CCIL

III Congreso sobre
Control Interno Local
Palencia 10/23

Consolidando el modelo. Fortaleciendo la profesión

5 y 6 de octubre

Teatro Ortega

Ciberseguridad en las Entidades Locales. Lecciones para el control interno de los casos de la EMT de Valencia y de la Gerencia Municipal de Urbanismo de Córdoba.

Enrique J. Benítez Palma
Vicepresidente Comisión INNOTEC de FIASEP
Ex Consejero Cámara de Cuentas de Andalucía

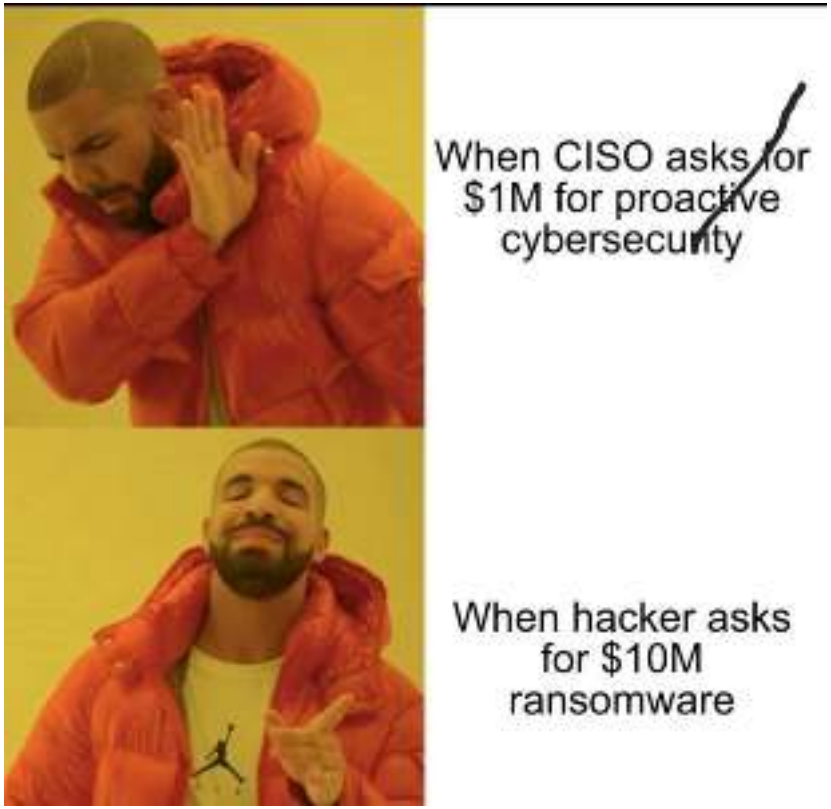
@Ebpal

Esquema de la comunicación

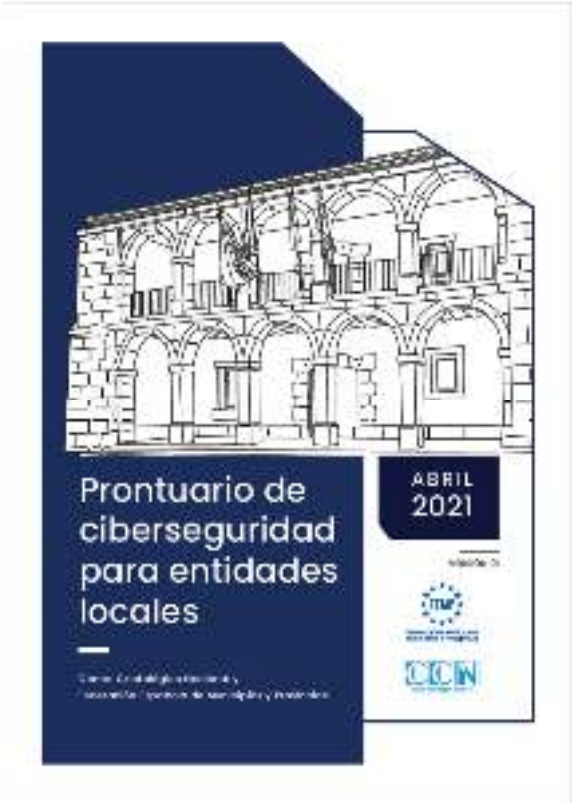
- Hackeos y estafas en el mundo local 2023.
- Hackeo al Ayto. de Jerez de la Frontera (2019).
- Estafa (2021) y hackeo (2023) al Ayto. de Sevilla.
- Estafa a la Gerencia Municipal de Urbanismo del Ayto. de Córdoba (Man in the Middle).
- Estafa a la EMT de Valencia. Seguimiento de la causa abierta por responsabilidad contable (Fraude del CEO o Business Email Compromise).
- Conclusiones y recomendaciones.

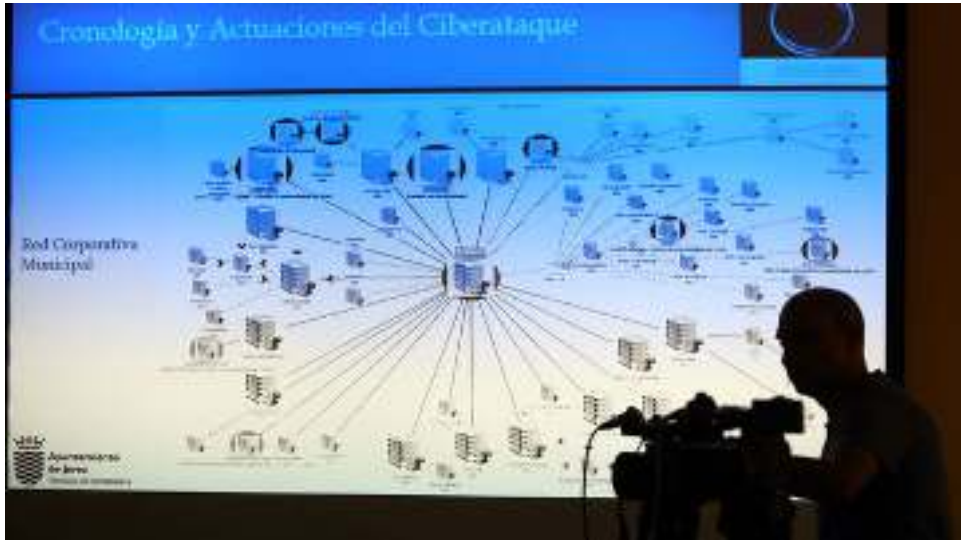
Hackeos y estafas mundo local 2023

- Búsqueda sencilla en Google: “estafa ayuntamiento 2023”, “hackeo ayuntamiento 2023”.
- Casos aparecidos: Navalcarnero (Madrid), Alcalá de Henares (Madrid), Arganda (Madrid), Illescas (Toledo), Telde (Gran Canaria), Vilaseca (Tarragona), Vitoria, Boiro (La Coruña), Palma de Mallorca, Barcelona, Mérida, Requena (Valencia), Cubelles (Barcelona), Diputación de Córdoba, Diputación de Zaragoza.



Ayuntamiento de Jerez (octubre 2019)





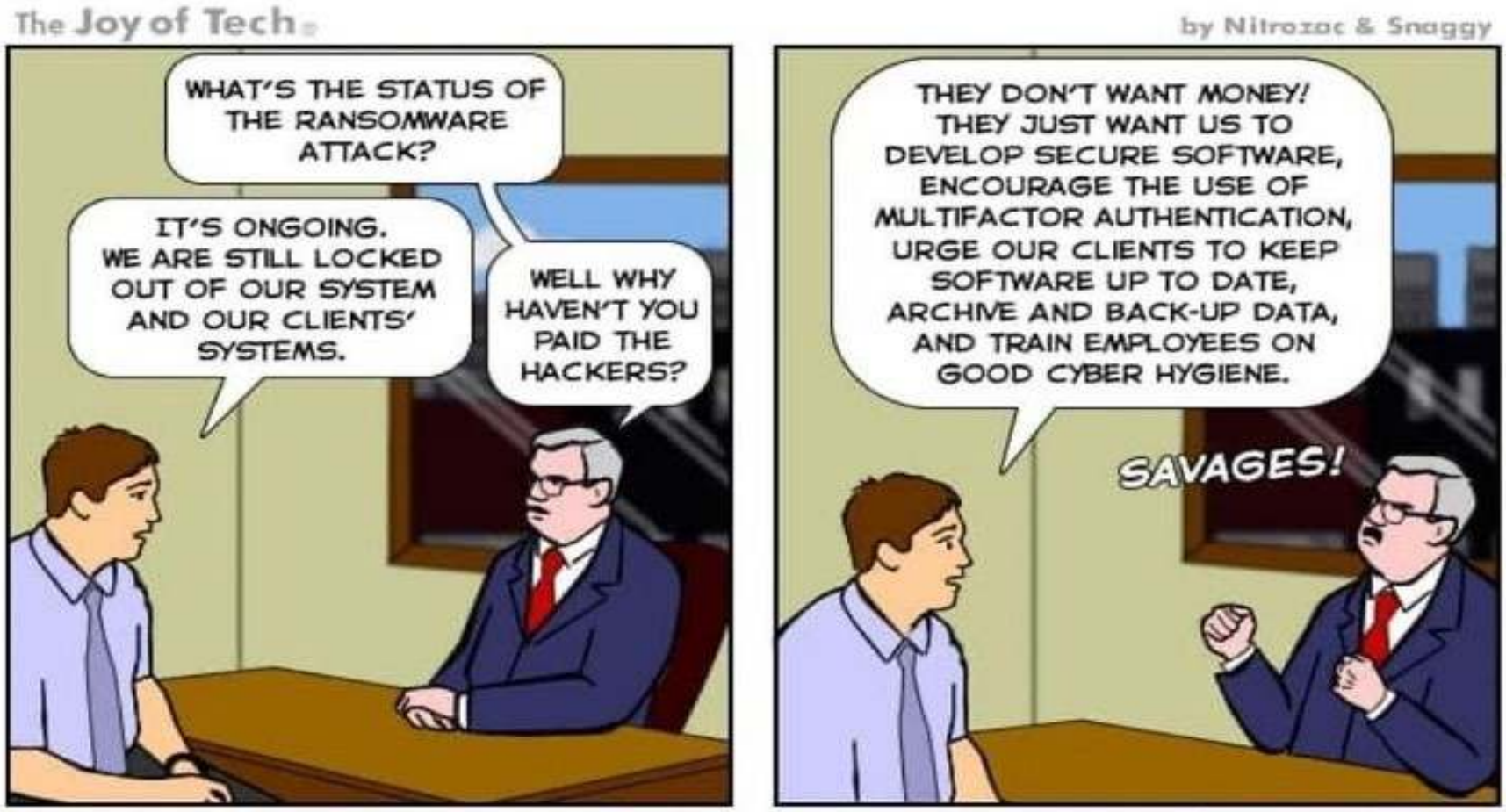
Ayuntamiento de Sevilla: estafa (2021)

- La Casa Consistorial sufrió el verano pasado una estafa en la que están cayendo desde hace unos años decenas de administraciones, instituciones y empresas en España. Se trata del conocido como **Man in the Middle o ataque del intermediario**, **un método que consiste en interceptar las comunicaciones entre dos interlocutores para acceder a la información y luego modificarla a su antojo, sin que ninguno de los afectados lo sepa**. En el caso investigado por la Policía Nacional, todo sigue apuntando a que los ciberdelincuentes interceptaron las comunicaciones del Ayuntamiento y la empresa adjudicataria del contrato de la iluminación navideña. Lo hicieron probablemente mediante la **introducción de un virus informático**.
- Giro de los acontecimientos sobre el timo de los ciberdelincuentes y las luces de Navidad. **El Ayuntamiento ha interpuesto una demanda contra un banco por responsabilidad extracontractual al considerar los servicios jurídicos de la Gerencia de Urbanismo que no obró con la suficiente diligencia** en la ejecución de las transferencias bancarias del contrato de la iluminación navideña 2020-2021 y que ocasionaron que el contratista (la empresa Iluminaciones Elecfes S. L.) no recibiera el abono de **962.797 euros** y este fuera aceptado por un tercero distinto al adjudicatario del contrato.

- Fuente: Diario de Sevilla (Manuel Ruesga), 8 septiembre 2022.
- https://www.diariodesevilla.es/sevilla/Ayuntamiento-reclama-millon-timo-Luces-Navidad_0_1718528136.html

Ayuntamiento de Sevilla: hackeo (2023)

- El Ayuntamiento de Sevilla ha vuelto a las anotaciones en papel y a los trámites presenciales tras sufrir el secuestro de sus sistemas informáticos por un grupo de ciberdelincuentes, según ha confirmado el Consistorio. **Los hackers han reclamado hasta un millón y medio de dólares (1.396.642 euros) al gobierno municipal**, aunque este ha asegurado que "en ningún caso negociará con ciberdelincuentes". Es el segundo ataque con éxito a la web municipal en tres años.
- **Hace dos años, el Ayuntamiento de Sevilla** sufrió otro secuestro, esta vez mediante el conocido como **fraude del CEO [Error]**, por el que los hackers suplantaron la identidad de la empresa adjudicataria del contrato de las luces de Navidad y lograron desviar a sus cuentas el millón de euros de la concesión. Los delincuentes consiguieron monitorizar la correspondencia digital a través de un virus, interceptaron los correos de la empresa suministradora de las luces navideñas, alteraron su contenido y se los remitieron a la Tesorería municipal pidiendo que cambiaran el número de cuenta, informa Eva Saiz**. Cuando el Banco de España detectó un pago de la Administración a una cuenta no habitual, alertó al Consistorio sevillano.**
- Fuente: Raúl Limón / Javier Martín Arroyo, El País, 6 septiembre 2023.
- https://elpais.com/tecnologia/2023-09-06/el-ayuntamiento-de-sevilla-suspende-todos-los-servicios-telematicos-por-un-secuestro-informatico-no-se-negociara.html


The Joy of Tech
by Nitrozac & Snaggy
WHAT'S THE STATUS OF THE RANSOMWARE ATTACK?
IT'S ONGOING. WE ARE STILL LOCKED OUT OF OUR SYSTEM AND OUR CLIENTS' SYSTEMS.
WELL WHY HAVEN'T YOU PAID THE HACKERS?
THEY DON'T WANT MONEY! THEY JUST WANT US TO DEVELOP SECURE SOFTWARE, ENCOURAGE THE USE OF MULTIFACTOR AUTHENTICATION, URGE OUR CLIENTS TO KEEP SOFTWARE UP TO DATE, ARCHIVE AND BACK-UP DATA, AND TRAIN EMPLOYEES ON GOOD CYBER HYGIENE.
SAVAGES!
©2021 Geek Culture
Help us keep the comics coming!
Nurture our work at:
joyoftech.com/support
joyoftech.com

Gerencia Municipal de Urbanismo de Córdoba

- En abril de 2020, la Gerencia de Urbanismo de Córdoba fue víctima de un hackeo, de una estafa informática. **Pagó 428.000 euros que le correspondía a la constructora de la Ronda Norte (Vialex) en una cuenta suministrada por una banda de delincuentes**. En estos momentos, **hay una persona imputada, una joven modelo de Mijas, y el caso está en los tribunales. De toda la cantidad pagada, una parte, unos 50.000 euros, sigue en manos de los estafadores**. Un informe de Intervención ha establecido por primera vez qué falló organizativamente para que la estafa se pudiese llevar a cabo, qué hay que reparar para que algo así no pueda ocurrir de nuevo.

- El sistema con el que se estafó es simple y similar al que le ha costado un millón de euros al Ayuntamiento de Sevilla . Hacerse pasar por un representante de la empresa y pedir que, en vez de que se pague la factura en una cuenta, se haga en otra. **Eso ocurrió el 25 de febrero de 2020 cuando, en un correo genérico de Urbanismo (urbanismo@gmu.cordoba.es) se recibió un presunto mensaje de Vialex remitido desde la cuenta vialex-constructorasaragonesa@oficinaproveedores.es. Urbanismo contestó al mensaje pidiendo certificado bancario de la nueva cuenta. El día 15 de abril quedó hecho el cambio**. Para que esta estafa sea posible, es necesaria una brecha de seguridad. Los estafadores monitorizan que hay pagos a una empresa concreta y es donde actúan para suplantar identidades y cambiar las cuentas corrientes de referencia.
- Fuente: Rafael Ruiz, ABC Córdoba, 22 septiembre 2021.
- https://sevilla.abc.es/andalucia/cordoba/sevi-hackeo-gerencia-urbanismo-cordoba-202109221943_noticia.html

GMU Córdoba: Informe de la Intervención.

- Informe dentro del **Plan Anual de Control Financiero 2020**.
- El primer departamento que respondió ante la Intervención fue el de Contratación, con dos hallazgos relevantes. Por una parte, el jefe de la oficina de contratación de la gerencia municipal de urbanismo reconoce expresamente en su informe, evacuado a instancias de la Intervención, que "**los documentos relativos al reconocimiento de la obligación, ordenación del pago y pago material no constan en el expediente**" (Intervención General Ayto. Córdoba, p. 11). En cuanto a las recomendaciones para este departamento, **la Intervención recuerda la necesidad de mantener la plenitud documental de los expedientes, y sugiere además que se mejora la coordinación entre los diferentes departamentos de la gerencia de urbanismo, ya que una comunicación adecuada podría haber evitado la suplantación de la cuenta del proveedor y el intercambio de correos con los estafadores**.

GMU de Córdoba: Informe de la Intervención

- Respecto al Servicio de Economía de la GMU, está compuesto por dos economistas y dos auxiliares administrativos. Uno de estos economistas, adjunto a la jefatura de servicio, llevaba en comisión de servicio mucho más tiempo del año previsto en la legislación vigente (RD 364/1995, citado por la Intervención). Además, se hace énfasis en el artículo 6 del RD 128/2018, que establece que **la responsabilidad administrativa de las funciones de contabilidad, tesorería y recaudación corresponde a puestos de trabajo reservados a funcionarios de Administración local con habilitación de carácter nacional**. Además de recuperar para la Tesorería municipal estas competencias hasta entonces ejercidas por el Servicio de Economía de la GMU, **aquí ubica el informe de la Intervención el apartado de las posibles responsabilidades penales y contables, *por un importe no recuperado de 52.523'28 euros*.**

GMU de Córdoba: Informe de la Intervención

- Finalmente, **la investigación sobre el procedimiento de alta/modificación de terceros ha permitido averiguar un hecho tan habitual en muchas administraciones locales como inaudito al verlo reflejado en papel: "cualquier usuario de la aplicación SICALWIN con acceso a la entidad Gerencia de Urbanismo, y no sólo los pertenecientes al Servicio de Economía de la GMU, dependiendo del perfil de usuario que tenga, puede tener acceso al módulo de Terceros y puede modificar datos de los mismos. La modificación de datos de Terceros no deja rastro en SICALWIN, en cuanto a qué usuario la ha realizado**" (Intervención General Ayto. Córdoba, p. 20).
- El informe finaliza con severas recomendaciones relacionadas con la plenitud documental de los expedientes, la organización interna del Servicio de Economía de la GMU y el procedimiento de alta/baja/modificación de terceros, y cifra con exactitud el perjuicio económico causado a la entidad. De esta manera, el último párrafo sostiene lo que sigue: "**Entiende esta Intervención que la determinación del alcance de las posibles responsabilidades (penales y contables) en que haya podido incurrir cualquier empleado público procedería una vez dirimidas las actuaciones en vía judicial penal, momento en que podrá determinarse el daño causado. Todo ello prestando especial atención a los plazos legales de prescripción y sin perjuicio de las posibles responsabilidades disciplinarias que pudieran depurarse en el seno de esta organización pública**".
- Fuente: Enrique Benítez y Carlos Vaz: "Estafas informáticas y responsabilidad de los empleados públicos. Tres casos reales del sector local". Revista CUNAL, nº 245, 2021.

EMT de Valencia: ¿víctima o culpable?

- **La Razón, 20 de agosto de 2023**: “De víctimas a culpables: se abre la puerta a que los funcionarios asuman el coste de los ciberataques contra la Administración”.
- Celia Zafra, víctima del fraude del CEO, condenada a pagar los 4 millones que le estafaron a la EMT de Valencia. «Es como si vas a denunciar un robo y te dicen que la culpa es tuya por dejarte robar».
- El caso de Celia es el paradigma de la estafa del CEO. Celia trabajaba para la EMT desde hacía 38 años y era directora del negocio de administración desde hacía 20, puesto en el que se ocupaba de facilitar a la dirección del área el balance y la cuenta de resultados mensual, aunque tenía dos responsables superiores: la dirección de finanzas y la dirección del área de gestión. Sin embargo, ella fue la elegida por los defraudadores para perpetrar el delito.
- «Se puso en contacto conmigo un presunto abogado de Deloitte, firma con la que trabajábamos en Valencia, pero este era de Madrid, y me dijo que había una operación con una empresa de China. Me insistió que era absolutamente confidencial y que el importe total de la operación eran 9 millones, pero antes de que el presidente de la compañía lo anunciara en rueda de prensa había que tener abonado el 60%», explica Celia.

EMT de Valencia: ¿víctima o culpable?

- Cuando los delincuentes iniciaron la estafa, el gestor de la compañía estaba de vacaciones. Al volver de sus días de descanso, toda la operativa pasó a él. «**Cuando hicimos la novena transferencia**, el gestor me pasó un modelo para que lo firmasen los apoderados porque era necesario para que la EMT autorizase al banco a tramitar las operaciones», señala Celia, que al no poderse comunicar directamente con los apoderados, mandó el modelo al presunto abogado y este lo devolvió con las firmas. No obstante, **el gestor quiso pedirle confirmación telefónica a alguno de los apoderados y ahí fue cuando el gerente les alertó de que no había estado firmando ninguna transferencia**.
- Celia asegura que durante el proceso comentó al supuesto abogado que no estaba «cómoda trabajando con tanto secreto». Además, «también ponía en copia a la jefa de gestión» para dejar constancia de los trámites que estaba realizando. Sin embargo, **cuando se destapó el fraude la EMT de Valencia dirigió todas las responsabilidades contra ella, pese a no formar parte de la alta dirección, lo que derivó en la condena por la que se le reclaman los 4 millones de euros perdidos y 300.000 en costas e intereses**.
- Fuente: Inma Bermejo, La Razón, 20 de agosto 2023.
- https://www.larazon.es/economia/victimas-culpables-abre-puerta-que-funcionarios-asuman-coste-ciberataques-administracion_2023082064e15b559598e30001ca84a7.html

EMT de Valencia: el Tribunal de Cuentas

- **23 de junio de 2021**: Auto nº 17 del año 2021 dictado por la Sala de Justicia. Recurso del artículo 48.1 de la Ley 7/1988 nº 7/21, Actuaciones Previas nº 93/20. Ramo: Sector Público Local.- (Empresa Municipal de Transportes de Valencia, S.A.U.-EMT-), Valencia.
- **3 de junio de 2022**: Sentencia nº4 del año 2022 dictada por Departamento Tercero de Enjuiciamiento. Sentencia dictada en el procedimiento de reintegro por alcance nº C102/2021, SECTOR PÚBLICO LOCAL, (E.M. de T. de V., S.A.U. - EMT) V.
- **24 de noviembre de 2022**: Sentencia nº 14 del año 2022 dictada por SALA DE JUSTICIA. Recurso de apelación núm. 25/2022 Procedimiento de reintegro por alcance Nº C-81/2021. Ramo: Sector público local (Empresa Municipal de Transportes, S.A.U. -EMT-) Valencia.
- **31 de mayo de 2023**: Sentencia nº 4 del año 2023 dictada por Sala de Justicia. Recurso de apelación nº 29/22, interpuesto contra la Sentencia nº 4/2022, de 3 de junio, dictada en el procedimiento de reintegro por alcance nº C-102/2021, del ramo de Sector Público Local (Empresa Municipal de Transportes de Valencia, S.A.U. -EMT-). VALENCIA.

EMT de Valencia: el Tribunal de Cuentas

- Sentencia 4/2022.
- Hecho probado segundo: En el momento de las actuaciones, la autorización electrónica y mancomunada para los pagos recaía en el Gerente de la EMT y la Directora del Área de Gestión. A doña C. Z. R., como Directora de Negociado de Administración, solamente le correspondía la preparación material de los pagos y la subida de los correspondientes ficheros a la plataforma de la banca en línea.
- Hecho probado tercero: El 3 de septiembre de 2019, en ausencia de sus superiores jerárquicos con competencia para la ordenación de pagos, el G. (que se encontraba de vacaciones) y la D. del A. de G. (de baja por lactancia) se produjeron los hechos siguientes:
  - Una persona desconocida contactó por teléfono con doña C. Z. R., diciendo actuar en nombre de un abogado de la sociedad D., le informó de una supuesta adquisición de dos empresas chinas y le pidió información sobre quiénes eran las personas autorizadas en la EMT para aprobar pagos, mediante la banca en línea. En la conversación, le encareció la necesidad de guardar confidencialidad.

EMT de Valencia: el Tribunal de Cuentas

Posteriormente, doña C. Z. R. recibió dos correos electrónicos, procedentes de cuentas creadas a nombre del supuesto abogado de la sociedad D., que le remitía las instrucciones para realizar la operación y un acuerdo de confidencialidad, con arreglo al cual debería abstenerse de comunicación alguna al respecto con sus superiores. Pretendía actuar en nombre del Presidente de la EMT, confirmaba la operación de compraventa y reiteraba la necesidad de guardar confidencialidad sobre el asunto.

En virtud de esas instrucciones y **sin realizar otras comprobaciones, doña C. Z. R. remitió a los presuntos estafadores documentos de la EMT que les facilitaban muestras de las firmas del G. (un escrito dirigido al Ayuntamiento en el que constaba su firma) y de la D. del A. de G. (una factura con la firma de conformidad), así como sus documentos nacionales de identidad escaneados**.

Igualmente, elaboró y les proporcionó un borrador de carta de ordenación de transferencia de pago de una factura correspondiente a la supuesta operación.

A continuación, **utilizando los datos proporcionados por doña C. Z. R., los estafadores le reenviaron un documento supuestamente original de la carta de ordenación de transferencia de pago, con las firmas falsificadas del G. y de la D. del A. de G., que la Sra. Z. remitió a la entidad bancaria C. para que procediera al pago de la primera factura, por valor de 334.419,07 euros, con destino a una cuenta del B. de C. en H. K., de titularidad de una supuesta sociedad extranjera.**

A pesar de que no correspondía a la práctica bancaria establecida por la EMT con la entidad bancaria C., la entidad financiera tramitó manualmente la transferencia.

- *Se realizaron en total 8 transferencias manuales, por importe de 4.054.971,98 €. El importe total de la operación, de no haberse detenido, habría doblado esta cantidad.*

ENCUESTA

- https://wall.sli.do/event/hKZeZ3D365CnXKgPuUSfQ7?section=989d3a26-9233-42c2-a8d2-98bdd45873bf

III Congreso sobre Control Interno Local
Palencia 10/23
CCIL

Conclusiones y recomendaciones (1)

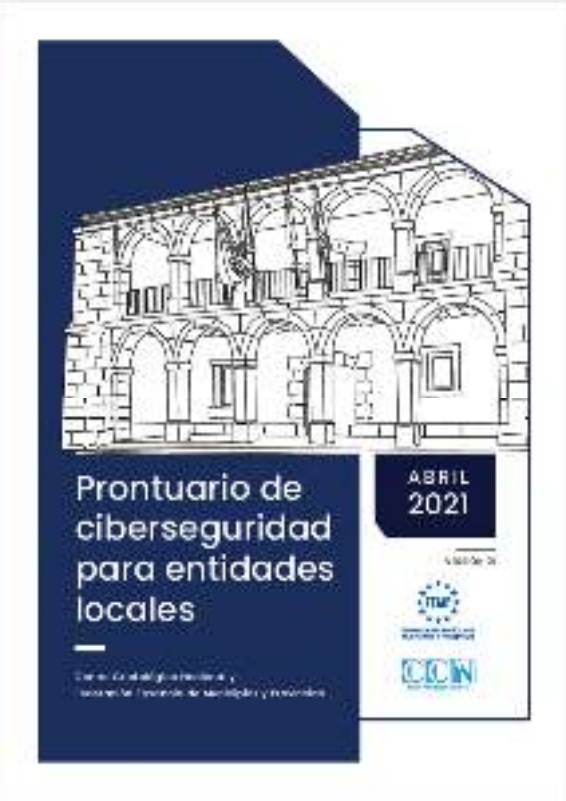
- Estafas y fraudes más comunes: Man in the Middle (Ayto. de Sevilla, GMU de Córdoba, y varios más), y Fraude del CEO (EMT de Valencia).
- ¿CÓMO PODEMOS PREVENIR LOS ATAQUES “MAN IN THE MIDDLE”?
- INCIBE nos ofrece en su web una serie de recomendaciones que podemos seguir para evitar sufrir este tipo de ataque del intermediario, como medida de protección. Algunas acciones que podemos seguir para minimizar el riesgo son las siguientes:

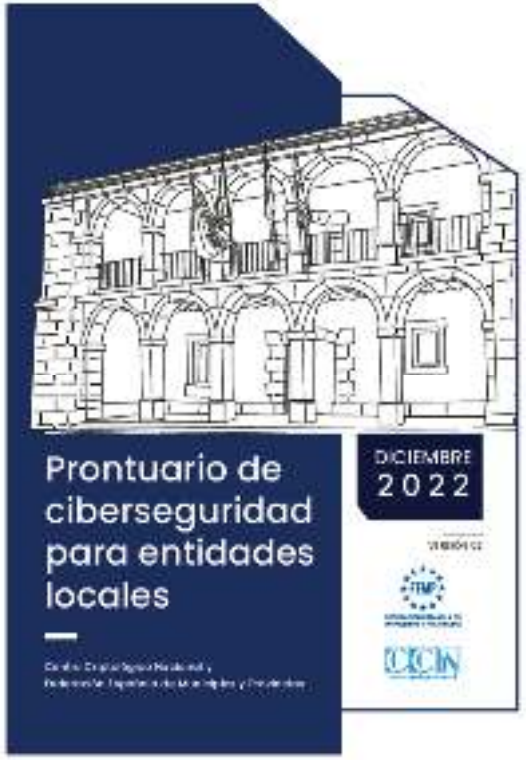
  - Acceso a sitios web seguros con certificado. (Aquellos que empiezan por HTTPS, comprobando que el certificado pertenece a la compañía o entidad que corresponde).
  - Actualizar continuamente el software de nuestros equipos, especialmente el sistema operativo y el navegador.
  - Utilizar contraseñas robustas y habilitar la autenticación en dos pasos.
  - Evitar conectar a redes wifi abiertas (Hoteles, espacios públicos). En el caso de acceder a este tipo de conexiones, evitar difundir información personal conectándose a redes sociales o banca online.
  - Evitar abrir enlaces de correo procedentes de fuentes desconocidas.
  - Actualizar el antivirus en los equipos corporativos, realizando escaneos frecuentemente.

Conclusiones y recomendaciones (2)

- Lo primero que se recomienda mirar es la **urgencia** de la solicitud en el correo electrónico.
- Muy a menudo, las campañas de phishing tienen un carácter urgente incorporado a la solicitud y amenazan con **consecuencias nefastas si no se actúa con prontitud-** algo así como “confirme sus credenciales o su cuenta será desactivada”.
- Conviene también **fijarse en si es una solicitud atípica para el remitente.** ¿Se solicita información personal o confidencial que normalmente no se recibe? ¿Se está pidiendo cambiar la cuenta utilizada para recibir pagos por transferencia? **Cualquiera de estas solicitudes atípicas debería ser marcada con bandera roja para el destinatario.**
- **Una de las mejores medidas que pueden tomar los individuos para evitar que se comprometa una cuenta es confirmar que el supuesto remitente del correo electrónico sospechoso realmente envió la comunicación. Puede hacerlo llamando para confirmar la solicitud incluida en correo electrónico**. Es muy importante tener una confirmación real antes de cambiar la cuenta en la que se está transfiriendo el dinero o antes de proporcionar las credenciales de acceso. Usar una forma alternativa de comunicación – el teléfono, o algún otro medio – que esté diseñada para llegar a la persona legítima.
- Siempre es peligroso buscar la confirmación por correo electrónico, porque puede que, sin percatarnos, la comunicación sea directamente con el delincuente.

Para empezar:





ORGANIZADORES

Diputación DE PALENCIA

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

IGAE

COLABORADORES

PALENCIA

COSITAL

LA LEY

PATROCINADORES

Platino

SPAI innova

Oro

SCIPION

audifilm GRUPO AL

Plata

FAURA-CASAS

inter pública

oesia