GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

crue
Universidades Españolas

EL CORREO ELECTRÓNICO

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1.

Ataques a través del correo electrónico

Es una herramienta de comunicación imprescindible

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

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

crue Universidades Españolas

1.

Phising

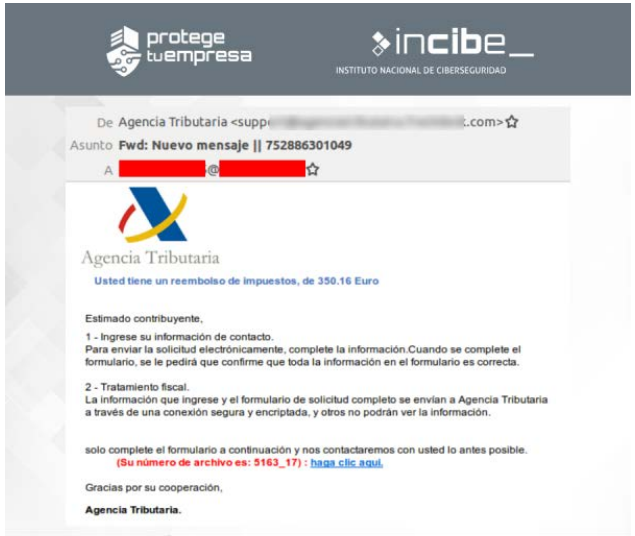
- Suplantar empresa o entidad fiable
- Robar claves de acceso e información sensible

1.

Phising

Ejemplos:

www.incibe.es/protege-tu-empresa



www.incibe.es/protege-tu-empresa

1.

Scam

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

1.

Scam

Ejemplo:

lun 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 visite **Nuestro Sitio**

1.

Sextorsión

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

1.

Sextorsión

Ejemplos:

protege tuempresa — incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

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

¡Hola!

Como te habrás dado cuenta, te envié un correo electrónico desde tu cuenta.
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.

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.

¿Por qué tu antivirus no detectó malware?
Respuesta: Mi malware usa el controlador, actualizo sus firmas cada 4 horas para que su antivirus esté silencioso.

Hice un video que muestra cómo te satisfaces yo mismo en la mitad izquierda de la pantalla, y en la mitad derecha ves el video que viste.
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 desea evitar esto, transfiera 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: 1JgjcCi7sWmr3L7YXKaTAW2qoQdKztcSeu

Después de recibir el pago, eliminaré el video y usted es nunca más oirá a saber de mí.
Te doy 48 horas para pagar.
Tengo un aviso leyendo esta carta, y el temporizador funcionará cuando abres esta correo.

Archivar una queja en algún lugar no tiene sentido porque este correo electrónico no puede ser rastreado como y mi dirección de bitcoin.
No cometo errores.

www.incibe.es/protege-tu-empresa

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD — protege tuempresa

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 con me o encuentrame, es imposible, desde que para ti envié 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 pasaste bien (usted sabe a qué {me refiero|quiero decir).
Mientras estar vía 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 cambiarlos, 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. 1ª parte muestra el video que usted estaba viendo (tiene buen gusto, jaja...), y la segunda parte muestra la grabación de su cámara web.
¿Qué es exactamente lo que tiene que hacer?
Está 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 billetera 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

1.

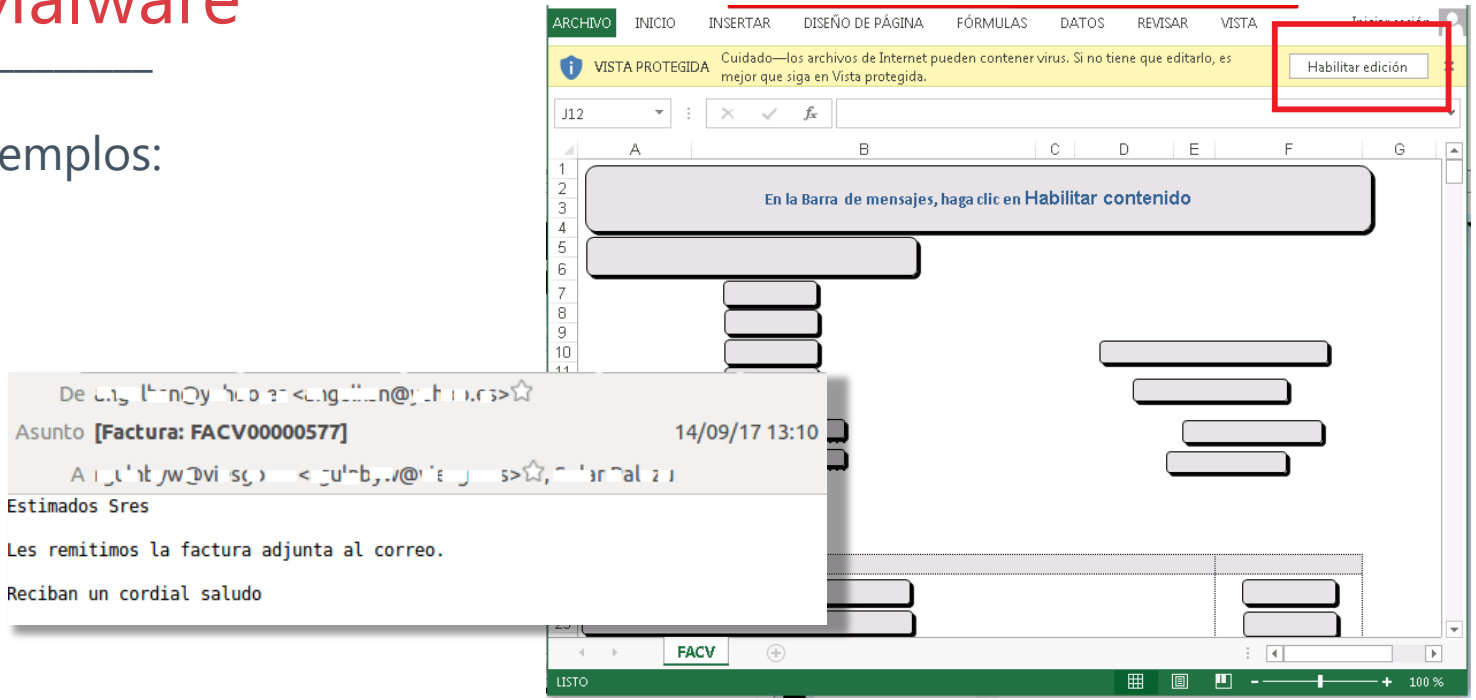
Malware

Ejemplos:

1.

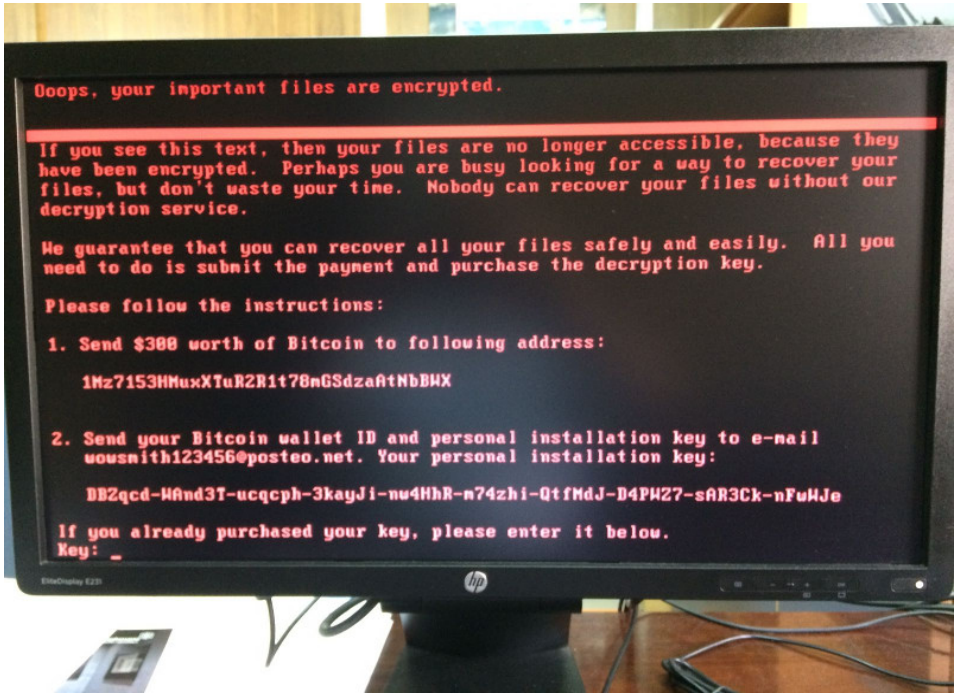
Malware

Ejemplos:



1.

Ransomware



¿Cómo detectar correos fraudulentos?

2.

De: Banco <jose_ramos@cochesymotos.es>

Asunto: Tu cuenta ha sido bloqueada

Remitente desconocido, no coincide con la entidad

BANCO

Ingenieria 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

2.

MessageId	[redacted]JavaMail.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 <protege[redacted]@gmail.com>
Subject:	Protege, las empresas han cubierto 170 vacantes
SPF:	pass
DKIM:	pass
DMARC:	pass

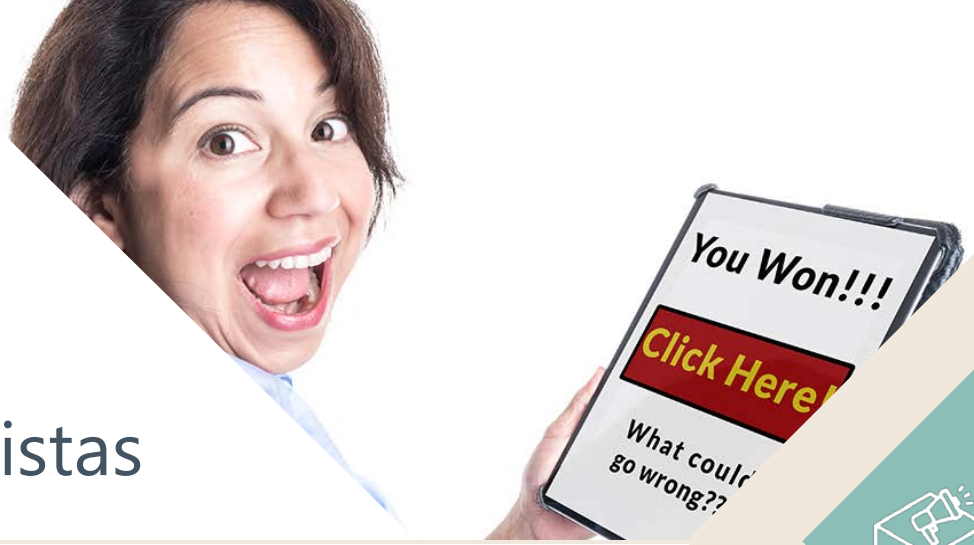
#	Delay	From *		To *	Protocol	Time received
0		mailb-ac.linkedin.com.	→ [Google]	mx.google.com	ESMTPS	23/2/2019 18:11:01 CET
1			→ [Google]	[redacted]:cc85::	SMTP	23/2/2019 18:11:01 CET
2	1 sec		→ [Google]	[redacted]1:0:0:0:0:0	SMTP	23/2/2019 18:11:02 CET

MessageId	[redacted]-EUR03.prod.protection.outlook.com
Created at:	25/3/2019 21:16:10 CET (Delivered after 2 hours)
From:	Thank You Amazon <from@chukzem.xyz>
To:	[redacted]@hotmail.com
Subject:	[redacted]Amazon :your order has arrived
SPF:	pass
DKIM:	fail
DMARC:	bestguesspass

#	Delay	From *		To *
0	2 hours	[redacted].prod.protection.outlook.com	→	[redacted].prod.protection.outlook.com
1	1 sec	[redacted].prod.protection.outlook.com	→	[redacted].PROD.OUTLOOK.COM

2.

¿Cómo detectar correos fraudulentos? Ingeniería social y otras pistas



Ingeniería social en el cuerpo y en el asunto

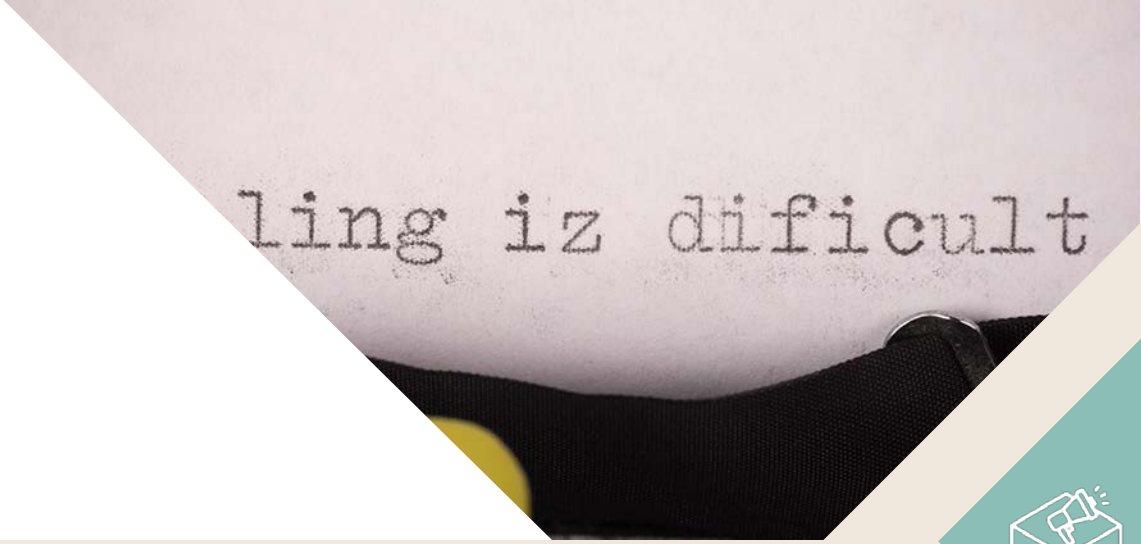
- Alerta o urgencia y forzar una acción del usuario
- Cancelaciones de servicio y/o supuesto reembolso
- Sextorsión

2.

Comunicaciones impersonales

Las entidades legítimas suelen utilizar los nombres y apellidos del destinatario

2.



Mala redacción

Graves faltas de ortografía y expresiones no habituales

2.

¿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.

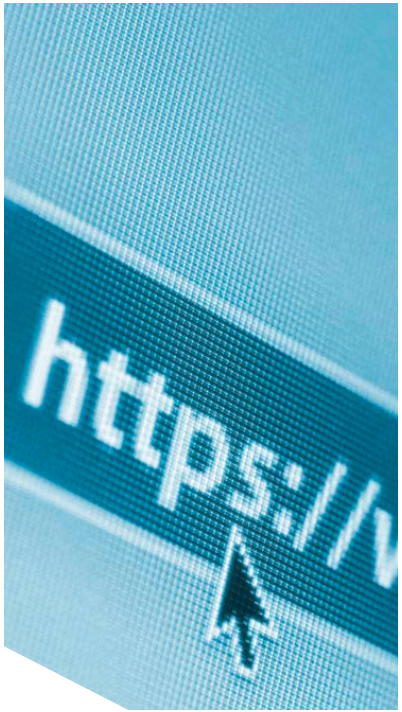
¿Cómo detectar correos fraudulentos?

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?

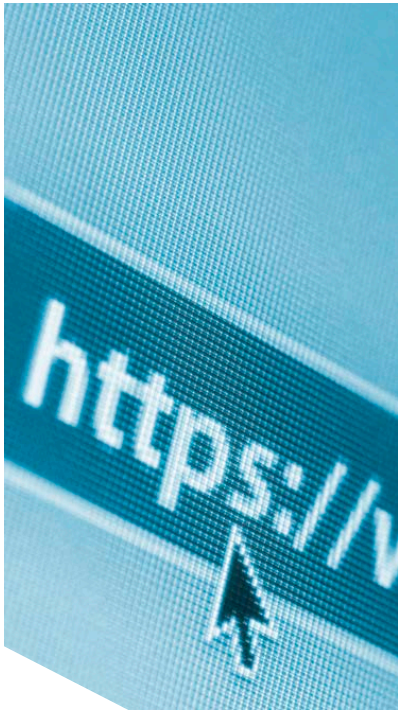


Enlaces falseado

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

2.

¿Cómo detectar correos fraudulentos?

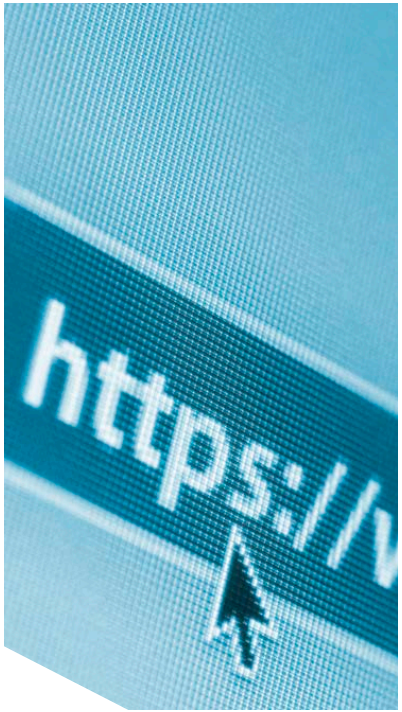


Enlaces falseado

- Construcción de la dirección web «https://www.um.es/»
  - «https» - protocolo utilizado para acceder al sitio web
  - «://» - símbolos de separación entre el protocolo y el
  - «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.

2.

¿Cómo detectar correos fraudulentos?

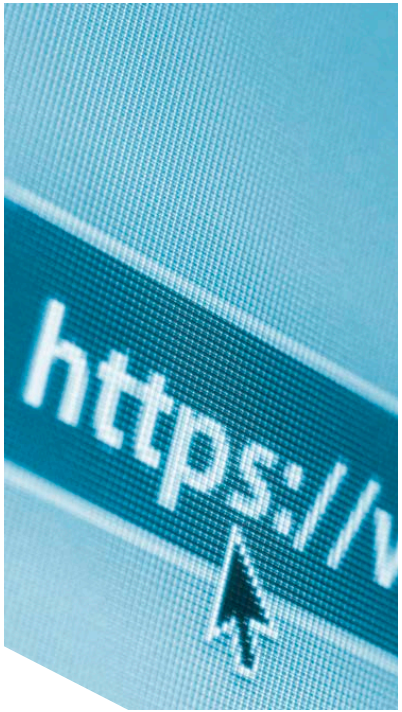


Enlaces falseado

- «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.

2.

¿Cómo detectar correos fraudulentos?

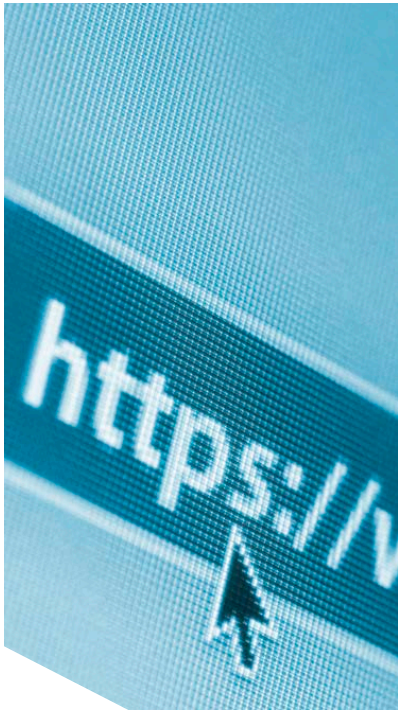


Enlaces falseado

- Cybersquatting. Modificación del dominio o extensión para suplantar al legítimo.
  - Adición. Se añade un carácter al final del nombre del 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 “inclbe.es”
  - Separación. Se añade un guion en alguna parte del nombre del dominio “inci-be.es”

2.

¿Cómo detectar correos fraudulentos?

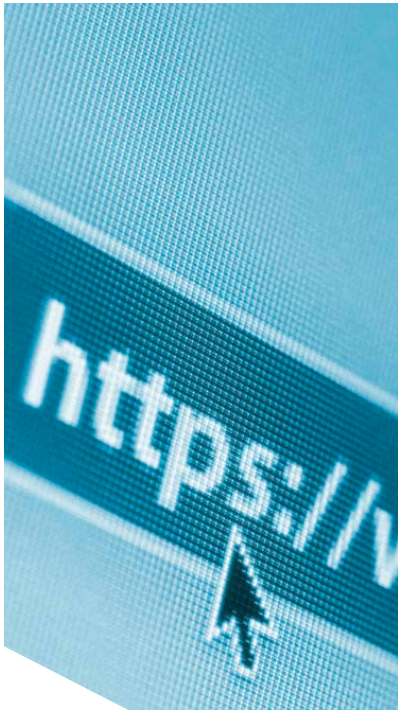


Enlaces falseado

- 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. Se registra un nombre de dominio con el nombre parcial del legitimo y se añaden los caracteres restantes por medio de un subdominio “inci.be.es”
- Trasposición. Se alterna 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 falseado

- Otros. Algunas otras técnicas utilizadas consisten en añadir “w” al comienzo del nombre o “com2 al final, “wwwincibe.es” “incibecom.es”

- Aun así, si hay dudas comprobar con VirusTotal

- Ante la menor duda no acceder al enlace

3.

Otros riesgos derivados del uso del correo electrónico

Los miembros de la comunidad universitaria pueden poner en riesgo la universidad involuntariamente

- CC y CCO : Fugas de información
- Función de autocompletad
- Descarga automática de imágenes: riesgo para la privacidad y seguridad

GRACIAS POR SU ATENCIÓN