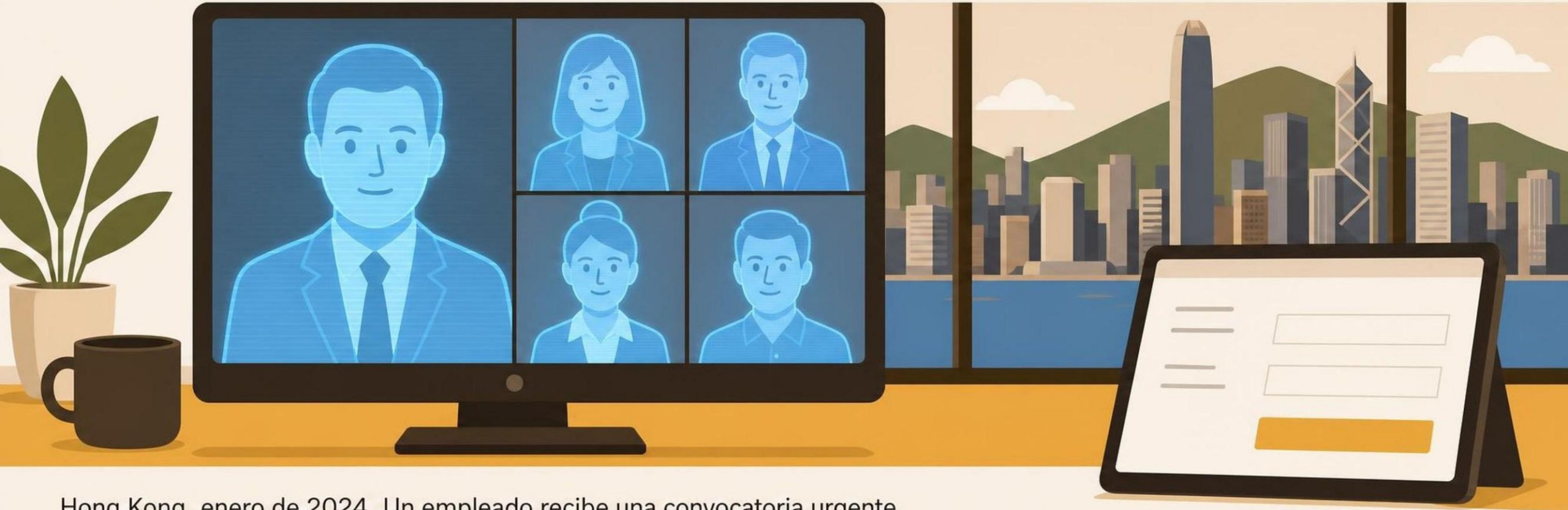


El anzuelo inteligente

- Correos perfectos, sin errores ortográficos, en cualquier idioma
- Voces clonadas con IA a partir de segundos de audio público
- Videollamadas falsas con deepfakes en tiempo real
- Europol: la IA generativa impulsa la ingeniería social a escala industrial
- FBI: unas 22.000 denuncias relacionadas con IA en 2025



Arup: 25 millones en una videollamada



Hong Kong, enero de 2024. Un empleado recibe una convocatoria urgente. En la llamada aparecen el director financiero y varios compañeros habituales. Todos parecen reales. Todos son deepfakes.

15 transferencias. Unos 25 millones de dólares.

La videollamada no fue el anzuelo: fue lo que desactivó la sospecha.

Ferrari: la pregunta del libro



WhatsApp y llamada con la voz clonada del consejero delegado.
El directivo nota algo extraño y decide dudar en voz alta: «*Necesito identificarte.*»

Le pregunta por un libro que le había recomendado en persona.
La llamada se corta en seco.

Una pregunta compartida vale más que cualquier software de seguridad.

La mano del forense

Cinco puntos para inspeccionar cualquier mensaje



- 1 Remitente:** ¿el dominio o número es realmente oficial?
- 2 Enlace:** pasa el cursor — ¿a dónde lleva de verdad?
- 3 Petición:** ¿qué me piden hacer exactamente?
- 4 Cebo:** ¿hay urgencia, autoridad, miedo o afecto?
- 5 Canal:** ¿es la vía habitual para este tipo de comunicación?

Método PARA



Pausa: diez segundos antes de actuar cambian todo



Analiza: quién envía, qué piden y por qué tanta prisa



Reverifica por otro canal: llama tú al número de siempre



Avisa: al departamento de informática, a tu banco o al 017

Cuatro pasos que convierten el instinto en defensa activa.



En la empresa

- **Doble verificación** obligatoria para pagos y cambios de cuenta
- **Pregunta de control** acordada para órdenes por voz o vídeo
- **MFA, DMARC y filtros** como primera capa técnica de apoyo
- **Simulacros y formación** periódicos — la práctica crea reflejo
- **Aplicaciones y herramientas** que ayuden a detectar en tiempo real



Si ya has picado



- Llama al banco de inmediato y bloquea tarjetas y operaciones pendientes
- Cambia todas las contraseñas y activa el doble factor
- Guarda las pruebas: capturas, mensajes, correos
- Llama al **017** y presenta denuncia ante la Policía o la Guardia Civil

La vergüenza es la mejor aliada del delincuente. Actúa rápido, sin culparte.

El cortafuegos humano



La tecnología puede clonar una voz, fabricar una videollamada e imitar cualquier logotipo a la perfección.

Lo que todavía no sabe hacer es dudar en el momento justo. Eso sólo lo haces tú.

No eres el eslabón débil. Eres el cortafuegos más inteligente de toda la cadena.



Fuentes

- INCIBE: Balance de ciberseguridad 2025 y avisos a la ciudadanía
- Ministerio del Interior, Policía Nacional y Guardia Civil
- Europol: IOCTA 2025
- FBI: Internet Crime Report 2025 (IC3)
- Casos Arup, WPP y Ferrari: CNN, Fortune, The Guardian, Bloomberg
- Banco de España: comunicaciones sobre fraude por suplantación

Toda la información es verificable y de acceso público.



Gracias por vuestro tiempo

Una persona informada
es el mejor cortafuegos
contra el phishing

