sedian

Seguridad Digital
de Andalucía

Presentación

Los peligros del timo del CEO: consecuencias para un organismo público y cómo prevenirlo.

26 de febrero de 2021

Junta de Andalucía

INTRODUCCIÓN

- El timo del CEO es una de las formas más elaboradas de comprometer la seguridad de una organización es el uso de la ingeniería social.
- El uso de argucias, para obtener un beneficio económico, está a la orden del día.
- Es muy importante concienciar a los usuarios de los peligros que corren ante los ataques de los ciberdelincuentes.
- Explicaremos, con detalles, en qué consiste el timo del CEO; cómo identificarlo y mitigar sus efectos.

¿QUÉ ES EL TIMO DEL CEO?

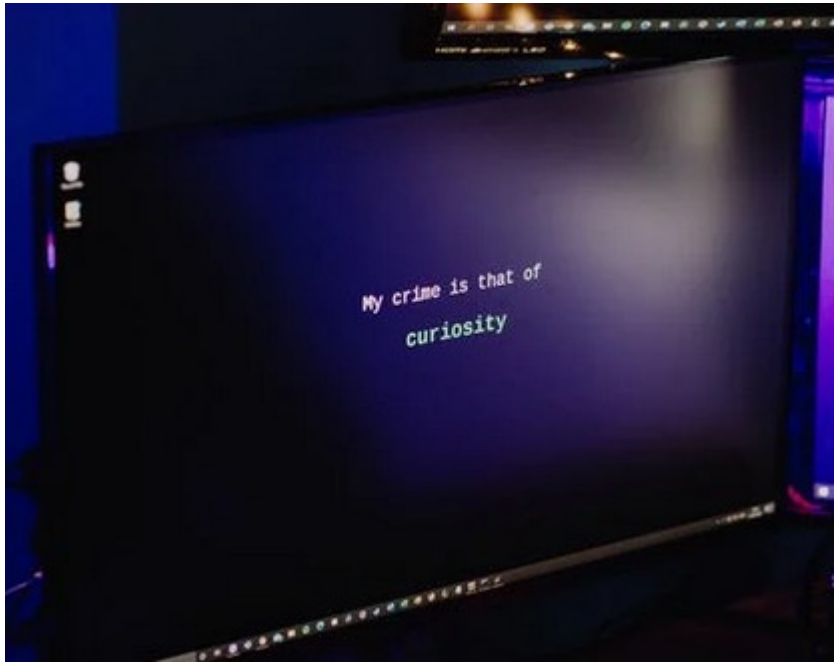
- Utiliza la ingeniería social para conseguir un propósito.
- Tres factores definen el timo del CEO:
  - Urgencia → «Estoy a punto de despegar, por favor, realiza la transferencia antes de que llegue»
  - Suplantación de alto cargo directivo con poder de decisión económica.
  - Confidencialidad de la operación.

FUNDAMENTOS PSICOLÓGICOS DE LA INGENIERÍA SOCIAL

- Respeto a la autoridad → El atacante se puede hacer pasar por un responsable.
- Voluntad de ser útil, ayudar o colaborar.
- Temor a perder algo → Los atacantes aprovechan el hecho de la posibilidad de perder un trabajo al no acatar la orden de un superior.
- Ego →Hacen creer a la víctima que han ganado alguna cosa (timo nigeriano).
- Vanidad → Adulación por conocimientos, posición e influencia.
- Urgencia → Utilizan el desconocimiento de la víctima sobre la situación.

FASES DE UN ATAQUE BASADO EN EL TIMO DEL CEO

- Selección de la víctima.
- Manipulación del empleado.
- Reacción del empleado.
- Impacto.



SELECCIÓN DE LA VÍCTIMA

- Reconocimiento en redes sociales
  - Publicación de vacaciones.
  - Eventos empresariales → Localización de altos responsables → Cuándo no van a estar disponibles.
- Investigación OSINT de la víctima seleccionada:
  - Colaboradores.
  - Transacciones habituales.
  - Noticias de possibles fusiones.
  - Asistencia a eventos importantes.

SELECCIÓN DE LA VÍCTIMA

- Cómo se gana la confianza:
  - Falso directivo → Contactar con empleado → Operación urgente a cuenta no habitual.
  - Empresa de compraventa → solicita transferencia urgente para continuar fusión.
- Qué aprovechan:
  - Directivo ilocalizable.
  - Información pública en Internet.

SELECCIÓN DE LA VÍCTIMA

lun 16/01/2017

Confidencial

Para

Hola ,

Necesito tu ayuda para una operación financiera confidencial.
¿Puedo contar con tu discreción?

(Tenemos que hablar solamente por mail)

Cordialmente

mié 11/01/2017

Confidencial

Para

Hola

Te informo que el tratamiento de una operación financiera confidencial será tratada por ti.
¿Puedes atenderme esta tarde con prioridad?

Atentamente,

Enviado desde mi iPhone

MANIPULACIÓN DE LA VÍCTIMA

- Se envía un correo electrónico al empleado con permisos para realizar transacciones o acceder a información sensible.
- Correo enviado desde dominio similar:
  - melia.com /= melia.com → Aquí se sustituye la L minúscula por una i mayúscula.
  - Iberostar.com /= íberostar.com → Codificación de carácter diferente que puede llevar a confusión; sobretodo en dispositivo móvil.

MANIPULACIÓN DE LA VÍCTIMA

- Estructura del correo eléctronico enviado:
  - Breve introducción → indica que es confidencial.
  - Solicitud de información sensible → operación bancaria de valor alto a cuenta no habitual.
  - Recordatorio de la confidencialidad y la urgencia de la operación.

MANIPULACIÓN DE LA VÍCTIMA

- El correo enviado, por parte del atacante, también puede ir acompañado de lo siguiente:
  - Llamadas o correos confirmando disponibilidad del empleado.
  - Documentos → Acuerdo de confidencialidad
  - Detalles de operaciones realizadas por la empresa → Generar confianza en el empleado con datos de acciones habituales.

MANIPULACIÓN DE LA VÍCTIMA

lun 16/01/2017 [redacted]

[redacted]

Re: RE: Confidencial

Para [redacted]

Perfecto [redacted],

Estamos en este momento efectuando una operación financiera en relación con una adquisición de empresa.
En esta etapa, esta operación debe permanecer estrictamente confidencial, y te obliga no hablar de esto con nadie de momento en la empresa que sea por teléfono o de viva voz.

El anunció legal de esta adquisición tendrá lugar el 30 de enero de 2017 en nuestras instalaciones y en presencia de toda la administración implicadas.

Vas a ser mi contacto con el fin de finalizar esta transacción, que es tan importante para nuestra empresa.

¿Cuáles son los saldos bancarios?

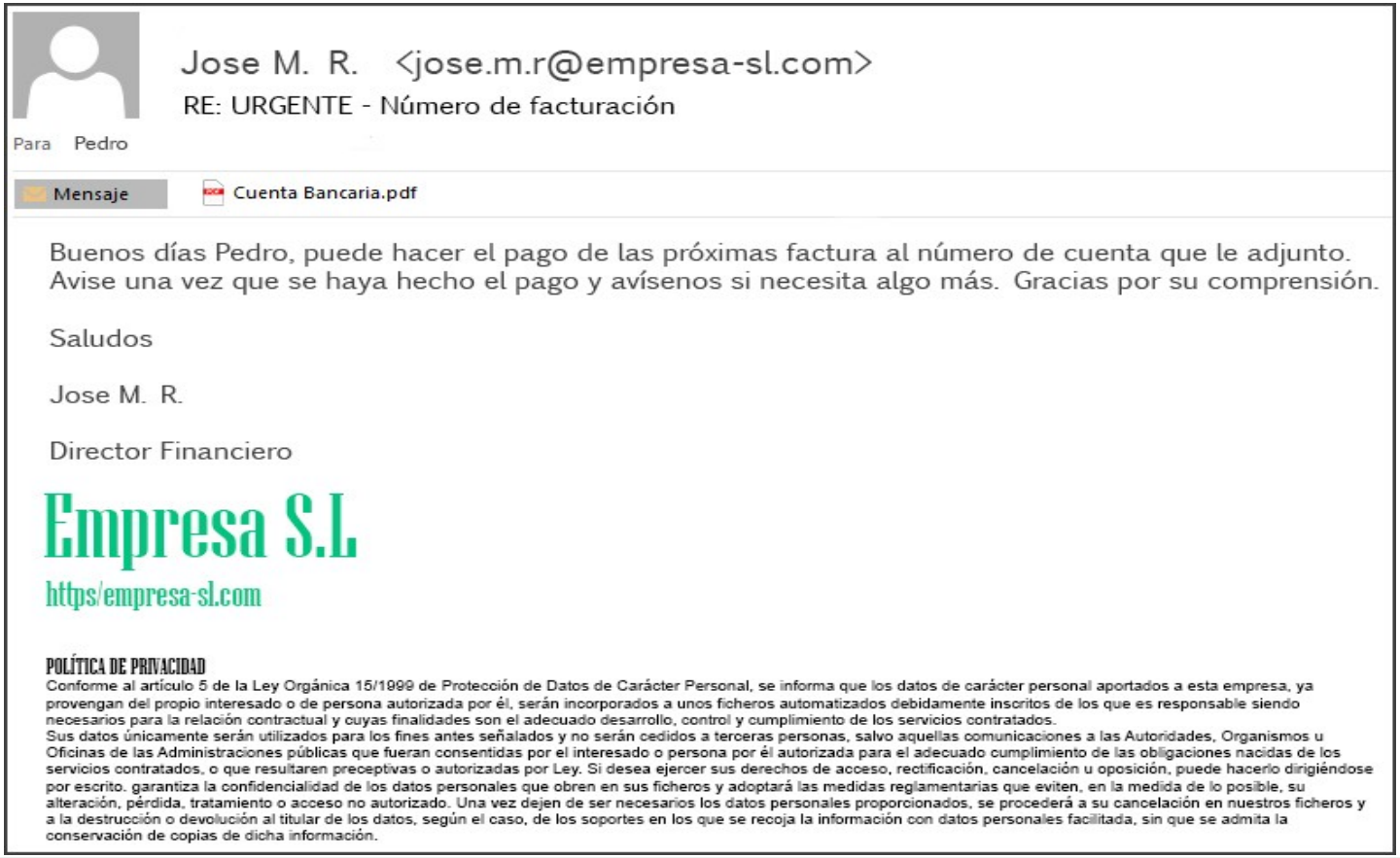
Cordialmente

[redacted]

REACCIÓN DE LA VÍCTIMA

- ¿Por qué la víctima lleva a cabo la acción, muchas veces, sin dudar?
  - Urgencia del mensaje:
    - No se comprueba la dirección del remitente correctamente.
    - No se verifica la ortografía y la gramática.
    - No se detiene a pensar si es el procedimiento habitual.
  - Confianza en los datos aportados.
  - Miedo a represalias → No se comparte con compañeros

REACCIÓN DE LA VÍCTIMA



Jose M. R. <jose.m.r@empresa-sl.com>

RE: URGENTE - Número de facturación

Para Pedro

Mensaje | Cuenta Bancaria.pdf

Buenos días Pedro, puede hacer el pago de las próximas factura al número de cuenta que le adjunto. Avise una vez que se haya hecho el pago y avísenos si necesita algo más. Gracias por su comprensión.

Saludos

Jose M. R.

Director Financiero

Empresa S.L

https/empresa-sl.com

POLÍTICA DE PRIVACIDAD

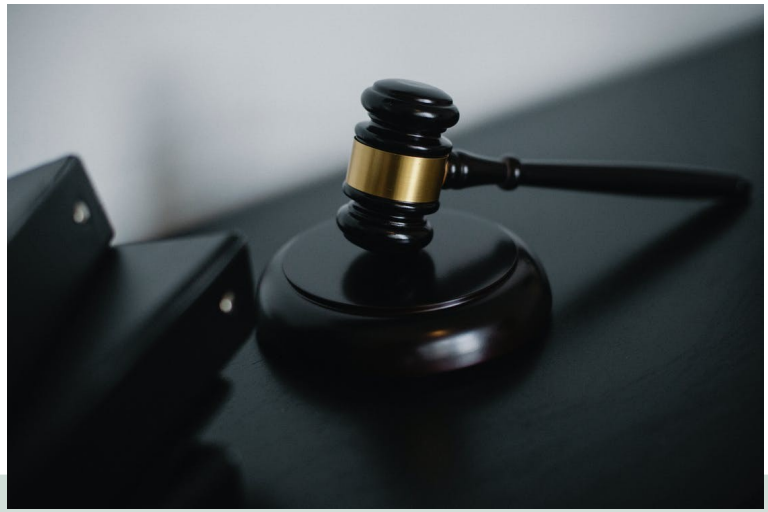
Conforme al artículo 5 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, se informa que los datos de carácter personal aportados a esta empresa, ya provengan del propio interesado o de persona autorizada por él, serán incorporados a unos ficheros automatizados debidamente inscritos de los que es responsable siendo necesarios para la relación contractual y cuyas finalidades son el adecuado desarrollo, control y cumplimiento de los servicios contratados.
Sus datos únicamente serán utilizados para los fines antes señalados y no serán cedidos a terceras personas, salvo aquellas comunicaciones a las Autoridades, Organismos u Oficinas de las Administraciones públicas que fueran consentidas por el interesado o persona por él autorizada para el adecuado cumplimiento de las obligaciones nacidas de los servicios contratados, o que resultaren preceptivas o autorizadas por Ley. Si desea ejercer sus derechos de acceso, rectificación, cancelación u oposición, puede hacerlo dirigiéndose por escrito. garantiza la confidencialidad de los datos personales que obren en sus ficheros y adoptará las medidas reglamentarias que eviten, en la medida de lo posible, su alteración, pérdida, tratamiento o acceso no autorizado. Una vez dejen de ser necesarios los datos personales proporcionados, se procederá a su cancelación en nuestros ficheros y a la destrucción o devolución al titular de los datos, según el caso, de los soportes en los que se recoja la información con datos personales facilitada, sin que se admita la conservación de copias de dicha información.

IMPACTO

- Impacto sobre las personas:
  - En departamentos de RRHH puede afectar al ingreso de las nóminas de los empleados → Suplantación de empleado.
  - Puede causar reclamaciones importantes por parte de los usuarios.

IMPACTO

- Inclumplimiento de leyes o normativas:
  - Revelar datos confidenciales de la organización.
  - No acatar procedimientos de verificación establecidos por políticas en nuestra organización.



IMPACTO

- Impacto sobre la economía:
  - Causa pérdidas económicas en la organización → algunas irrecuperables.
  - Pérdida de ventaja estratégica.
  - Disminución de la facturación.

IMPACTO

- Interrupción de las operaciones:
  - Debido a las pérdidas económicas, nuestra organización, puede dejar de funcionar.

IMPACTO

- Pérdida de confianza:
  - Los trabajadores de la organización pueden ver mermadas sus relaciones personales.
  - La imagen de nuestra organización puede verse seriamente afectada.

SEÑALES DE ALERTA Y MITIGACIONES

- Dudamos del remitente:
  - Comprobaremos de quién es el dominio (algo@dominio.com):
    - Revisaremos si realmente es el dominio corporativo.
    - En el caso de un correo tipo «hotmail» o «gmail» llamaremos a la persona remitente.
  - Comprobación de las cabeceras de los correos:
    - Seguiremos la guía adjunta para entender las cabeceras
      - https://clouding.io/hc/es/articles/360011403640-Entender-una-cabecera-de-correo

SEÑALES DE ALERTA Y MITIGACIONES

- Si el mensaje tiene adjunto sospechoso:
  - Habilitar, en nuestro sistema operativo, la visualización de la extensión del archivo → archivo.pdf.exe
  - Comprobar si tiene algún tipo de virus o troyano utilizando nuestro antimalware (siempre profesional y de pago).
  - Deshabilitar macros en nuestros paquetes ofimáticos.
  - Impedir ejecución de archivos (por parte del departamento TIC)

SEÑALES DE ALERTA Y MITIGACIONES

- Si el mensaje contiene links sospechosos:
  - Copiar el link y analizarlo en VirusTotal -> virustotal.com
  - Enlaces cortos no son fiables. Para analizarlo -> unshorten.me

CONSEJOS

- Tener el sistema operativo siempre actualizado.
- Instalar y configurar un buen antivirus y filtro antispam.
- Desactivar la vista html en las cuentas críticas.
- Concienciar a TODOS los empleados de los peligros de la ingeniería social.
- No abrir correos de desconocidos o que no hayamos solicitado.
- Verificar siempre con la persona que hace la solicitud que esta sea real.
- Passwords fuertes y MFA en la cuentas (válido para las personales).

CONSEJOS

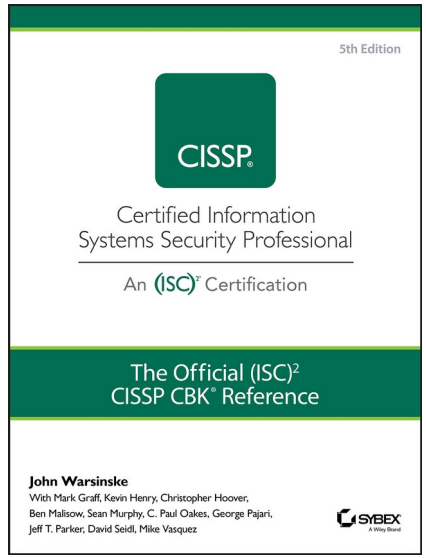
- LEER LA GUÍA DEL INCIBE DE CIBERSEGURIDAD PARA USUARIOS NO TÉCNICOS.

  https://www.osi.es/es/guia-ciberataques

FUENTES

- INCIBE
- ANALISYS AND RISK MITIGATION (CISSP CBK)

INSTITUTO NACIONAL DE CIBERSEGURIDAD



sedian Seguridad Digital de Andalucía

Junta de Andalucía