Fraude en Internet:
Una actividad industrializada

Fernando Fons Gómez

D. Técnicas de Sistemas

Bancaja

Fraude en Internet:
Una actividad industrializada

índice.

- Introducción al fenómeno. Tipología del fraude.
  - spam, scam, troyanos, man-in-the …, … phishing
- Algunas cifras
- ¿Qué hacer?

Introducción al fenómeno. Tipología del fraude

- spam
- scam
- troyanos
- man in the …
  - middle
  - browser
- …
- phishing

Cortesía del Grupo de Delitos Telemáticos
de la Guardia Civil

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

Bancaja

DELITOS INFORMÁTICOS

"Prop Intelec"

"hacking"

"falsificación y fraudes"

"pedofilia"

DELITOS RELACIONADOS CON INFRACIONES DE LA PROPIEDAD INTELECTUAL Y DE LOS DERECHOS AFINES

Delito contra la Propiedad intelectual e industrial (270 y ss.)

DELITOS CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS INFORMÁTICOS

Descubrimiento y revelación de secreto y acceso ilegal (197) Intrusión en sistema informático (197.3)
Apoderamiento de secreto de empresa (278)
Daños en datos y sistema informático (264) DoS (264.2)
Abuso de los dispositivos (270)

DELITOS INFORMÁTICOS

Falsedad documental (390 y ss.)
Estafa informática (248) Uso de tarjetas de crédito (248.2-c)
Defraudación en fluido telecomunicaciones (255 y 256)

DELITOS RELACIONADOS CON EL CONTENIDO

Tenencia y difusión de pornografía infantil (189)
Provocación sexual y prostitución (186 y 187)
Amenazas (169), injurias (208) y calumnias (205)
Apología racismo y xenofobia (607)

Protocolo adicional referente a la apología del racismo y xenofobia (Enero 2003)

Cortesía del Grupo de Delitos Telemáticos de la Guardia Civil

Conductas habituales constitutivas de delito informático

ISACA® Al servicio de los profesionales encargados de la gobernabilidad de la informática Valencia Chapter

Bancaja

"Prop Intelec"

- Descargas ilegales (P2P)
- Venta de música, video y software
- Servidores privados FTP

"hacking"

- Malware
- DDoS
- Botnets
- Espionaje industrial
- Apoderamiento de correo electrónico
- Accesos para vulneración intimidad
- Tenencia de cracks

"fraudes"

- Estafas en el comercio electrónico
- Phishing
- Timos

"contenido"

- Adicción al consumo de pornografía infantil (pedofilia).
- Relaciones engañosas con fines sexuales (Grooming)
- Contenidos de adultos a menores.
- Amenazas
- Injurias y calumnias
- Apología racismo y xenofobia

Cortesía del Grupo de Delitos Telemáticos de la Guardia Civil

Conductas habituales constitutivas de delito informático

ISACA® Al servicio de los profesionales encargados de la gobernabilidad de la informática Valencia Chapter

Bancaja

"Prop Intelec"

- Descargas ilegales (P2P)
- Venta de música, video y software
- Servidores privados FTP

"hacking"

- Malware
- DDoS
- Botnets
- Espionaje industrial
- Apoderamiento de correo electrónico
- Accesos para vulneración intimidad
- Tenencia de cracks

"fraudes"

- Estafas en el comercio electrónico
- Phishing
- Timos

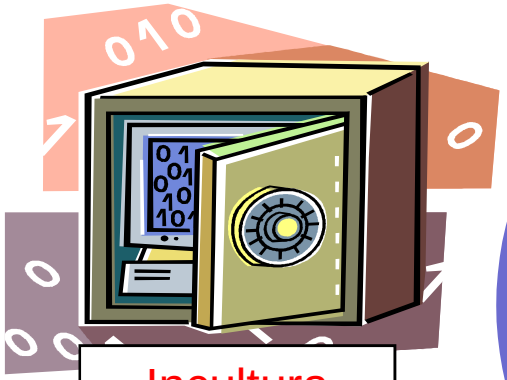
"contenido"

- Adicción al consumo de pornografía infantil (pedofilia).
- Relaciones engañosas con fines sexuales (Grooming)
- Contenidos de adultos a menores.
- Amenazas
- Injurias y calumnias
- Apología racismo y xenofobia

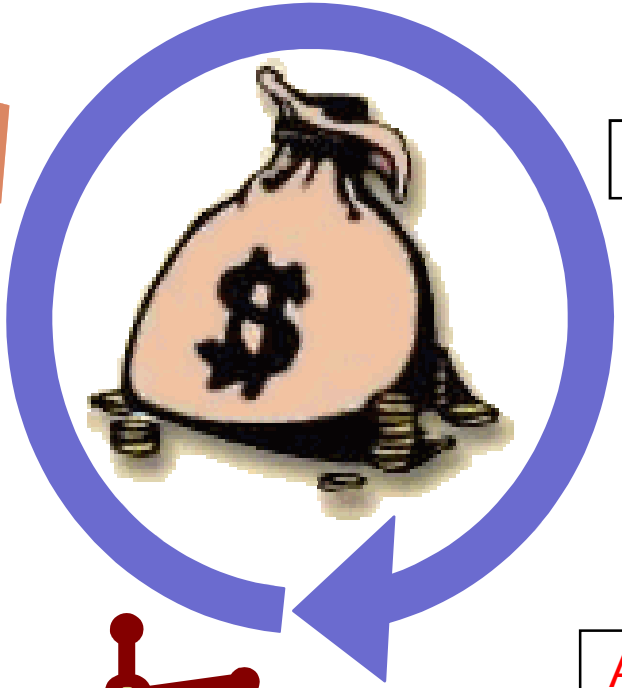
Cortesía del Grupo de Delitos Telemáticos
de la Guardia Civil

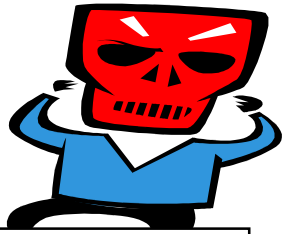
INMADUREZ

SNOBISMO

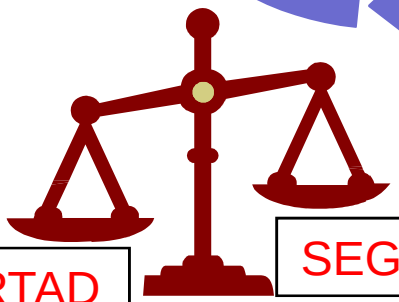


Incultura
seguridad
informática





ANONIMATO

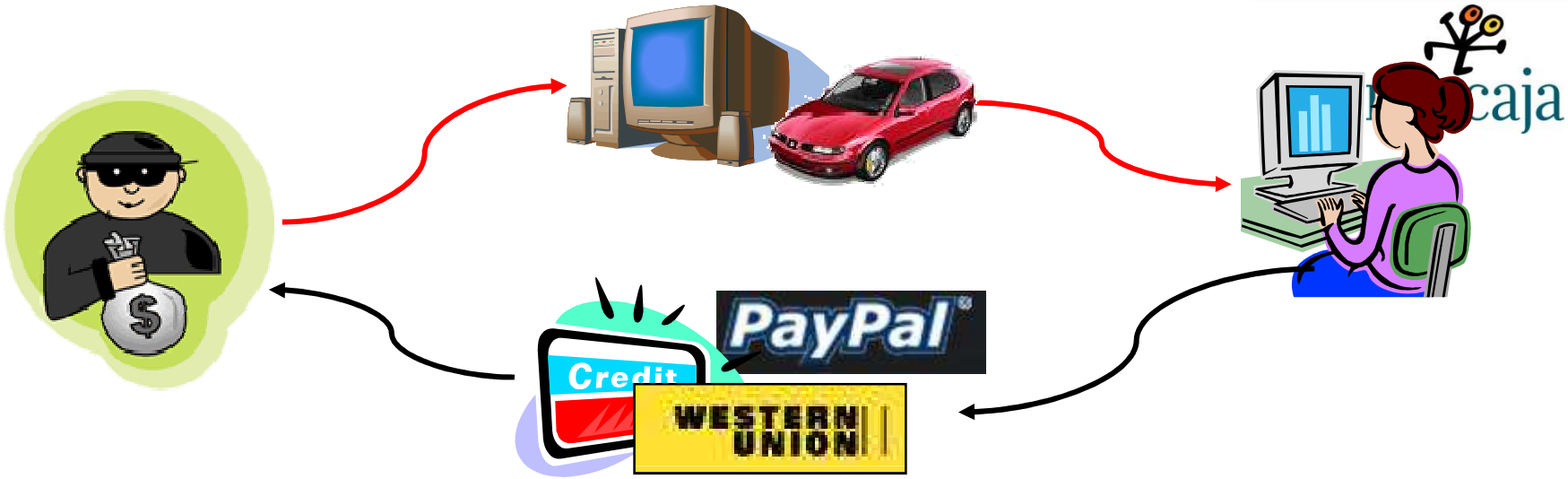


LIBERTAD

SEGURIDAD

Cortesía del Grupo de Delitos Telemáticos de la Guardia Civil

Estafa en el comercio electrónico (C2C)



- Exceso de confianza de compradores
- Fluida comunicación para generar confianza
- Escenarios de engaño (empresas scroll, transportes, copias reales, …) “CARRING”, “HOUSHING”,
- Manipulación portales subastas (credibilidad)
- “Honorarios adelantados”
- Puntos de compromiso (oficinas de empresas de transferencias de fondos)

Cortesía del Grupo de Delitos Telemáticos
de la Guardia Civil

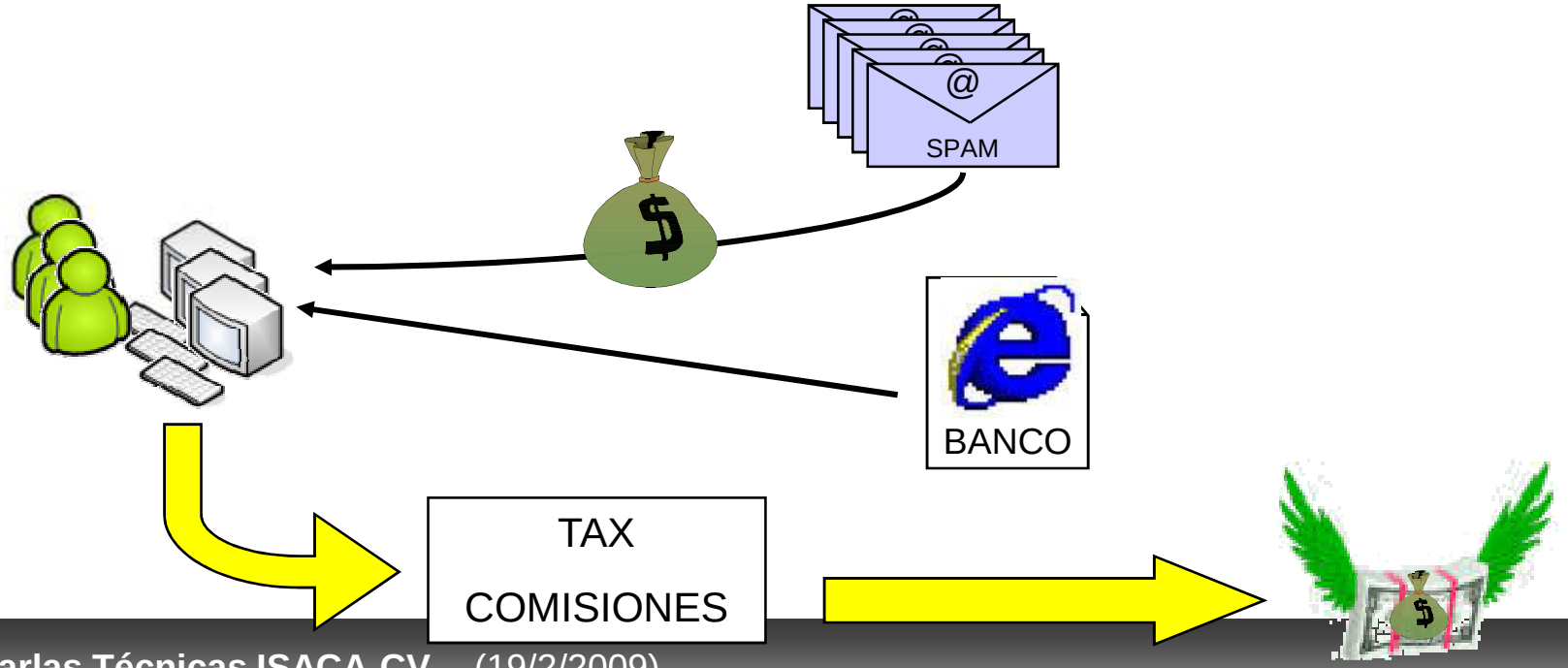
Timos de la red

Exportación del timo a la Red

Nigerianos (Fortunas sin herederos)

Premios de Loterías internacionales

Solidaridad humana, filantropía (Tsunami, Muerte de S.S. el Papa, Katherina)



Cortesía del Grupo de Delitos Telemáticos
de la Guardia Civil

FRAUDE EN BANCA ELECTRÓNICA (PHISHING)

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

Bancaja

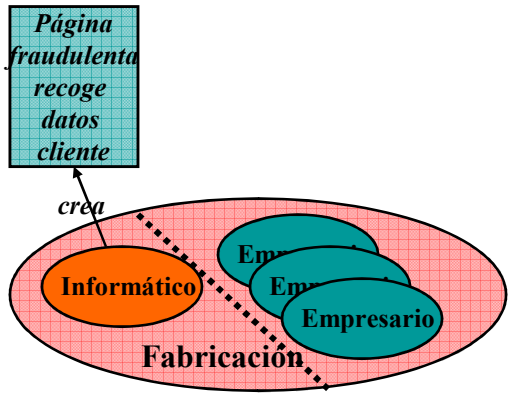
PROCESO DEL FRAUDE:

1. Robo de códigos de acceso a banca electrónica mediante manipulación informática.
2. Usurpación de identidad y orden de transferencia bancaria electrónica a colaboradores financieros (MULAS).
3. Tráfico de dinero hasta defraudador.

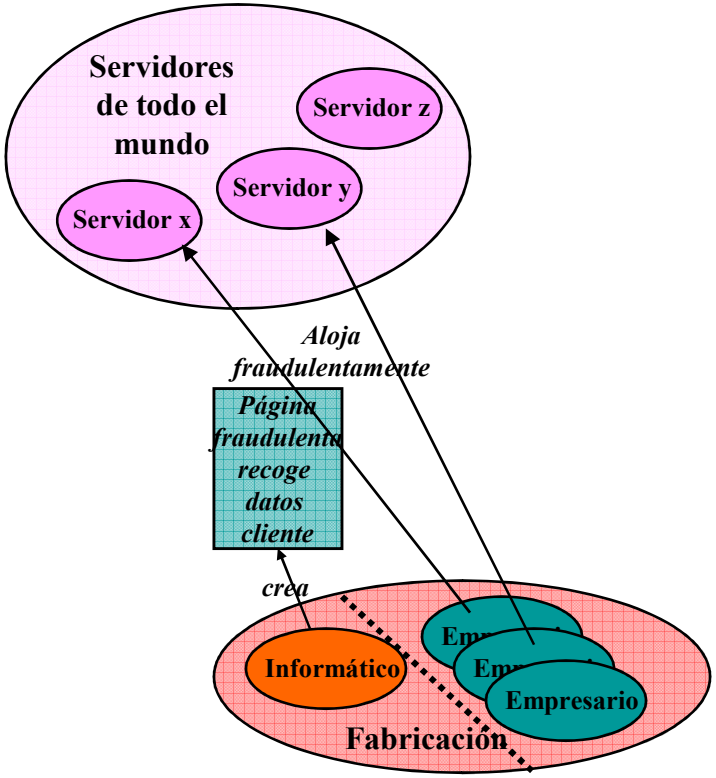
OBJETIVOS (beneficio económico)

1. Datos de acceso a servicio de banca electrónica (login/password/firma electrónica)
2. Datos de tarjetas de crédito (numeración y PIN)
3. Datos de cuentas de acceso a servicios comerciales de la red (subastas, apuestas, ...)

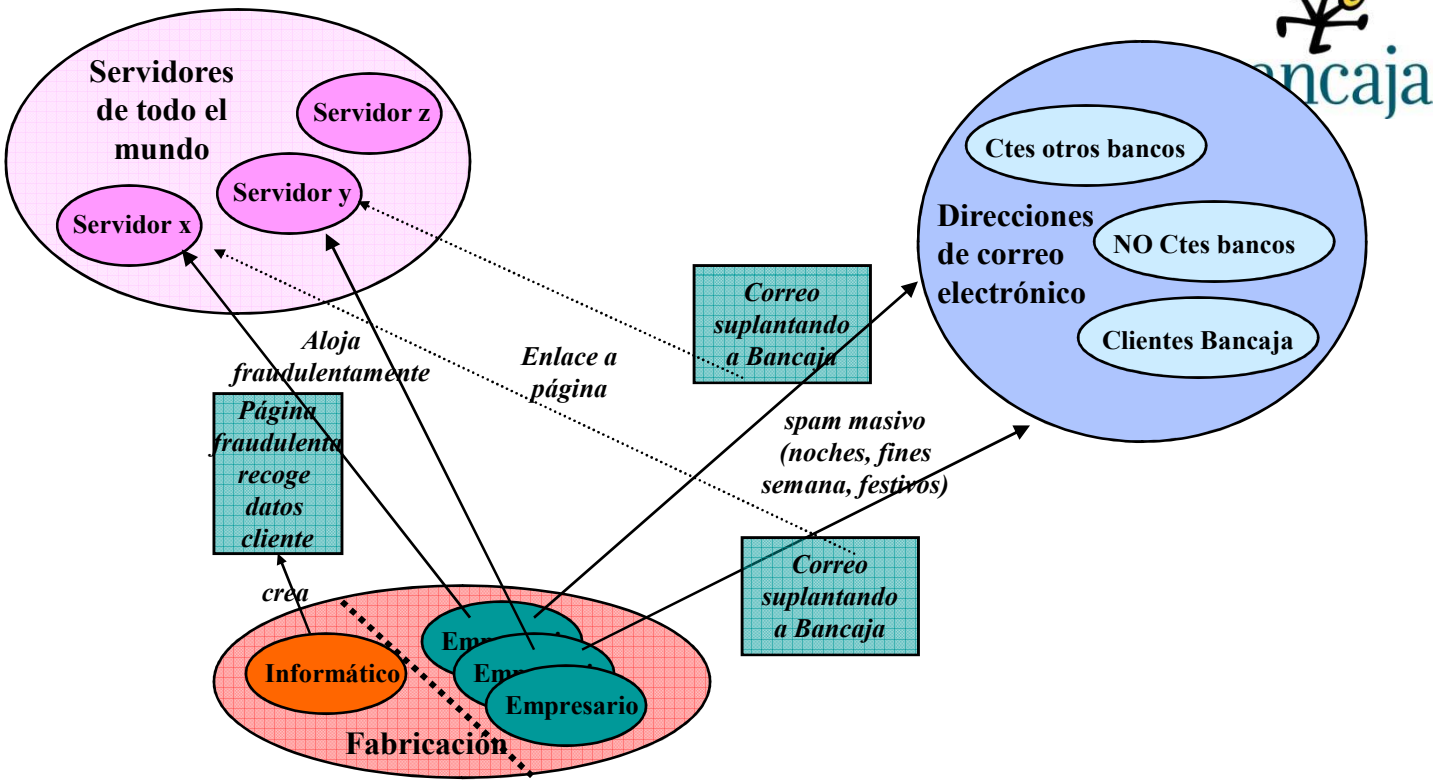
El phishing I



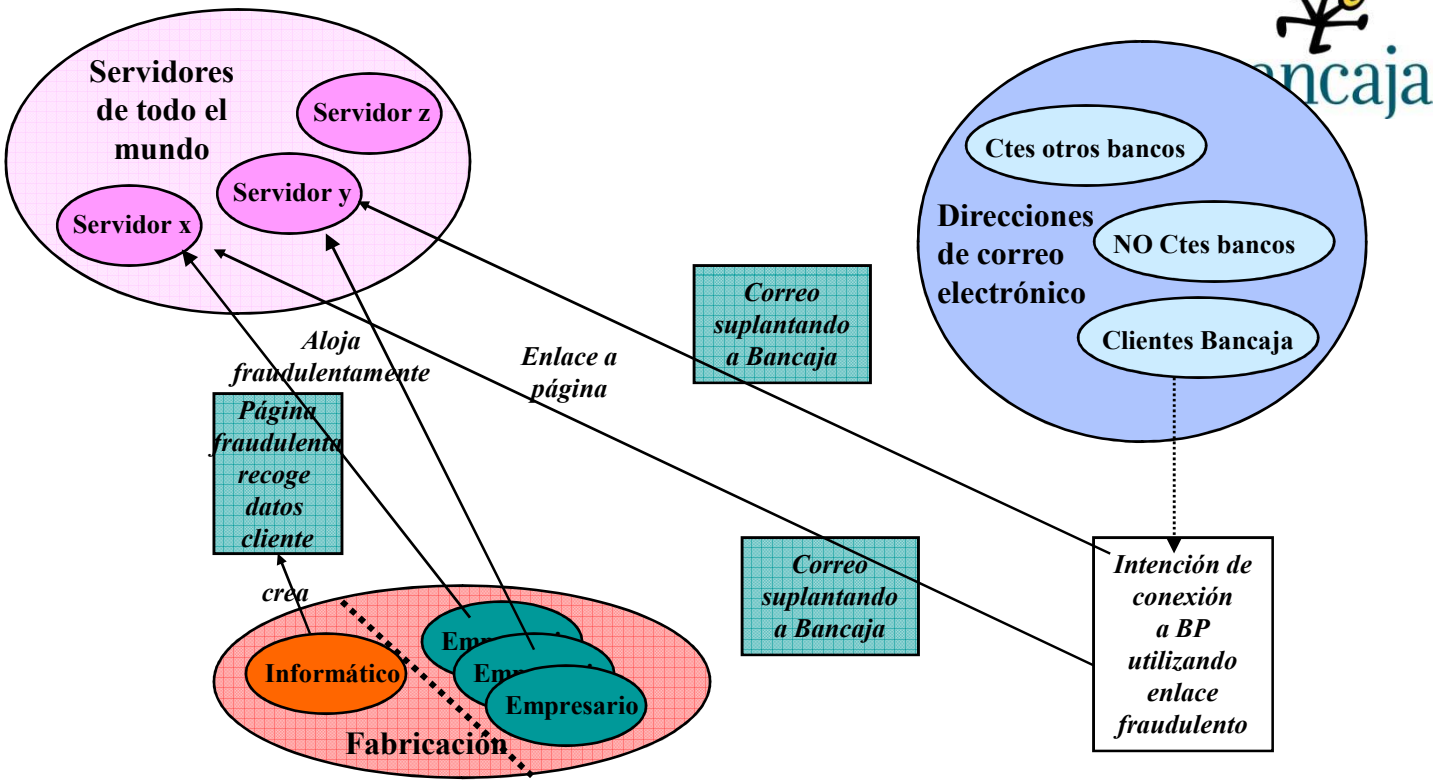
El phishing II



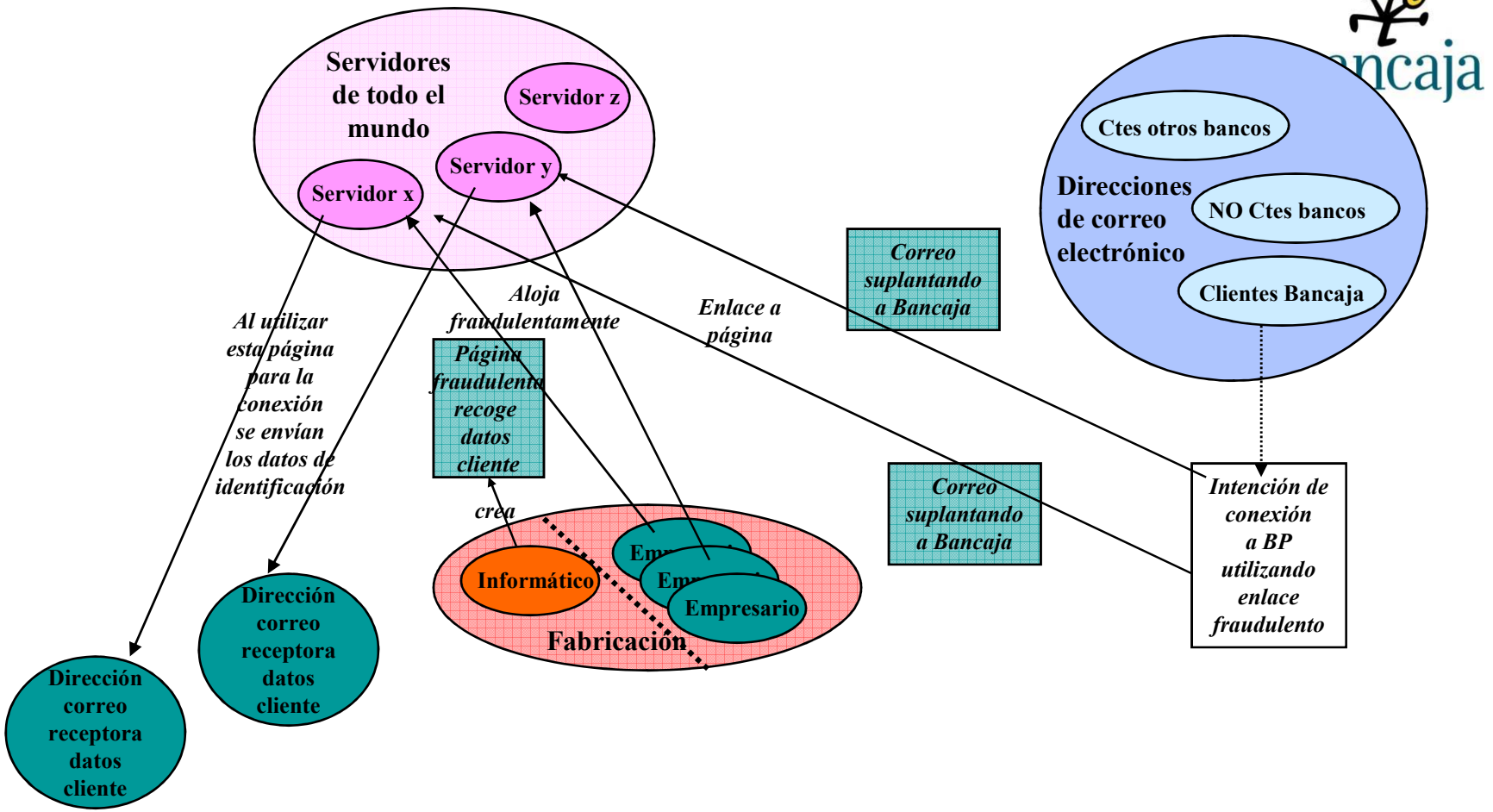
El phishing III



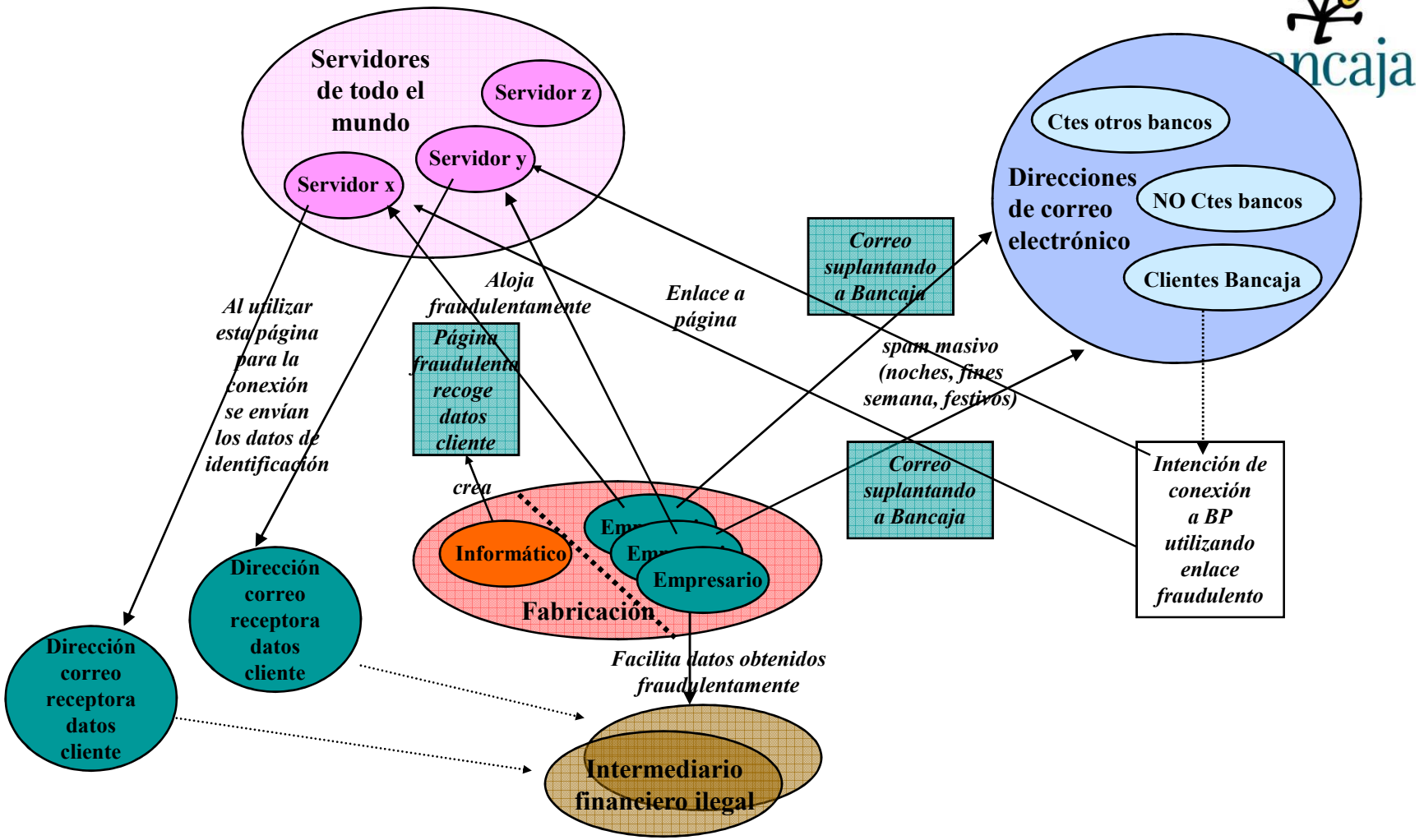
El phishing IV



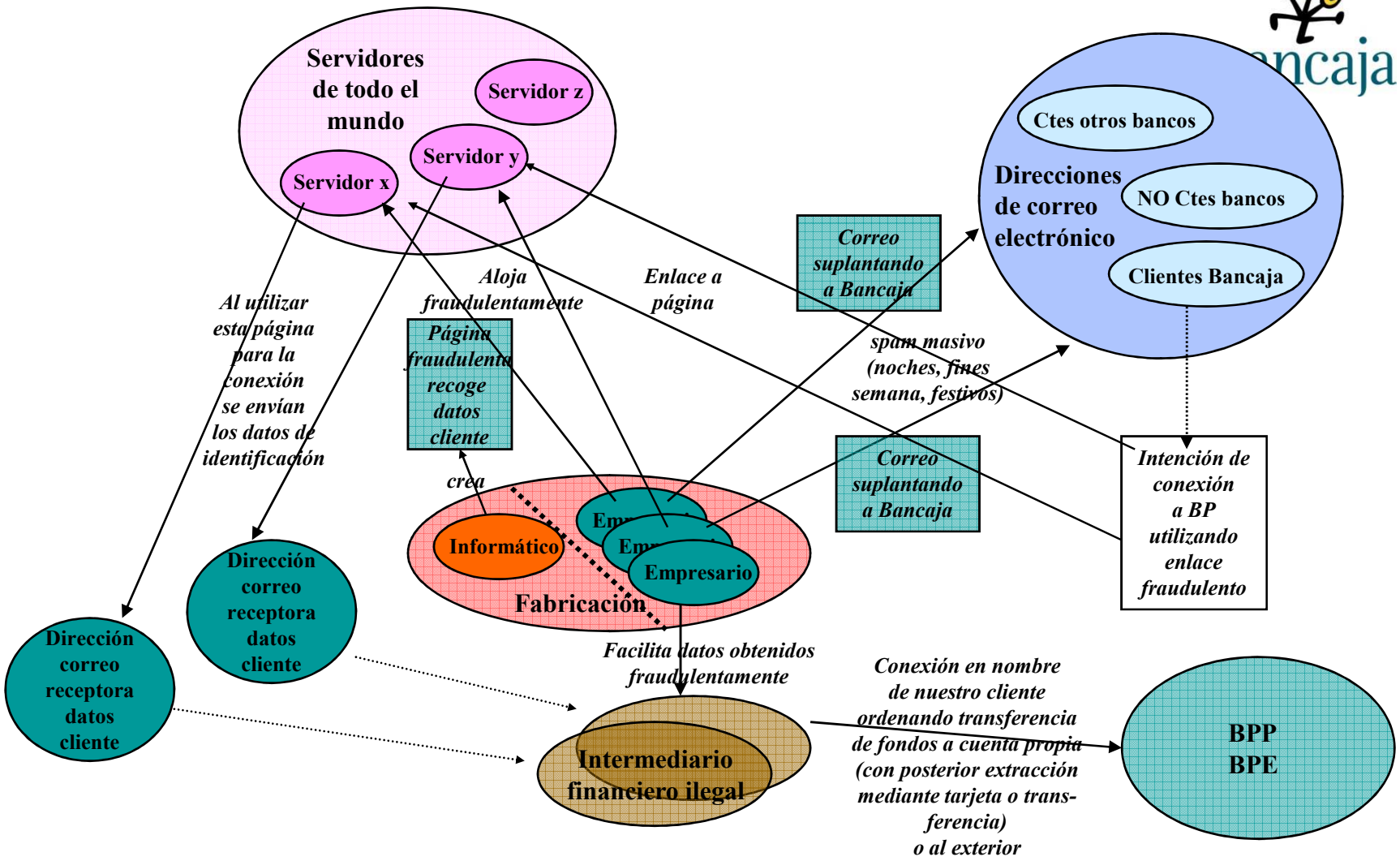
El phishing V



El phishing VI



El phishing VII



Un proceso industrializado: Ciclo de vida de un ataque

- Planificación
  - Objetivos, método, selección de herramientas, …
- Desarrollo del sistema de ataque
  - Se crean los materiales sw y hw, selección destinos, se implantan los sw, muleros, …
- Ataque
  - Envío de correos, recepción de llamadas, man in the …
- Recolección datos
  - Recogida y filtraje de los datos, posible venta, …
- Fraude
  - Suplantación de identidad en acceso a home baking, compra con tarjetas, transferencia fondos, …
- Tareas finales
  - Destrucción evidencias, análisis de resultados, mejora de las herramientas, …
- Reinicio del ciclo

Un proceso industrializado: Del lado de los malos

- Diversas funciones:
  - Inversores / empresarios
  - Desarrolladores.- Existe todo un mercado de malware con SLAs incluido
  - Especialistas en sistemas, red ... seguridad
  - Foros en los que se compra y se vende
  - Muleros
- No es necesario ser un genio para participar … todo se puede comprar y externalizar

Un proceso industrializado: Del lado de los buenos

- Diversas funciones:
  - Especialistas y administradores en seguridad informática
  - Formación en seguridad de la información
  - Fabricantes de elementos de seguridad informática
  - Consultores de seguridad informática
  - Auditores de seguridad informática
  - Compañías de seguridad informática
  - Divulgadores
  - …
- Es necesario ser muy bueno en temas de seguridad para afrontar los retos de cada día. El mercado está muy activo

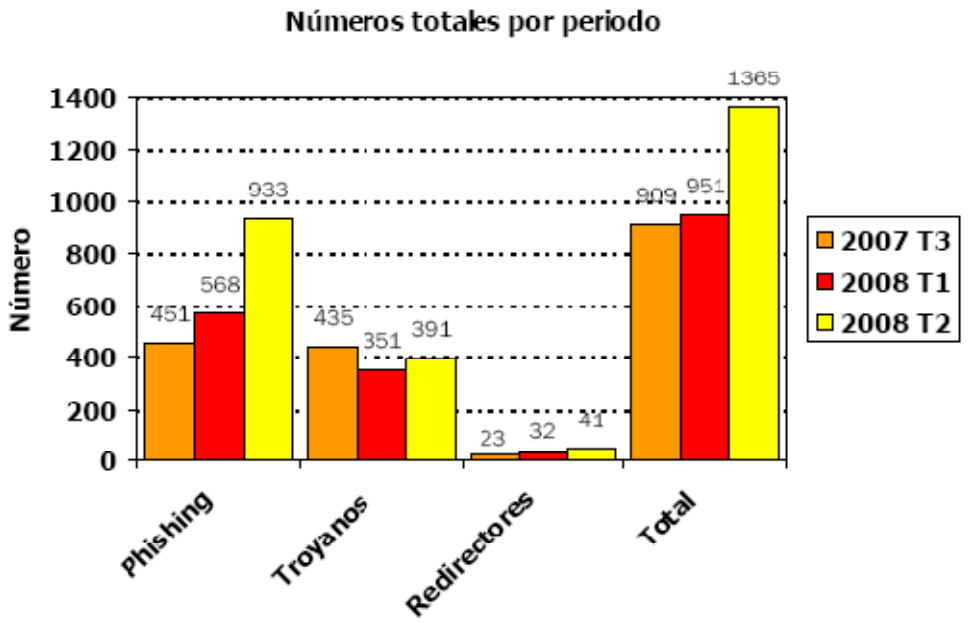
Un proceso industrializado: Del lado de los clientes

- Diversos retos:
  - Mejorar la cultura en temas de seguridad
  - Mantener correctamente instalados los sistemas
  - Mantener correctamente operativos los sw de seguridad
- Es imprescindible utilizar el sentido común y tener un cierto nivel de desconfianza, sin llegar al paroxismo

Algunas cifras

- Nadie quiere dar cifras concretas y precisas por lo que las cifras que se manejan son poco consistentes …
- No obstante:
  - Crecimiento continuo.- *2.5 los casos de phishing en 2008 vs 2007
  - Volumen defraudado …
  - El 98.2% del correo recibido es spam
  - Evolución.- en los últimos meses se aprecia un notable incremento de los troyanos vs ingeniería social
  - Otros mercados.- se observa un notable incremento en la captura de tarjetas para compra por Internet
  - El sector sigue en constante evolución técnica y en cifras

Cifras de un proveedor de servicios español



¿Qué hacer? - Prevención

- Medidas preventivas
  - Nivel de “seguridad” de nuestros “sistemas” por encima de la media:
    - *Nivel de Seguridad perimetral muy alto*
    - *Nivel de Seguridad red interna muy alto*
    - *Identificación de acceso robusta*
    - *Autentificación mediante tercer factor*
      - *¡No nos asegura ante troyanos sofisticados!*
  - Información para los usuarios y empleados
  - Hacking ético y auditorias de seguridad
  - Gestión de la visibilidad de la web …
  - Seguimiento de la industria de la seguridad
  - …

¿Qué hacer? - Detección

- Medidas detección temprana
  - Sistemas de control del fraude
  - Gestión del fraude normalmente apoyándonos en compañías especializadas
    - *Patrullaje*
  - IPS
  - …

¿Qué hacer? - Defensa

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

Bancaja

- Medidas de defensa
  - Autentificación robusta mediante tercer factor
  - Alto nivel de la seguridad de las aplicaciones expuestas a Internet
  - Alto nivel de la seguridad perimetral
  - Gestión del fraude normalmente apoyándonos en compañías especializadas
    - *Cierre de casos de phishing*
  - …

¿Qué hacer? - Reacción

- Medidas reactivas
  - Sistemas de detección del fraude
  - Gestión del fraude normalmente apoyándonos en compañías especializadas
    - *Identificación de clientes afectados por troyanos …*
  - Denuncias
  - Compartir información en foros controlados
  - Seguimiento la industria de la seguridad…

¿Qué hacer? – Otros aspectos

- Tarea continua
  - Los atacantes están evolucionando continuamente sus herramientas y métodos y nos obligan a seguirles
- Alta Especialización
  - Formación continua
  - Externalización de servicios y funciones mas sofisticadas
- Gestión de costes
  - Alineamiento con el negocio … ¿de quien?
- Los clientes
  - Implementar la LISI
  - Definir política corporativa respecto a ellos

Autentificación mediante tercer factor

- Se utiliza un medio físico en poder del usuario.
- La clave generada es de un solo uso y valida durante un corto periodo de tiempo.
- Hay distintos soportes físicos (token, llaves usb, moviles, …)
- Hay soluciones alternativas basadas en certificados digitales (DNI electrónico, smartcards,..)
- Las soluciones basadas en tarjetas de barcos se han demostrado poco robustas frente al phishing.

Bancaja

ISACA®

Al servicio de los profesionales encargados
de la gobernabilidad de la informática

Valencia Chapter

GRACIAS POR SU ATENCIÓN

CISA® 30 THIRTY YEARS OF EXCELLENCE

CERTIFIED INFORMATION SYSTEMS AUDITOR™