UAEM

EL CORREO ELECTRÓNICO

Principales fraudes y riesgos

DTIC

metared

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

www.incibe.es

ÍNDICE

ÍNDICE DE FIGURAS

1. EL CORREO ELECTRÓNICO COMO HERRAMIENTA

El correo electrónico es una herramienta de comunicación imprescindible para el funcionamiento de la universidad. Sus beneficios son evidentes: accesibilidad, rapidez, posibilidad de enviar documentos adjuntos, etc., aunque cuando se creó, no se hizo pensando en su uso actual, ni en la seguridad.

Como toda herramienta de comunicación es necesario definir su uso correcto y seguro, ya que, además de abusos y errores no intencionados **el correo electrónico se ha convertido en uno de los medios más utilizados por los ciberdelincuentes para llevar a cabo sus ataques.**

Es habitual que a los buzones llegue spam, correos de tipo phishing o correos que suplantan entidades o personas. En estos casos utilizan técnicas de ingeniería social[1] para conseguir sus fines maliciosos, por ejemplo, infectar el equipo o incluso toda la red de la universidad, robar credenciales, datos bancarios o información confidencial.

En un correo malicioso, tanto el remitente, como el asunto, el cuerpo, los adjuntos o los enlaces que contiene, pueden estar diseñados para engañar al receptor del mensaje.

1. La ingeniería social utiliza cualquier reclamo para captar nuestra atención y conseguir que actuemos de una determinada forma. ¿Y cómo lo hacen? Se ganan nuestra confianza y, muchas veces, se aprovechan de la curiosidad o el morbo que nos produce conocer y manejar cierta información, del respeto a la autoridad, de la voluntad de ser útil, del temor a perder algo, de la vanidad o crean situaciones de urgencia. Así, consiguen manipularnos y hacernos actuar de la forma que ellos quieren.

2. TIPOS DE CORREOS FRAUDULENTOS

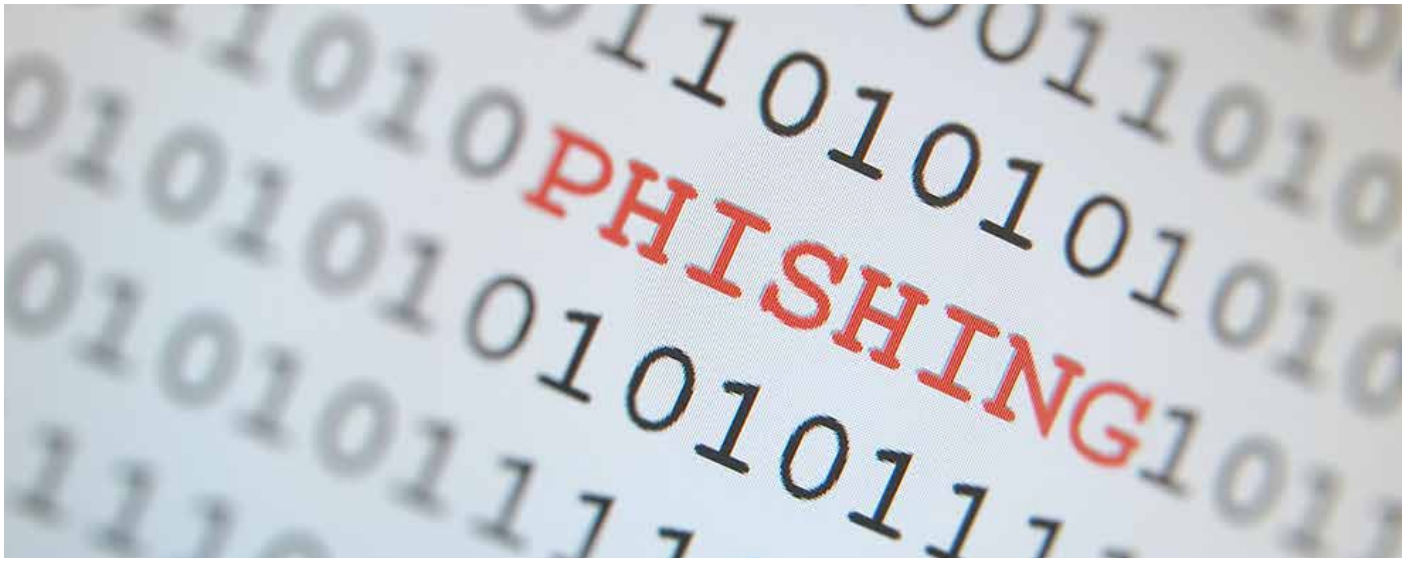
El correo electrónico es la principal puerta de entrada de los ciberdelincuentes en cualquier organización. Basándose en diferentes técnicas de ingeniería social consiguen engañar a los usuarios y robar información confidencial o infectar los equipos con malware. Los tipos de fraudes más comunes son:

2.1. Phising

Posiblemente, se trate de uno de los fraudes más conocidos y extendidos. Se trata de un engaño basado, **generalmente,** en la **suplantación de una empresa o entidad fiable** como un banco, una red social o entidades públicas. **La finalidad es hacerse con claves de acceso o información sensible** como pueden ser datos fiscales o bancarios. El canal mediante el cual se intenta perpetuar el fraude suele ser el correo electrónico, pero también pueden usarse otros como los SMS o aplicaciones de mensajería instantánea como WhatsApp.

Algunos ejemplos reales de avisos de seguridad de tipo phishing:

- Detectada campaña de phishing contra PayPal **[Ref. - 1]**
- ¡Cuidado no piques! Campaña de phishing suplantando a ING **[Ref. - 2]**
- Nueva campaña de correos fraudulentos suplantan a la Agencia Tributaria **[Ref. - 3]**
- Campaña de phishing suplanta falsas devoluciones de Endesa **[Ref. - 4]**



2.2. Scam

Se basa en un tipo de correos electrónicos cuya única finalidad es **perpetrar engaños y estafas** a sus receptores y obtener tanta información personal, de la empresa o bancaria como puedan. El gancho, en este caso, suele girar en torno a falsos premios de lotería, herencias millonarias, ofertas de empleo que requieren de desembolsos, etc., aunque los ciberdelincuentes, cada día, inventan nuevas formas de engaño.

Este es un ejemplo de este tipo de estafa:

- Historias reales: Un galán vació las cuentas de mi empresa **[Ref. - 5]**

2.3. Sextorsión

El objetivo es **extorsionar al receptor con un supuesto video privado o de contenido comprometedor** (que lo más probable es que no exista), amenazando con difundirlo a todos sus contactos de correo y redes sociales a no ser que realice el pago de una cantidad económica. El pago, generalmente, es solicitado en criptomonedas como el bitcoin y el destinatario parece ser el remitente cuando en realidad, no es así.

Ejemplo de sextorsión:

- Campaña de correos extorsionan con supuestos vídeos privados **[Ref. - 6]**

2.4. Malware

En este caso, se trata de código malicioso que podría infectar los dispositivos. Los correos podrían contener algún tipo de **archivo adjunto o enlaces a webs donde una vez descargado y ejecutado el fichero infectará el dispositivo.** La infección también puede producirse al hacer clic en anuncios fraudulentos (malvertising) o aprovechando alguna vulnerabilidad en los navegadores (drive-by-download). Una vez en nuestro equipo, podría distribuirse a través de la red institucional, infectando todo tipo de dispositivos conectados a la misma, como discos duros, pero también otros sistemas de la red e incluso servicios en la nube.

Ejemplos de avisos de malware:

- Envío de falsos presupuestos en Excel como adjuntos maliciosos **[Ref. - 7]**
- Detectada oleada de correos con facturas que infectarán tu equipo **[Ref. - 8]**
- Nueva oleada de ransomware afectando a múltiples equipos **[Ref. - 9]**
- Importante oleada de ransomware afecta a multitud de equipos **[Ref. - 10]**

Nota: el ransomware es un tipo de malware que cifra la información del ordenador o impide el acceso a la misma, amenazando al usuario con destruirla, si no paga un rescate (ransom).

3. DETECCIÓN DE CORREOS FRAUDULENTOS

Los correos electrónicos fraudulentos suelen contar con varias características que permiten su detección. A continuación, por medio del siguiente ejemplo se analiza un ejemplo de correo electrónico fraudulento.

Ilustración 1. Ejemplo de correo electrónico fraudulento

3.1. Remitentes desconocidos

En muchas ocasiones, **comprobar el remitente del correo es suficiente para saber que la comunicación es fraudulenta,** ya que nada tiene que ver con la entidad a la que supuestamente representa. Los ciberdelincuentes suelen utilizar cuentas de correo de otros usuarios a los que han hackeado para enviar los correos electrónicos fraudulentos.

Si hemos recibido un correo que parece provenir de una entidad bancaria, lo normal es que el correo provenga de una cuenta conocida o bien cuentas como contacto@banco.es, no-reply@banco.es, etc. Pero este correo es enviado desde una dirección que nada tiene que ver con la entidad bancaria, como por ejemplo jose_ramos@cochesymotos.es. Es importante revisar cada carácter, pues también son frecuentes suplantaciones cambiando alguna letra o utilizando un carácter de grafía similar o que suene igual. En general, hay que sospechar de los mensajes cuyo remitente sea desconocido y comprobarlo por otro medio, como por teléfono.

3.2. Remitentes falseados y firma

En otras ocasiones, **los ciberdelincuentes falsifican la dirección del remitente haciendo que, a simple vista, no se identifique el correo como fraudulento.** Esta técnica se conoce como email spoofing. En este caso, para comprobar si el correo es legítimo es **necesario** analizar las cabeceras del **mismo**. Esta entre otra mucha información puede servir para saber si el correo procede, realmente, de la dirección que figura en el remitente o ha sido falseada. Esto se podría comprobar manualmente, pero es **recomendable utilizar herramientas que automaticen el proceso como** Messageheader **[Ref. - 11] ofrecida por Google.**

Para más información sobre cómo descargar las cabeceras en distintos clientes de correo y utilizar la herramienta Messageheader **[Ref. - 11]**, visita la siguiente entrada del blog:

- ¿Dudas sobre la legitimidad de un correo? Aprende a identificarlos **[Ref. - 12]**

Una característica que puede hacer saltar las alarmas frente a un correo fraudulento es la firma del mismo, si estamos familiarizados con la firma legítima que suele ser la misma, siempre un cambio de esta o su ausencia, debe ponernos en alerta.

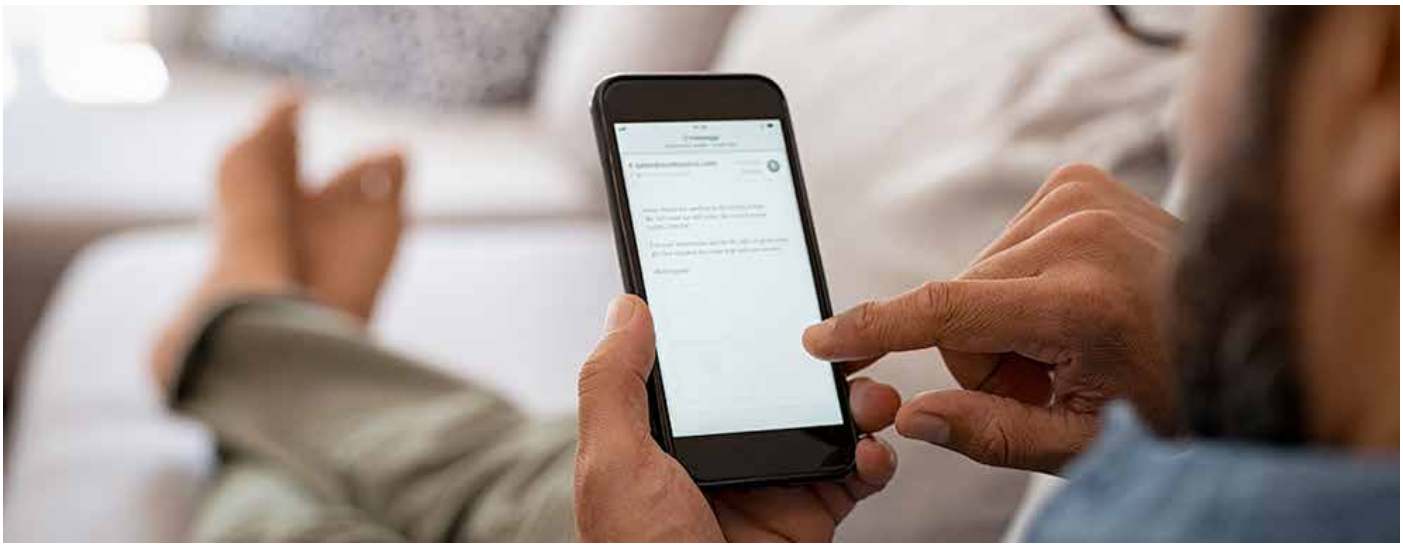
3.3. Ingeniería social en el cuerpo y asunto

Generar un sentimiento de alerta o urgencia e **instar al usuario a que realice una determinada acción,** de forma inmediata, es otra técnica usada en casi todos los correos fraudulentos. Los ciberdelincuentes suelen utilizar técnicas de ingeniería social para que las víctimas caigan en sus trampas, como abrir un adjunto malicioso, acceder a una web ilegítima que suplanta un servicio (phishing) o realizar un pago.

Habitualmente, indican en los correos que el servicio al que representan se cancelará en varias horas o directamente que ya ha sido cancelado. Otro método utilizado es llamar la atención con dinero como un supuesto reembolso que espera a que sea reclamado. O como sucede en los casos de sextorsión en los que se amenaza con difundir un video de carácter sexual en el que la víctima es el supuesto protagonista. En caso de no ceder al chantaje se amenaza con difundirlo a los contactos y conocidos de la víctima en un plazo de tiempo establecido por el delincuente.

3.4. Comunicaciones impersonales

Los ciberdelincuentes cuando envían correos fraudulentos realizan comunicaciones impersonales refiriéndose al destinatario como usuario, cliente, etc. **Las entidades legítimas en las comunicaciones suelen utilizar el nombre y apellidos del destinatario**, haciendo que la comunicación sea más personal.



3.5. Documentos adjuntos maliciosos

Cualquier documento adjunto en un correo electrónico debe ser una señal de alerta. Por norma, ninguna entidad ya sea bancaria, pública, energética, etc., envía a sus destinatarios documentos adjuntos en el correo. Si es necesario que se descargue algún archivo se hará desde su portal web o aplicación oficial.

Esta es la principal forma que usan los ciberdelincuentes para infectar los equipos con malware. Especialmente peligrosos son los archivos con las siguientes extensiones:

- **.exe** – El tradicional archivo ejecutable de Windows.
- **.vbs** – Archivo Visual Basic Script que también puede ser ejecutado.
- **.docm** – Archivo Microsoft Word con macros.
- **.xlsm** – Archivo Microsoft Excel con macros.
- **.pptm** – Archivo Microsoft PowerPoint con macros.

También hay que tener cuidado con ficheros comprimidos como los .zip o .rar, ya que pueden contener archivos maliciosos, como los anteriores, en su interior.

Si dudáis sobre si un documento adjunto puede estar infectado, lo mejor será analizarlo con un antivirus o con servicios online como VirusTotal **[Ref. - 13]** que utilizará varios motores antivirus para comprobar la legitimidad del mismo. **Recuerda no ejecutar nunca el archivo adjunto, únicamente, descárgalo para su posterior análisis.**

Si tras realizar las comprobaciones indicadas no sabes si el documento adjunto es legítimo o no, nunca hay que abrirlo. Si es posible, hay contactar con el remitente por otro canal, como una llamada de teléfono para que confirme el mensaje y el adjunto.

3.6. Mala redacción

Cuando un correo presenta **graves faltas de ortografía** es una señal bastante certera de que ese mensaje es fraudulento. Los correos fraudulentos, en ocasiones, utilizan **expresiones que no son las habituales.** Ante un correo cuya forma de expresarse no es la común también habrá que comprobar su procedencia **[Ref. - 12 y Ref. - 22].**

3.7. Enlaces falseados

Los correos electrónicos de tipo phishing **[Ref. - 14]** o sencillamente los que pretenden redirigir al usuario a un sitio web fraudulento, suelen contar con enlaces falseados. Las entidades legítimas por norma no envían enlaces en sus comunicaciones oficiales y solicitan al usuario que acceda al sitio web, utilizando su navegador web o la aplicación específica.

Antes de indicar cómo comprobar el enlace de un correo hay que conocer **cómo están construidas las direcciones web**. Pongamos como ejemplo la página oficial de la Universidad de Murcia cuyo enlace es https://www.um.es/ Las partes por las que está formado el enlace son:

- «https» - protocolo utilizado para acceder al sitio web.
- «://» - símbolos de separación entre el protocolo y el dominio presentes en todas las direcciones web.
- «www» - subdominio, es un subconjunto del dominio web, como por ejemplo la herramienta de la sede electrónica cuyo subdominio es «sede» siendo el enlace https://sede.um.es/ .Los ciberdelincuentes, en muchas ocasiones, crean subdominios que simulan al legítimo que pretenden suplantar para engañar a las víctimas.
- «um» - dominio, este es único para cada una de las extensiones disponibles como «.es». Esta es la parte que hay que comprobar con especial atención, ya que los ciberdelincuentes no la pueden copiar.
- «.es» - es la extensión del dominio o TLD **[Ref. - 15]** (del inglés Top Level Domain).

3. DETECCIÓN DE CORREOS FRAUDULENTOS

Mediante unos ejemplos se entenderán mejor los conceptos:

- https://adl.incibe.es **[Ref. - 16]** – Dominio legítimo de INCIBE cuyo subdominio es «adl».
- https://adl.incibe.es.otrodominio.com – Dominio fraudulento que pretende suplantar a uno legítimo de INCIBE. El verdadero dominio es «otrodominio.com».
- Otra técnica que utilizan los ciberdelincuentes para engañar a las víctimas suplantando a otra empresa o entidad es el denominado cybersquatting **[Ref. - 17 y Ref. - 23]**. Aquí los ciberdelincuentes pueden optar por cambiar la extensión del dominio por uno cuyo propietario legítimo no haya comprado o alterar el nombre para que lo simule.

Antes de abrir un enlace en un correo hay que comprobar cuál es su destino, para ello hay varias opciones:

- si se utiliza un cliente de correo como Outlook o Thunderbird al situar el ratón encima del enlace se mostrará el destino real del vínculo;
- si se utiliza un cliente de correo web como Gmail al situar el ratón encima del enlace se mostrará en la esquina inferior izquierda, en la mayoría de los casos, el destino real;
- en caso de utilizar un dispositivo móvil, se debe copiar el enlace y pegarlo en un bloc de notas, aplicación de mensajería o similar para comprobar cuál es el verdadero enlace.

Si tras estas comprobaciones no estás seguro de si el destino es legítimo o no, es recomendable utilizar un analizador de sitios web como VirusTotal **[Ref. - 13].**

Si aun así no sabes si el sitio es legítimo, es preferible no acceder al enlace.

4. OTROS RIESGOS DERIVADOS DE SU USO

Los ciberdelincuentes no son los únicos que pueden poner en riesgo la seguridad de la universidad, algunas acciones de los usuarios universitarios también pueden ser el origen. La mayoría de los incidentes de seguridad que tienen que ver exclusivamente con el usuario se deben a errores involuntarios. A continuación, detallamos los más frecuentes.

4.1. CC y CCO

Enviar correos electrónicos a **múltiples destinatarios usando la opción de CC (Carbon Copy) o en copia, en vez de la opción de CCO o copia oculta (o BCC, Blind Carbon Copy, en algunos casos) es uno de los incidentes de fuga de información** (en este caso, las direcciones de correo de los destinatarios) más comunes en una organización. Cuando se realiza el envío de un correo a múltiples destinatarios, siempre hay que utilizar la opción de CCO de forma que el receptor del correo no vea las direcciones del resto de destinatarios, ya que el correo electrónico es considerado un dato personal y estaríamos divulgándolo sin consentimiento del propietario.

4.2. Función de autocompletado

La función de autocompletado puede jugar malas pasadas. En ocasiones cuando se pretende enviar un correo electrónico a un usuario que habitualmente no se utiliza, puede suceder que la función de autocompletado ponga un correo similar gracias a esta función y no nos demos cuenta. Es recomendable deshabilitar esta función siempre que se pueda y en caso de no tener alternativa, **revisar bien el destinatario antes de enviar.**

4.3. Descarga automática de imágenes

Tener habilitado en el cliente de correo la descarga automática de imágenes es un riesgo para tu privacidad y seguridad. Las imágenes son usadas para monitorizar si un correo ha sido abierto o no, reduciendo así la privacidad en el uso de esta herramienta de trabajo. Además, dándose las circunstancias adecuadas, la carga automática de imágenes puede ser la puerta de entrada de malware. Siempre es recomendable desactivar esta opción cuando sea posible.

5. REFERENCIAS

1. INCIBE – Protege tu empresa – Avisos - Detectada campaña de phishing contra Paypal - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/detectada-campana-phishing-paypal

2. INCIBE – Protege tu empresa – Avisos - ¡Cuidado no piques! Campaña de phishing suplantando a ING - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/cuidado-no-piques-campana-phishing-suplantando-ing

3. INCIBE – Protege tu empresa – Avisos - Nueva campaña de correos fraudulentos suplantan a la Agencia Tributaria - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/nueva-campana-correos-fraudulentos-suplantan-agencia-tributaria

4. INCIBE – Protege tu empresa – Avisos - Campaña de phishing suplanta falsas devoluciones de Endesa - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-phishing-suplanta-falsas-devoluciones-endesa-0

5. INCIBE – Protege tu empresa – Avisos - Blog - Historias reales: Un galán vació las cuentas de mi empresa - https://www.incibe.es/protege-tu-empresa/blog/historias-reales-galan-vacio-las-cuentas-mi-empresa

6. INCIBE – Protege tu empresa – Avisos - Blog - Campaña de correos extorsionan con supuestos vídeos privados - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-correos-extorsionan-supuestos-videos-privados

7. INCIBE – Protege tu empresa – Avisos - Blog - Envío de falsos presupuestos en Excel como adjuntos maliciosos - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/envio-falsos-presupuestos-excel-adjuntos-maliciosos

5. REFERENCIAS

8. INCIBE – Protege tu empresa – Avisos - Blog - Detectada oleada de correos con facturas que infectarán tu equipo - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/detectada-oleada-correos-facturas-infectaran-tu-equipo

9. INCIBE – Protege tu empresa – Avisos - Nueva oleada de ransomware afectando a múltiples equipos - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/nueva-oleada-ransomware-afectando-multiples-equipos

10. INCIBE – Protege tu empresa – Avisos - Importante oleada de ransomware afecta a multitud de equipos - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/importante-oleada-ransomware-afecta-multitud-equipos

11. Caja de herramientas de G Suite – Messageheader - https://toolbox.googleapps.com/apps/messageheader/

12. INCIBE – Protege tu empresa – Blog - ¿Dudas sobre la legitimidad de un correo? Aprende a identificarlos - https://www.incibe.es/protege-tu-empresa/blog/dudas-legitimidad-correo-aprende-identificarlos

13. Virustotal - https://www.virustotal.com/gui/home/upload

14. INCIBE – Protege tu empresa – Blog - Busca otro al que engañar, yo no voy a picar - https://www.incibe.es/protege-tu-empresa/blog/busca-otro-al-enganar-yo-no-voy-picar

15. Iana - Root Zone Database - https://www.iana.org/domains/root/db

16. INCIBE – Protege tu empresa - ¿Conoces tus riesgos? - https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos

5. REFERENCIAS

17. INCIBE – Protege tu empresa – Blog - Cybersquatting, qué es y cómo protegerse - https://www.incibe.es/protege-tu-empresa/blog/cybersquatting-y-protegerse

18. INCIBE – Protege tu empresa – Herramientas - Políticas de seguridad para la pyme - Uso del correo electrónico - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-correo-electronico.pdf

19. INCIBE – Protege tu empresa – Blog - El correo electrónico como canal para el fraude digital - https://www.incibe.es/protege-tu-empresa/blog/el-correo-electronico-canal-el-fraude-digital

20. INCIBE – Protege tu empresa – Blog -¿Cómo nos engañan por correo electrónico? - https://www.incibe.es/protege-tu-empresa/blog/nos-enganan-correo-electronico

21. INCIBE – Protege tu empresa – Avisos - Campaña de correos extorsionan con supuestos vídeos privados - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-correos-extorsionan-supuestos-videos-privados

22. OSI – Blog - Aprende a identificar correos fraudulentos mediante una infografía - https://www.osi.es/es/actualidad/blog/2016/10/25/aprende-identificar-correos-fraudulentos-mediante-una-infografia

23. INCIBE – Protege tu empresa – Blog - Aprende a detectar el cybersquatting contra tu marca - https://www.incibe.es/protege-tu-empresa/blog/aprende-detectar-el-cybersquatting-tu-marca