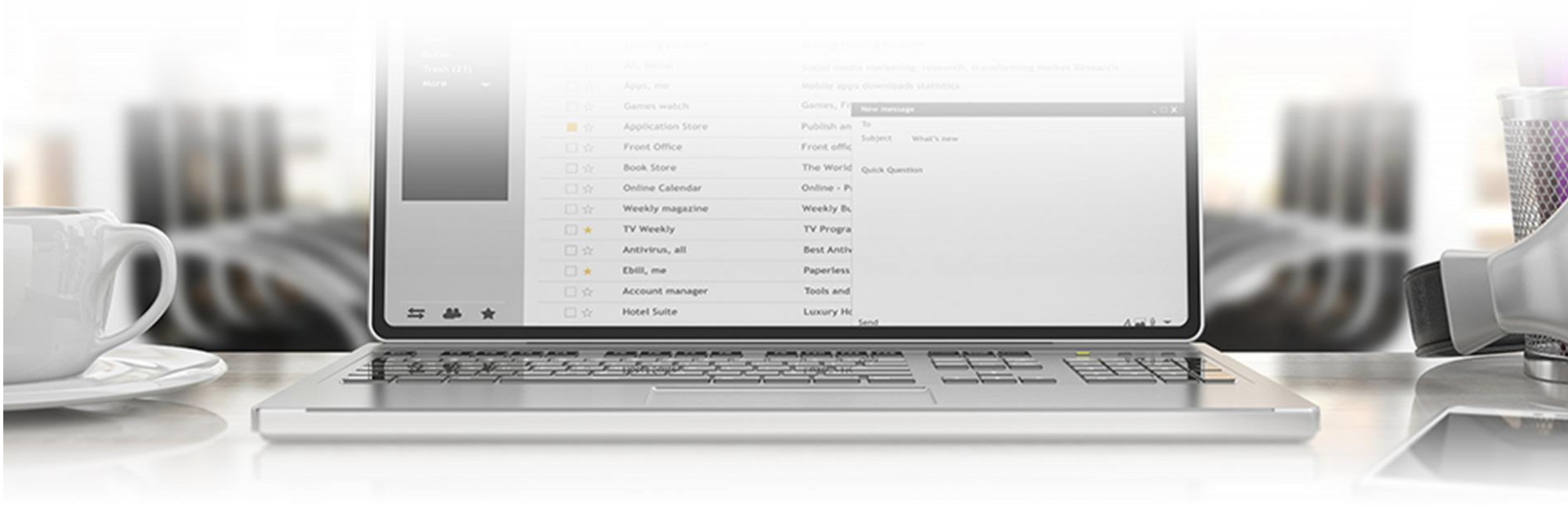
EL CORREO ELECTRÓNICO

Principales fraudes y riesgos



ÍNDICE

1.

Ataques a través del correo electrónico

Es una herramienta de comunicación imprescindible en la empresa

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**

1.

Phishing

- **Ejemplo:**

"Alerta de Phishing circulando en la red"

De: **Bancolombia** <contacto@co.bancofalabella.com>
Date: mar., 9 jun. 2020, 6:21 p. m.
Subject: Servicios de Alertas y Notificaciones Bancolombia
To: <ponal.csirt@policia.gov.co>

Notificación De Seguridad

Bancolombia le informa que todos sus productos y accesos a canales virtuales y fisicos han sido bloqueados por razones de seguridad.

Para restablecer todos sus producto, debemos verificar datos de titularidad.

Haga clic en el siguiente enlace y realice el proceso de verificacion para el restablecimiento de tus productos, diligencie toda la informacion solicitada de manera correcta.

Restablecer mi Cuenta

En Bancolombia a un Clic estamos innovando para que pueda disfrutar de mas tiempo libre, tener la oportunidad de contar con servicios agiles y simples, y estar para usted cuando, como y donde nos necesite.

Al dar clic sobre el link → Restablecer mi Cuenta → Es redireccionado al sitio web → https://www.strainguide.co.za/https/

1.

Phishing

- **Ejemplo:**

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.

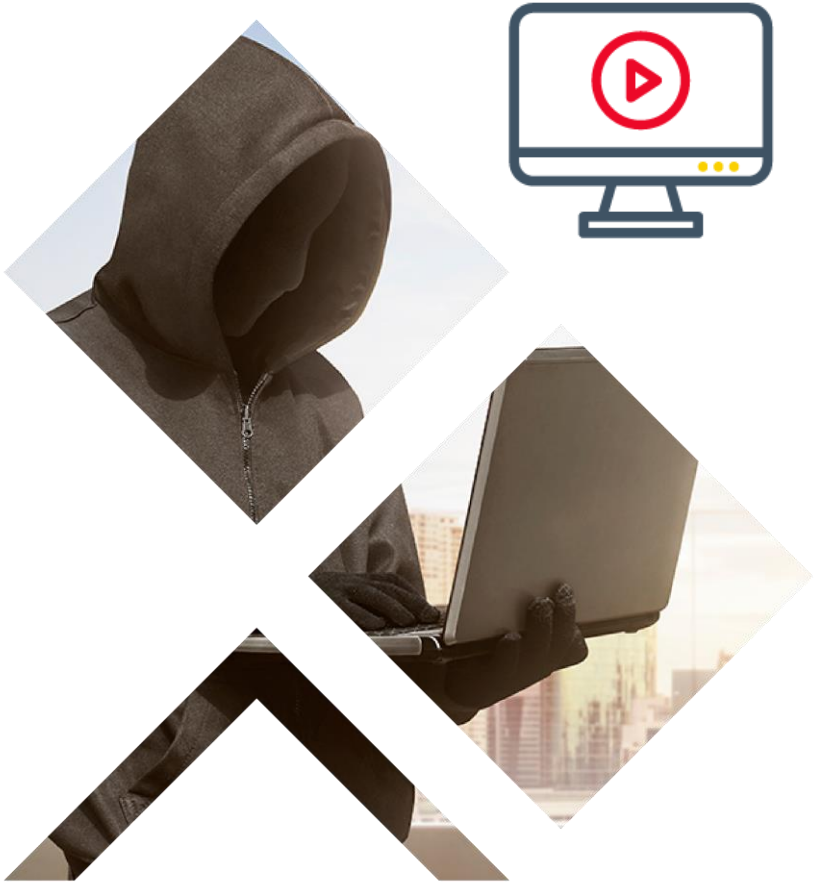
La mayor parte del trabajo usted puede realizar desde casa, es decir, a distancia.
Salario es de 2500 a 5000 EUR.

Si usted está interesado en esta oferta de trabajo, a continuación,
por favor visite **Nuestro Sitio**

1.

Sextorsión

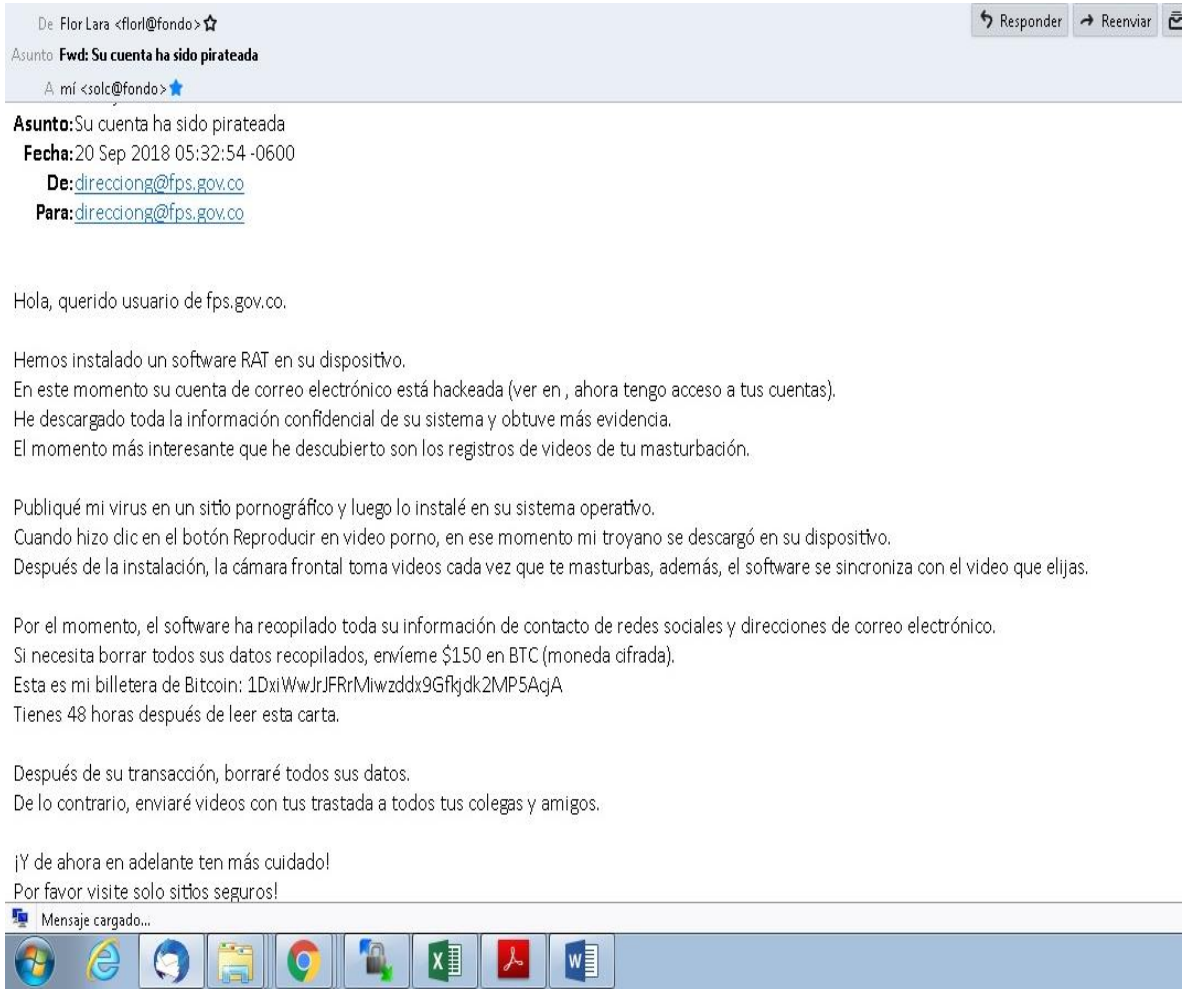
- **Extorsionar con un supuesto video privado o comprometedor**
- **Difusión por redes sociales y correo electrónico a contactos y conocidos de la víctima**
- **Pago en criptomonedas «Bitcoin»**



1.

Sextorsión

- **Ejemplo:**



De Flor Lara <florl@fondo>
Asunto **Fwd: Su cuenta ha sido pirateada**
A mí <solc@fondo>

Responder Reenviar

Asunto: Su cuenta ha sido pirateada
Fecha: 20 Sep 2018 05:32:54 -0600
De: direccionq@fps.gov.co
Para: direccionq@fps.gov.co

Hola, querido usuario de fps.gov.co.

Hemos instalado un software RAT en su dispositivo.
En este momento su cuenta de correo electrónico está hackeada (ver en , ahora tengo acceso a tus cuentas).
He descargado toda la información confidencial de su sistema y obtuve más evidencia.
El momento más interesante que he descubierto son los registros de videos de tu masturbación.

Publiqué mi virus en un sitio pornográfico y luego lo instalé en su sistema operativo.
Cuando hizo clic en el botón Reproducir en video porno, en ese momento mi troyano se descargó en su dispositivo.
Después de la instalación, la cámara frontal toma videos cada vez que te masturbas, además, el software se sincroniza con el video que elijas.

Por el momento, el software ha recopilado toda su información de contacto de redes sociales y direcciones de correo electrónico.
Si necesita borrar todos sus datos recopilados, envíeme $150 en BTC (moneda cifrada).
Esta es mi billetera de Bitcoin: 1DxiWwJrJFRrMiwzddx9GfkjdK2MP5AcjA
Tienes 48 horas después de leer esta carta.

Después de su transacción, borraré todos sus datos.
De lo contrario, enviaré videos con tus trastada a todos tus colegas y amigos.

¡Y de ahora en adelante ten más cuidado!
Por favor visite solo sitios seguros!

Mensaje cargado...

1.

Malware

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

1.

Malware

- **Ejemplo:**

1.

Malware

- **Ejemplo:**

De medico <medico@fps.gov.co>
Asunto **Fwd: NOTIFICACIÓN FOTO MULTA (IMAGEN_2332_IMAGEN_2333_IMAGEN_2334)**
A mí <seguridadinformacion@fps.gov.co>

Responder | Reenviar | Archivar | No deseado | Eliminar | Más
01/09/2016, 10:57 a. m.

-------- Mensaje reenviado --------
Asunto:NOTIFICACIÓN FOTO MULTA (IMAGEN_2332_IMAGEN_2333_IMAGEN_2334)
Fecha: Thu, 1 Sep 2016 09:20:58 -0500
De: Claudia ospina <claudiaospinaq@gmail.com>

El hecho queda registrado como antecedente en las fotografías mostradas en el siguiente reporte captadas por el equipo de sistema electrónico certificado con número de serie GTY900 el cual muestra que el conductor no respeto los límites de velocidad permitidos en dicha zona.
Por seguridad virtual adjunto encontrara las dichas imágenes (IMAGEN_2332_IMAGEN_2333_IMAGEN_2334) y multa respectiva por exceso de velocidad.

CLAUDIA OSPINA
COMPARENDOS TRANSITO Y TRANSPORTE.
SIMIT.

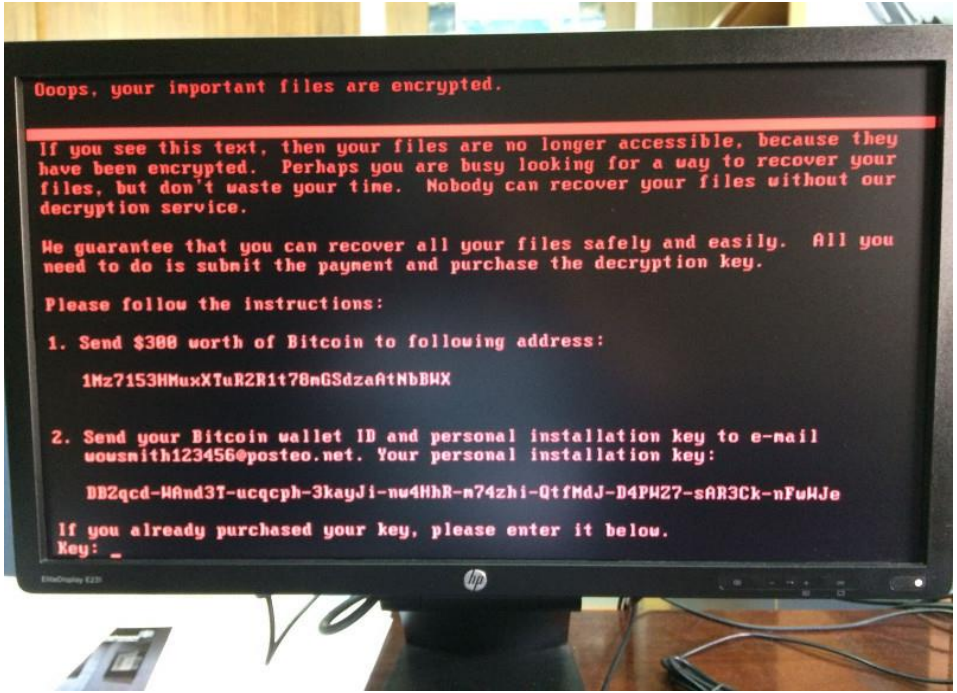
1 adjunto: IMAGEN_2332_IMAGEN_2333_IMAGEN_2334_COMPAR.tbz 96,8 KB
Guardar

Panel Para hoy

ES 10:08 p.m. 04/07/2020

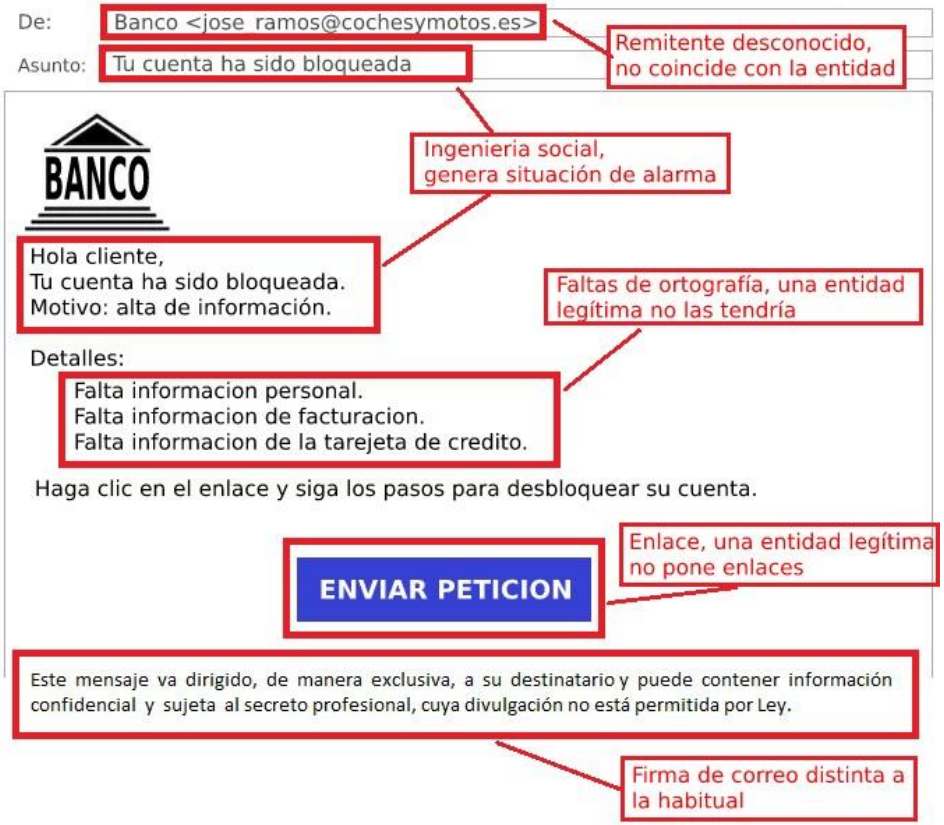
1.

Ransomware

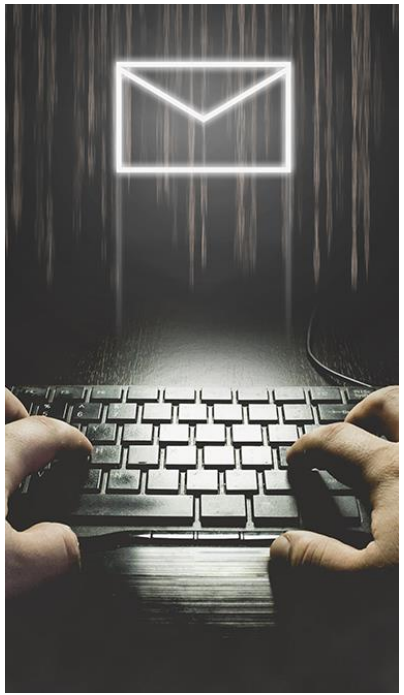


2.

¿Cómo detectar correos fraudulentos?



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 falsos 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

2.

"Alerta de Malware circulando en la red"

De: secretaria-ministeriotransporte-com@getresponse-mail.com <secretaria-ministeriotransporte-com@getresponse-mail.com> en nombre de SECRETARIA DE TRANSITO <secretaria@ministeriotransporte.com>

Email Spoofing

Asunto: Notificacion De Foto Comparendo Nº 5843528

Contexto

SECRETARIA DE TRANSITO
xx De Junio Del 2020
ACTA DE INFRACCIÓN DE TRANSITO

Orden de comparendo Nº 5843528

SEÑOR CONDUCTOR

Por este medio se le notifica a usted que presenta un comparendo por foto multa, valor de la sanción $ 876.830 (ochocientos setenta y seis mil ochocientos treinta pesos)

COMPARENDO C347, Ley 4117 del 12 de mayo del 2010: Conducir un vehículo a velocidad superior a la máxima permitida

se le anexa a descargar archivos adjuntos en el siguiente enlace donde encontrara fotos hora y lugar donde se origino su comparendo

DESCARGUE AQUI FOTOS COMPARENDO

• EVIDENCIAS: FOTOS, LUGAR Y FECHA DE LA INFRACCIÓN

Análisis

Al dar clic sobre el hipervínculo

DESCARGUE AQUI FOTOS COMPARENDO

https://app.getresponse.com/click.html?x=a6

Es redireccionado al sitio web

Desde donde se descarga un archivo malicioso.

Host malicioso identificado

servicios.accesoriossamsung1.cloud -- 181.48.139.42

MD5	2acbfbd0b6c407fb3c7a0cc5c7a39d77
SHA1	28f3aaebb1e74df11d1825ea86ea377618ff466b

POLICÍA NACIONAL
OFICINA DE TELEMÁTICA

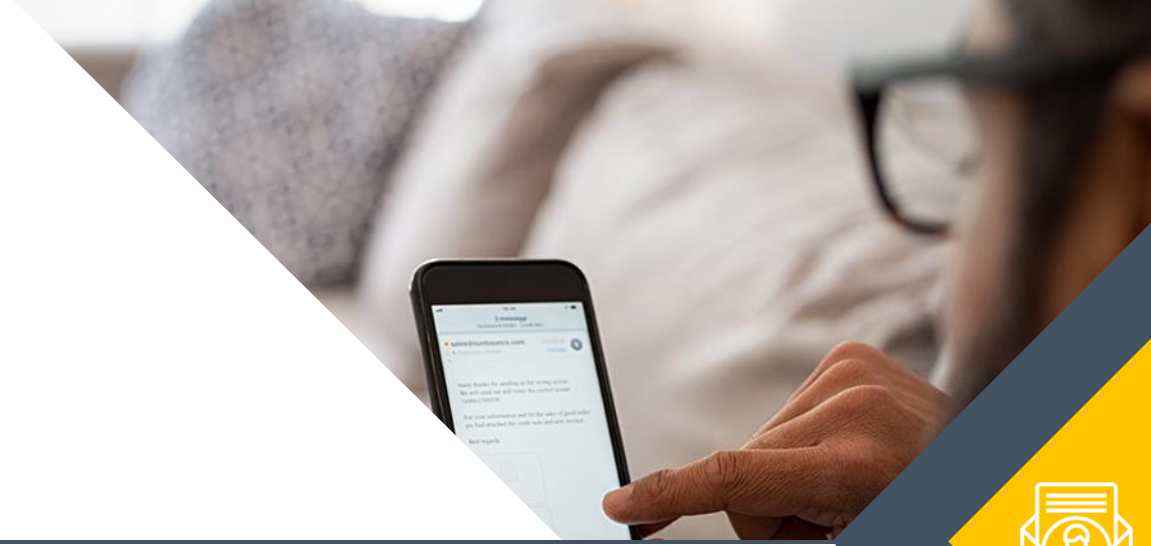
2.

¿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

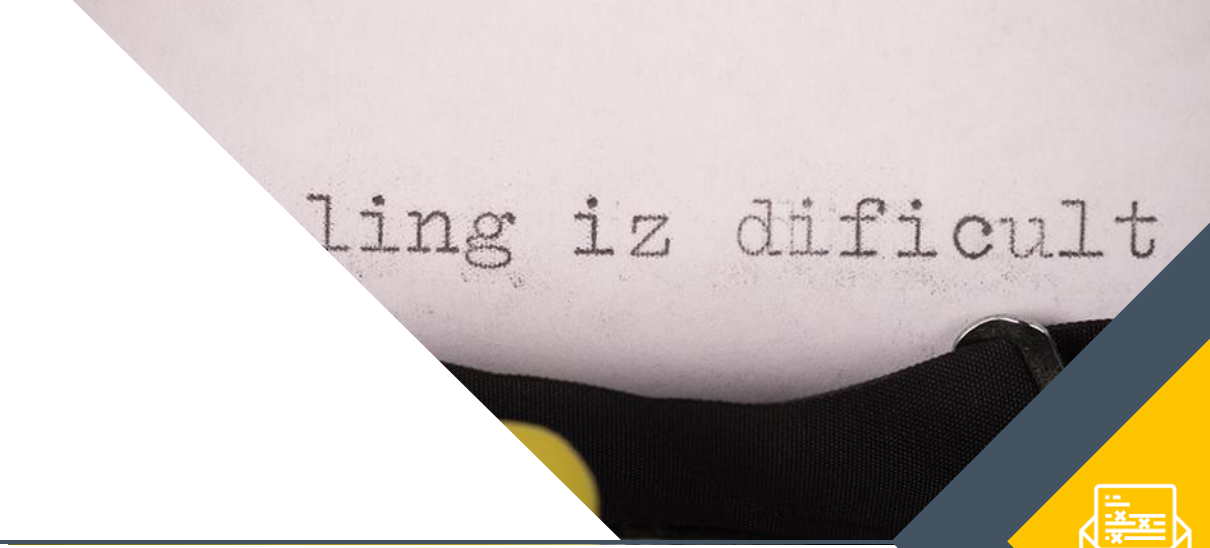
2.



Comunicaciones impersonales

- **Entidades legítimas suelen utilizar 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 falsos

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

2. ¿Cómo detectar correos fraudulentos?: Enlaces falsos

- 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 falsos

- «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 falsos

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 “incIbe.es”.
- Separación. Consiste en añadir un guion en alguna parte del nombre del dominio “inci-be.es”.

2. ¿Cómo detectar correos fraudulentos?: Enlaces falsos

- 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 falsos

- 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