

EL CORREO ELECTRÓNICO

Principales fraudes y riesgos





Ataques a través del correo electrónico



2.

¿Cómo detectar correos fraudulentos?



3.

Otros riesgos derivados del uso del correo electrónico



1.



Ataques a través del correo electrónico

Es una herramienta de comunicación imprescindible en la empresa



1.

Utilizado por ciberdelincuentes para llevar a cabo sus ataques

- **Infección por *malware***
 - **Robo de:**
 - credenciales de acceso (usuario y contraseña)
 - datos bancarios
 - información confidencial



1.



Utilización de ingeniería social por ciberdelincuentes



1.

Phishing

- **Suplantar empresa o entidad fiable**
- **Robar claves de acceso e información sensible**





Phishing

- Ejemplo:

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

Actualización de datos personales

ING
People in progress

Hola,

En ING queremos estar cerca de ti y poder ofrecerte un servicio cada día mejor.

Para ello, es necesario que actualices tus datos personales entrando en el "Área Clientes" de nuestra web y siguiendo los pasos que te indicaremos.

[Área Clientes](#)

Atentamente,

ING

PHISHING

IMPORTANTE: No contestes a este correo, la dirección desde la que se envía este mensaje no está habilitada para la recepción de mensajes. Recuerda que ING nunca te enviará por correo electrónico solicitud alguna para que informes de tus datos personales ni de tus claves.

www.incibe.es/protege-tu-empresa





Phishing

- Ejemplo:

The screenshot shows a phishing email with the following details:

From: De Agencia Tributaria <support@incibe.es> .com> ☆

Subject: Fwd: Nuevo mensaje || 752886301049

To: A [REDACTED]@[REDACTED].com ☆

Sender Logo: Agencia Tributaria (with a stylized blue and yellow logo)

Message Content:

Usted tiene un reembolso de impuestos, de 350.16 Euro

Estimado contribuyente,

1 - Ingrese su información de contacto.
Para enviar la solicitud electrónicamente, complete la información. Cuando se complete el formulario, se le pedirá que confirme que toda la información en el formulario es correcta.

2 - Tratamiento fiscal.
La información que ingrese y el formulario de solicitud completo se envían a Agencia Tributaria a través de una conexión segura y encriptada, y otros no podrán ver la información.

solo complete el formulario a continuación y nos contactaremos con usted lo antes posible.
(Su número de archivo es: 5163_17) : [haga clic aquí](#).

Gracias por su cooperación,

Agencia Tributaria.

Footer: www.incibe.es/protege-tu-empresa





Scam

- **Engañar y estafar**
- **Múltiples ganchos: premios de lotería, herencias, ofertas de empleo, etc.**





Scam

- **Ejemplo:**

 Jun 05/06/2017 16:38
[REDACTED]@[REDACTED]

La crisis ha acabado, Trabajen con nosotros!

Para: [REDACTED]

¡Hola!

estamos en búsqueda de empleados que trabajen a distancia.
Mi nombre es Nuncio, soy el gerente de personal de una gran empresa
internacional.

La mayor parte del trabajo usted puede realizar desde casa, es decir, a
distancia.
Salario es de 2500 a 5000 EUR.

Si usted está interesado en esta oferta de trabajo, a continuación,
por favor visita [Nuestro Sitio](#)

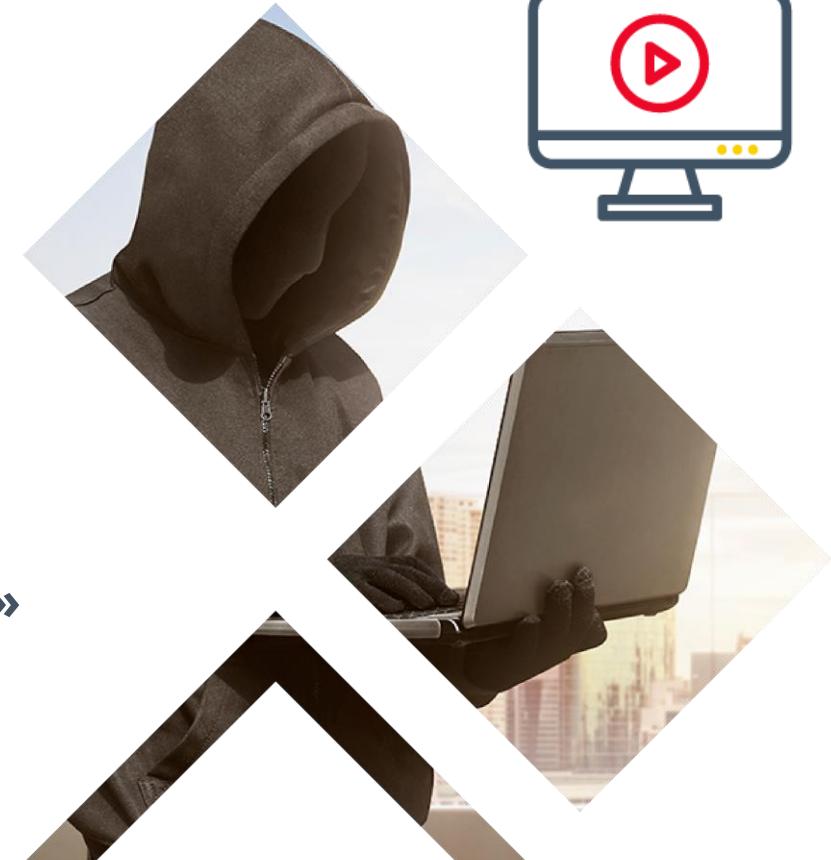




1.

Sextorsión

- Extorsionar con un supuesto video privado o comprometedor
- Difusión por redes sociales y correo electrónico a contactos y conocidos de la víctima
- Pago en criptomonedas «Bitcoin»





Sextorsión

• Ejemplo:

INCIBE-CERT_Cert
Los hackers piratearon tu cuenta. Cambie los datos de acceso inmediatamente.

Para: INCIBE-CERT_Cert

JHola!

Como te habrás dado cuenta, te envíé un correo electrónico desde tu cuenta. El hecho es que usted fue infectado con malware a través de un sitio para adultos que visitó. Esto significa que tengo acceso completo a su cuenta.

Te he estado observando desde hace unos meses. El hecho es que usted fue infectado con malware a través de un sitio para adultos que visitó. Esto significa que tengo acceso completo a su cuenta.

Si no estás familiarizado con esto, te lo explicaré. Trojan Virus me da acceso y control total sobre una computadora u otro dispositivo. Esto significa que puedo ver todo en su pantalla, encender la cámara y el micrófono, pero usted no lo sabe. También tengo acceso a todos sus contactos y toda su correspondencia.

JPor qué tu antivirus no detectó malware?

Respueta: Mi malware usa el controlador, actualizo sus firmas cada 4 horas para que su antivirus esté silencioso. Hice un video que muestra cómo te satisfices yo mismo en la mitad izquierda de la pantalla, y en la mitad derecha ves el video que visto.

Con un clic del mouse, puedo enviar este video a todos sus contactos de correo electrónico y contactos en las redes sociales. También puedo publicar el acceso a toda su correspondencia de correo electrónico y a los mensajeros que utiliza.

Si deseas evitar esto, transferiría la cantidad de \$289 a mi dirección de bitcoin (si no sabe cómo hacerlo, escriba a Google: "Comprar Bitcoin")

Mi dirección de bitcoin (BTC Wallet) es 1JgjcC7sWmr3L7YXKaTAW2qoQdKztcSeu

Después de recibir el pago, eliminaré el video y usted es nunca más oírá saber de mí. Te doy 48 horas para pagar.

Tengo un aviso leyendo esta carta, y el temporizador funcionará cuando abres este correo. Archivar una queja en algún lugar no tiene sentido porque este correo electrónico no puede ser rastreado como mi dirección de bitcoin.

No cometí errores.

www.incibe.es/protege-tu-empresa

Es posible que no me conozca y verosimilmente se está preguntando por qué recibe este e-mail, ¿cierto? Soy un hacker que descifró su e-mail y aparatos hace unos meses. No trate de hacer estar en contacto conmigo o encuentrame, es imposible, desde que para ti envíe un correo electrónico desde SU cuenta hackeada. Configuré malware en el sitio de videos para adultos (porno) y comprendo que visitó este sitio web para pasarse bien (usted sabe a qué [me refiero]quiero decir). Mientras estás viendo estos videos, su navegador de Internet puso en marcha a funcionar como un RDP (mando a distancia) con un registrador de teclas que me dio acceso a su pantalla y cámara web. Después de eso, mi programa de software obtuvo toda la información. Usted ingresó las contraseñas en los sitios web que visitó y yo las intercepté. Claro está, puede cambiármelas, o ya los ha cambiado. Pero no importa, mi malware lo actualiza todo el tiempo. Que hice: Hice una copia de seguridad del dispositivo. De todos los archivos y contactos. Hice un video de doble pantalla. 1^{er} parte muestra el video que usted estaba viendo (tienes buen gusto, jaja...), y la segunda parte muestra la grabación de su cámara web. ¿Qué es exactamente lo que tiene que hacer? Esta bien, en mi opinión, 1000€ es un precio justo para nuestro pequeño secreto. Realizará el pago por medio de bitcoins (si no lo sabe, busque "cómo adquirir bitcoin" en Google). Mi dirección de billtera bitcoin:

1AXTd7o7BRufoJ4a3xnuHgNjNkECz5ZZYB

(Es distingue MAYÚSCULAS y minúsculas, por lo tanto copiarlo y pegarlo.)

Importante:

Tiene cuarenta y ocho horas por hacer el pago. (Yo tengo un pixel único en este correo electrónico, y en este instante sé que ha leído este e-mail).

Para rastrear la lectura de un mensaje y las acciones en él, uso un pixel de Facebook. Gracias a ellos. (Cualquier cosa que se usa para las autoridades puede ayudarnos.)

Si no recibo el dinero, indudablemente voy a enviar su video a todos sus contactos, incluidos familia, compañeros de trabajo, etc.

www.incibe.es/protege-tu-empresa





1.

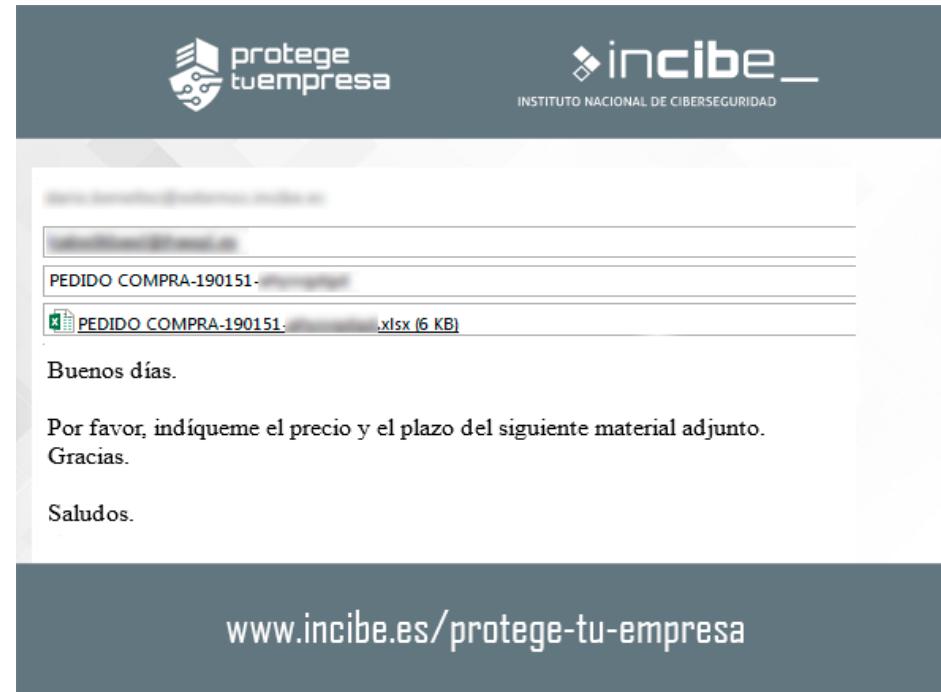
Malware

- Infectar el equipo o red empresarial de la víctima
- Archivos adjuntos, enlaces maliciosos, anuncios fraudulentos o vulnerabilidades en el navegador



Malware

- **Ejemplo:**



The screenshot shows an email with a dark header containing the logos for 'protege tu empresa' and 'incibe'. The body of the email contains a redacted subject line, a redacted file name, and a redacted file link. The message body reads:

Buenos días.

Por favor, indíqueme el precio y el plazo del siguiente material adjunto.
Gracias.

Saludos.

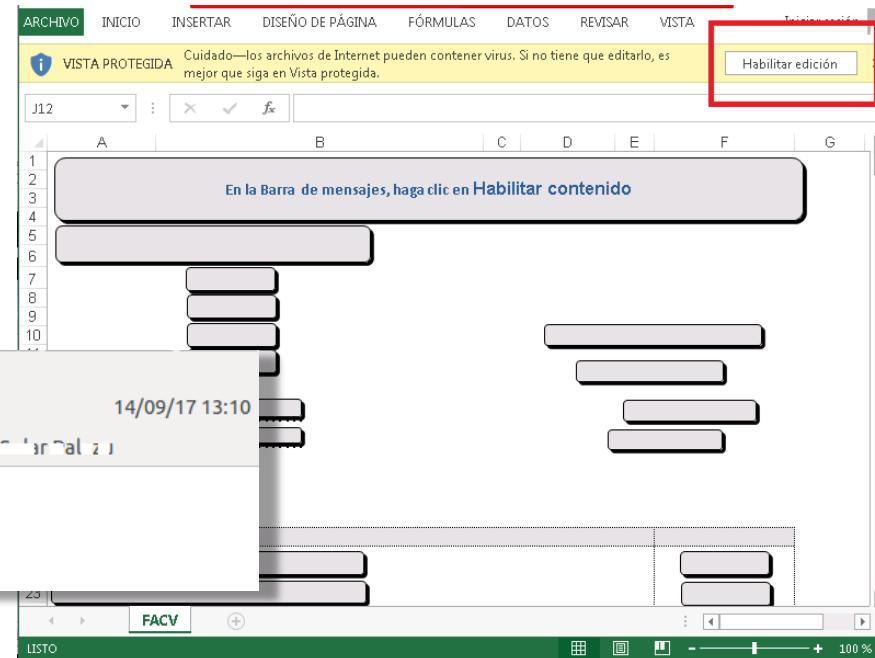
www.incibe.es/protege-tu-empresa





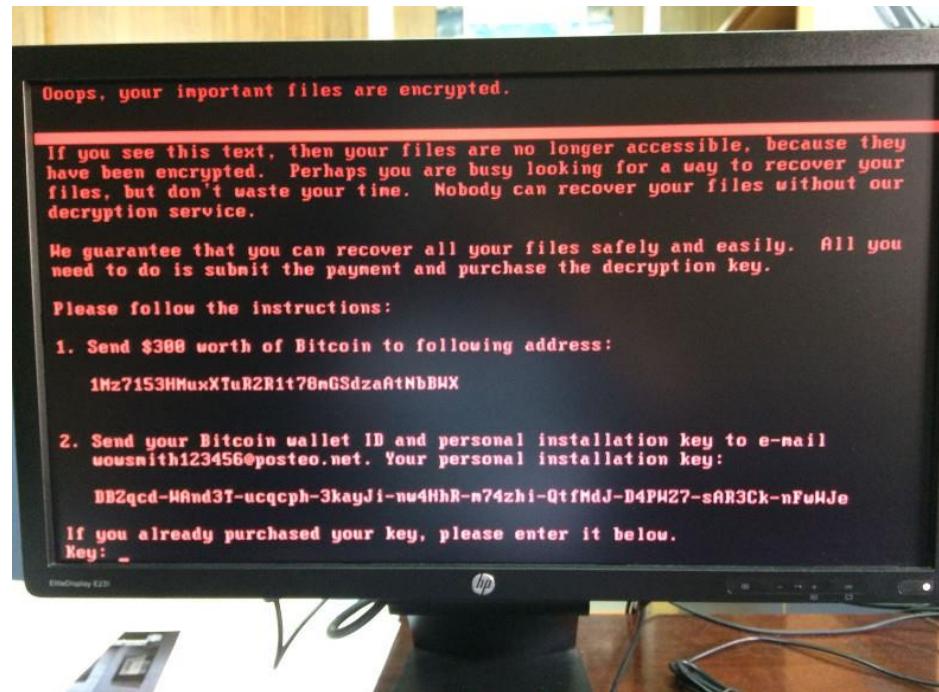
Malware

- **Ejemplo:**





Ransomware





2.

¿Cómo detectar correos fraudulentos?

De: Banco <jose ramos@cochesymotos.es>

Asunto: Tu cuenta ha sido bloqueada

Remitente desconocido, no coincide con la entidad



Ingeniería social, genera situación de alarma

Hola cliente,
Tu cuenta ha sido bloqueada.
Motivo: alta de información.

Faltas de ortografía, una entidad legítima no las tendría

Detalles:
Falta informacion personal.
Falta informacion de facturacion.
Falta informacion de la tarejeta de credito.

Haga clic en el enlace y siga los pasos para desbloquear su cuenta.

ENVIAR PETICION

Enlace, una entidad legítima no pone enlaces

Este mensaje va dirigido, de manera exclusiva, a su destinatario y puede contener información confidencial y sujeta al secreto profesional, cuya divulgación no está permitida por Ley.

Firma de correo distinta a la habitual



2.

¿Cómo detectar correos fraudulentos?: Remitente



• Remitentes desconocidos

- En muchas ocasiones comprobar el remitente es suficiente
- Correo tipo entidad bancaria:
contacto@banco.es o noreply@banco.es
- Revisar cada carácter
contacto@banico.es
- Sospechar de todos los correos con remitente desconocido



2.

¿Cómo detectar correos fraudulentos?: Remitente



• **Remitentes falseados y firma**

- Estar atentos ante cambios en la firma
- Cambios o ausencia puede ser síntoma de fraude.
- «Email spoofing»
- A simple vista no puede ser identificada como fraudulenta
- Analizar las cabeceras con herramientas automáticas como Messageheader



MessageId	XXXXXXXXXXXXXXXXXXXXXXJavaMail.app@lva1-app1707.prod.linkedin.com
Created at:	23/2/2019 18:11:01 CET (Delivered after 1 sec)
From:	LinkedIn <jobs-noreply@linkedin.com>
To:	Protege Tu Empresa <protegetuempresa-170@outlook.com>
Subject:	Protege, las empresas han cubierto 170 vacantes
SPF:	pass
DKIM:	pass
DMARC:	pass

#	Delay	From *	To *	Protocol	Time received
0		mailb-ac.linkedin.com.	→ [Google]	ESMTPS	23/2/2019 18:11:01 CET
1			→ [Google]	SMTP	23/2/2019 18:11:01 CET
2	1 sec		→ [Google]	SMTP	23/2/2019 18:11:02 CET

MessageId	XXXXXXXXXXXXXXXXXXXXXXprod.protection.outlook.com
Created at:	25/3/2019 21:16:10 CET (Delivered after 2 hours)
From:	Thank You Amazon <from@chukzem.xyz>
To:	XXXXXXXXXX@hotmail.com
Subject:	XXXXXXXXXXAmazon: your order has arrived
SPF:	pass
DKIM:	fail
DMARC:	bestguesspass

#	Delay	From *	To *
0	2 hours	XXXXXXXXXXprod.protection.outlook.com	→ XXXXXXXXXXXXXXXXXprod.protection.outlook.com
1	1 sec	XXXXXXXXXXprod.protection.outlook.com	→ XXXXXXXXXXXXXXXXXPROD.OUTLOOK.COM



¿Cómo detectar correos fraudulentos?: Ingeniería social y otras pistas



Ingeniería social en el cuerpo y en el asunto

- Alerta o urgencia y forzar una acción del usuario
- Cancelaciones de servicio y/o supuesto reembolso
- Sextorsión





2.



Comunicaciones impersonales

- **Entidades legítimas suelen utilizar nombres y apellidos del destinatario**



2.

ling iz dificult

Mala redacción

- **Graves faltas de ortografía y expresiones no habituales**





¿Cómo detectar correos fraudulentos?: Adjuntos maliciosos



- **Ante cualquier adjunto se deben extremar las precauciones**
- **Las entidades legítimas no suelen enviar adjuntos**
- **Documentos adjuntos maliciosos**
 - Las entidades legítimas no suelen enviar adjuntos
 - Extensiones especialmente peligrosas:
.exe - .vbs - .docm - .xlsm - .pptm



2.

¿Cómo detectar correos fraudulentos?: Adjuntos maliciosos



- Ficheros comprimidos
- Ante la menor duda VirusTotal
- Nunca ejecutar ningún adjunto antes de comprobarlo, solamente descargarlo
- Ante cualquier duda nunca ejecutar archivo



2. ¿Cómo detectar correos fraudulentos?: Enlaces falseados



- **Enlaces falseados**
 - Entidades legítimas no suelen enviar enlaces en los correos
 - Objetivo de ciberdelincuentes redirigir al usuario web fraudulenta



2.

¿Cómo detectar correos fraudulentos?: Enlaces falseados

- Construcción de la dirección web «<https://www.incibe.es/protege-tu-empresa/>»
 - «https»: protocolo utilizado para acceder al sitio web
 - «://»: símbolos de separación entre el protocolo y el
 - «www»: subdominio, es un subconjunto del dominio web. Los ciberdelincuentes, en muchas ocasiones, crean subdominios que simulan al legítimo que pretenden suplantar para engañar a las víctimas



2.

¿Cómo detectar correos fraudulentos?: Enlaces falseados

- «incibe»: 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



2. ¿Cómo detectar correos fraudulentos?: Enlaces falseados

Cybersquatting. Modificación del dominio o extensión para suplantar al legítimo.

- Adición. Consiste en añadir un carácter al final del nombre de dominio “incibes.es”.
- Sustitución. Se cambia un carácter del nombre de dominio por otro “incive.es”
- Homográfico. Se sustituye por otro que a simple vista resulta similar “inlbe.es”.
- Separación. Consiste en añadir un guion en alguna parte del nombre del dominio “inci-be.es”.



2. ¿Cómo detectar correos fraudulentos?: Enlaces falseados

- Inserción. Se añade un carácter entre el primero y el último del nombre del dominio “incinbe.es”
- Omisión. Se elimina un carácter “incbe.es”
- Subdominio. Radica en registrar un nombre de dominio con el nombre parcial del legitimo y añadir los caracteres restantes por medio de un subdominio “inci.be.es”
- Trasposición. Alternación del orden de los caracteres del nombre de dominio “inicbe.es”.
- Cambio de dominio. Se utiliza un dominio libre pero utilizando el mismo nombre de dominio “incibe.eu”.



2. ¿Cómo detectar correos fraudulentos?: Enlaces falseados

- Otros. Algunas otras técnicas utilizadas consisten en añadir “w” al comienzo del nombre o “com2 al final, “wwwincibe.es” “incibecom.es”
- Aun así hay dudas comprobar con VirusTotal
- Ante la menor duda no acceder al enlace



3.

Otros riesgos derivados del uso del correo electrónico

Los empleados pueden poner en riesgo la empresa involuntariamente

- CC Y CCO
 - Fugas de información
- Función de autocompletado
- Descarga automática de imágenes
 - Riesgo para la privacidad y seguridad

GRACIAS POR SU ATENCIÓN



INSTITUTO NACIONAL DE
CIBERSEGURIDAD

SPANISH NATIONAL
CYBERSECURITY INSTITUTE

www.incibe.es


INSTITUTO NACIONAL DE CIBERSEGURIDAD