

# Uso Seguro de Internet

Precauciones y métodos de protección



**CYL** digital

@cyldigital

# Contenidos



# ¿A qué nos enfrentamos?



@cyldigital



# ¿A qué estamos expuestos?



- Incremento del 125% de los ciberataques en España en 2021 respecto al último trimestre de 2020.

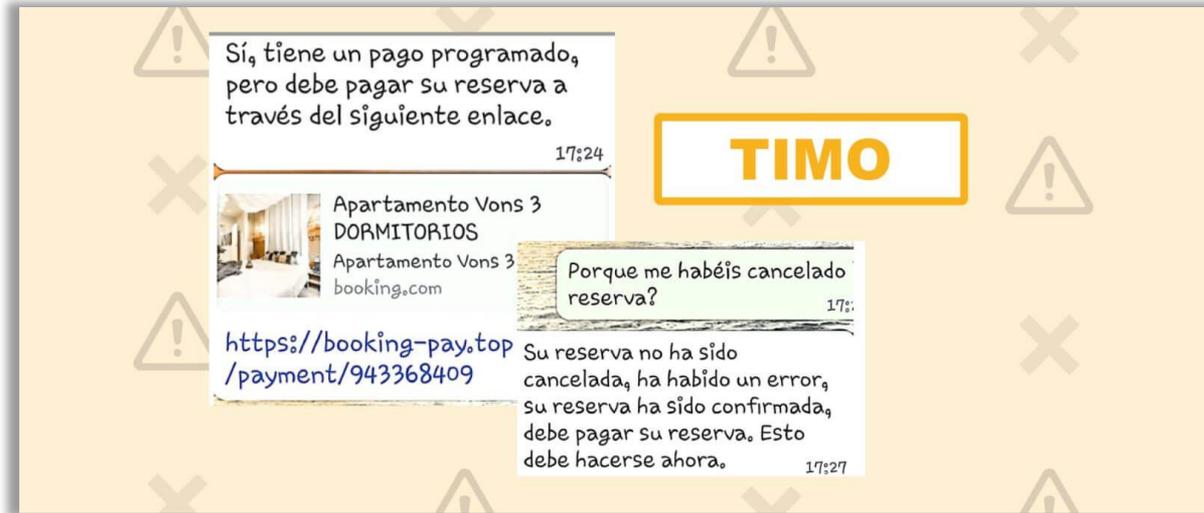
- 40.000 ataques diarios

(Información de Datos101, empresa dedicada a soluciones de seguridad de datos)

# Datos = Materia prima del siglo XXI

MATERIAS PRIMAS	MÁQUINAS	MODELOS DE NEGOCIO
SIGLO XIX CARBÓN		
SIGLO XX PETRÓLEO, ACERO, ELECTRICIDAD		
SIGLO XXI DATOS		

# Trending Topic de las estafas en Internet



**Booking para intentar hacerse con tus datos y tu dinero**

# Trending Topic de las estafas en Internet



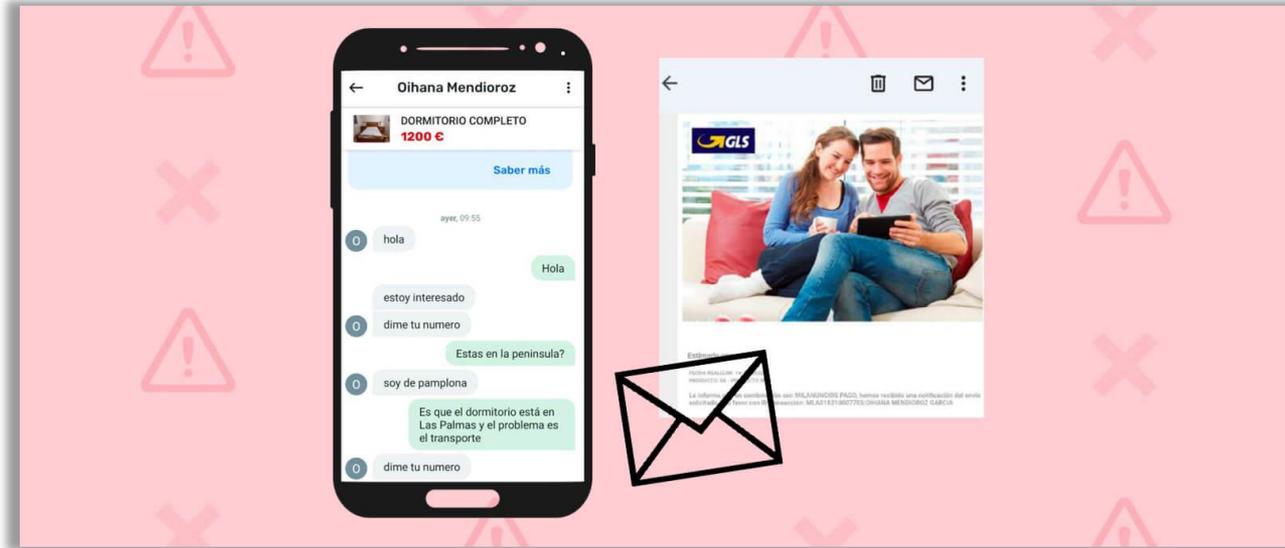
**El falso sargento estadounidense destinado en Ucrania que te quiere robar el corazón (y el dinero) en Tinder**

# Trending Topic de las estafas en Internet



**Correos Express no ha parado tu paquete en aduanas hasta que pagues 1'98 euros: es 'phishing'**

# Trending Topic de las estafas en Internet



**Cuidado con los timos si vendes un producto en plataformas de compraventa: suplantan a Milanuncios y GLS para intentar estafarte**

# Las grandes compañías también sufren

- Servidores de correo vulnerables de **Microsoft**. Marzo 2021
- El **SEPE**. Marzo 2021. Ataque con Ryuk (ransomware)
- Venta de datos de usuarios de **Facebook**. Abril 2021. Brecha en la privacidad y venta en Surface web (foro) de datos robados de 533 millones de usuarios
- Ataques sincronizados a varios organismos con el objetivos de la red **SARA** (Sistema de Aplicaciones y Redes para las Administraciones) que conecta a la mayoría de webs de administraciones estatales y autonómicas y que interviene en servicios como CI@ve, la firma electrónica o procedimientos burocráticos.
- Ransomware **HIVE** en **Mediamarkt**



## Agencias estatales de ciberseguridad

# Peligros



# Contraseñas



[Vídeo "Las contraseñas no son nada seguras"](#)

@cyldigital

## Malas prácticas:

- Usar la misma contraseña para distintos servicios
- Usar contraseñas débiles
- Usar información personal (fecha de nacimiento...)
- Apuntar las contraseñas en notas
- Guardar las contraseñas en webs o en el navegador
- Uso de patrones sencillos



# Contraseñas

## Cómo se obtienen:

- Prueba de diferentes combinaciones con nuestros datos personales que han conocido por otras vías
- Keylogger
- Software de diccionario. Prueba de combinaciones de palabras simples a más complejas



# Contraseñas



[Configurar doble factor](#)

## Cómo protegerse:

- Doble factor de Autenticación



[Google Authenticator](#)

[Microsot Autenticator](#)

# Contraseñas

## Cómo protegerse:

LastPass



- Contraseñas robustas
- Factor de autenticación múltiple
- Gestor de contraseñas ([lastpass](#))
- Cerrar sesiones

# Ingeniería social



## En qué consisten estos ataques:

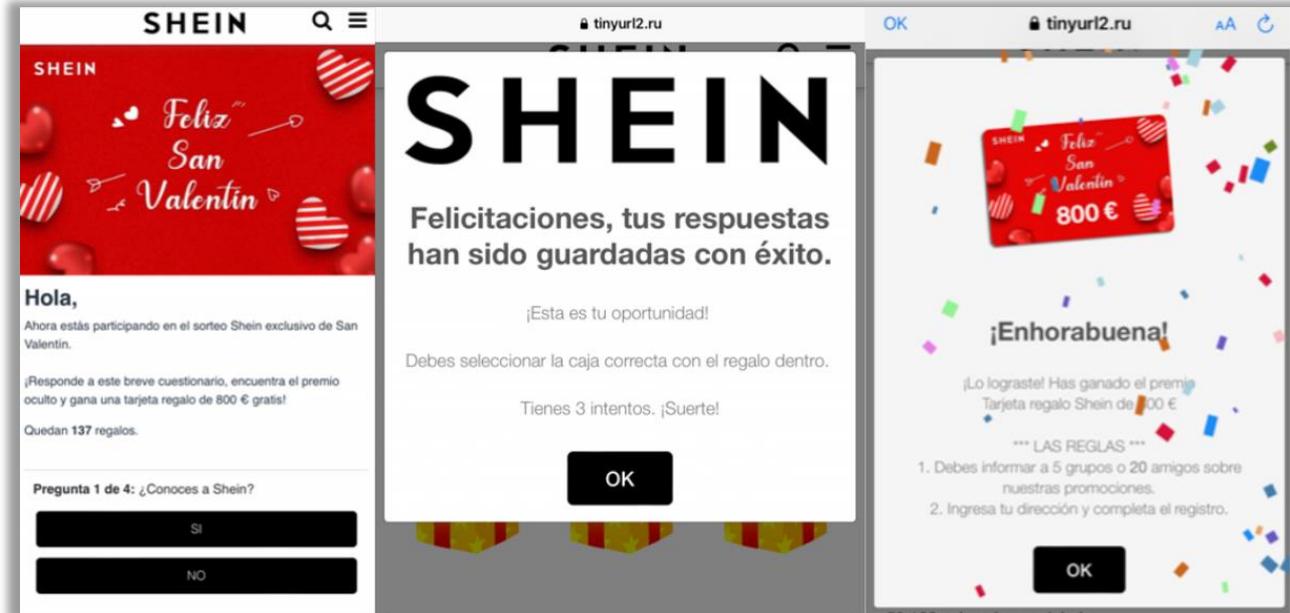
- Conjunto de técnicas que buscan conseguir que revelemos información personal o tomar el control de nuestros dispositivos.
- Objetivos:
  - Obtener datos personales y/o bancarios.
  - Descarga de malware con el que infectar o tomar el control de dispositivos.



## Fraudes online

- Estafas online para engañarnos con el fin de revelar nuestros datos personales o con el fin de obtener un beneficio económico.

# Ingeniería social



# Ingeniería social

The image displays three sequential screenshots of a phishing website designed to steal user credentials for a SHEIN gift card. The first screenshot shows a congratulatory message: "¡Felicitaciones!" and a red gift card for 800€. The second and third screenshots show a registration form with a 28 min 34 sec timer and a "CONTINUAR" button. The form fields include: NOMBRE DE PILA, APELLIDO, DIRECCIÓN, CÓDIGO POSTAL, CIUDAD, NÚMERO DE TELÉFONO, and EMAIL. A progress bar at the top of the form indicates the user is at the "Información" stage. A toggle switch at the bottom of the form is labeled "Recibir recibir notificaciones de novedades, ofertas y promociones de servicios".

# Ingeniería social

## Aviso de compensación

Hola estimado beneficiario

La Unión Europea proporciona compensación a todas las víctimas de fraude. Su correo electrónico fue encontrado en la lista de víctimas de estafa. Se pagarán un total de 3.500.000,00 € como compensación por todos los casos de fraude en 2022. Considérate afortunado de haber sido seleccionado para recibir una compensación de la Unión Europea.

NOTA. Envíe la siguiente información para sus reclamos de seguro.

Tu nombre completo: .....  
Su dirección: .....  
Copia de su pasaporte .....  
Tu país: .....  
Número de teléfono: .....

Contáctenos ahora para más información @

[compensación.offizier@gmail.com](mailto:compensación.offizier@gmail.com) o WhatsApp:  
[+49 1577 5530794](tel:+4915775530794)

Saludos  
oficina europea de indemnizaciones



Emilio Galán



Lo he recibido hoy, ¡muchas gracias!

El paquete llegó a mi casa a tiempo y en excelentes condiciones

A 978 personas les ha parecido esto útil

## Comentario de la web fraudulenta



Pitter

sports and fitness, Internet technology

4 followers · 1 following



alice88auto1

Registered

Joined: May 19, 2017

Last seen: Jul 11, 2022

Replies

0

**Imágenes originales**

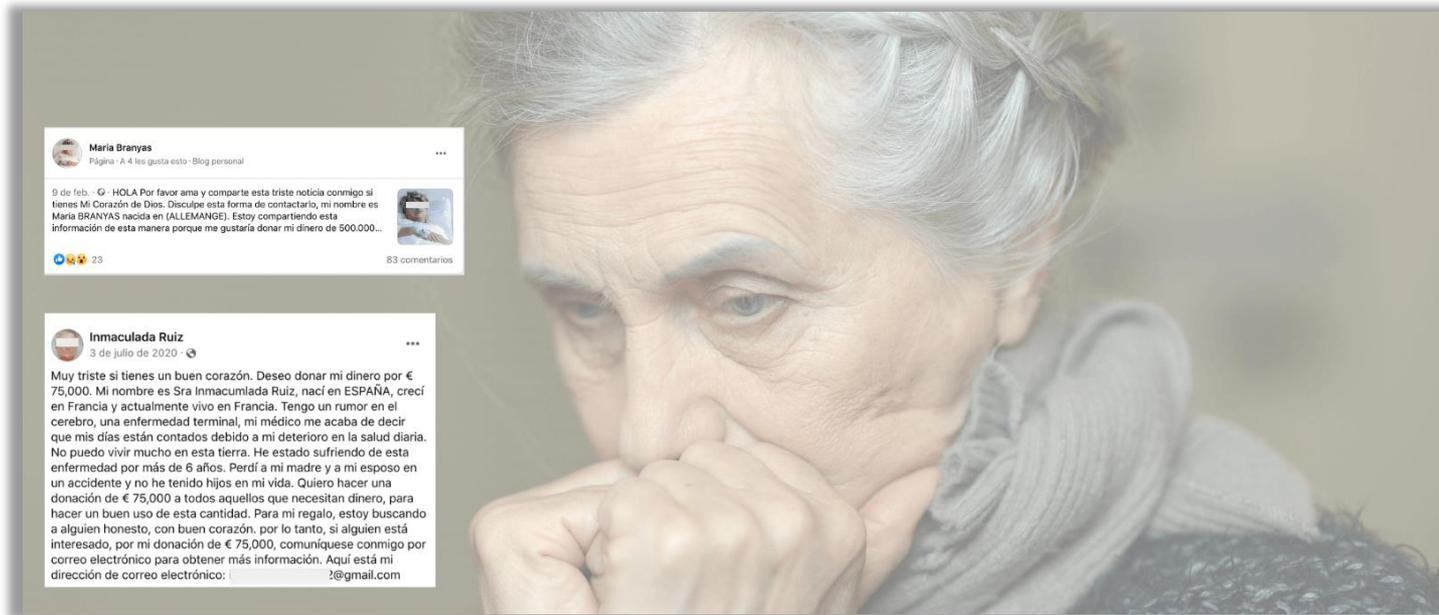
# Ingeniería social



## Phishing

- A través de medios como el correo electrónico, redes sociales o aplicaciones de mensajería instantánea

# Ingeniería social



**El timo de la persona enferma que busca herederos en Facebook: decenas de perfiles intentan cazar víctimas para pedirles dinero por supuestas gestiones**

# Ingeniería social



## Vishing

- Mediante llamadas de teléfono

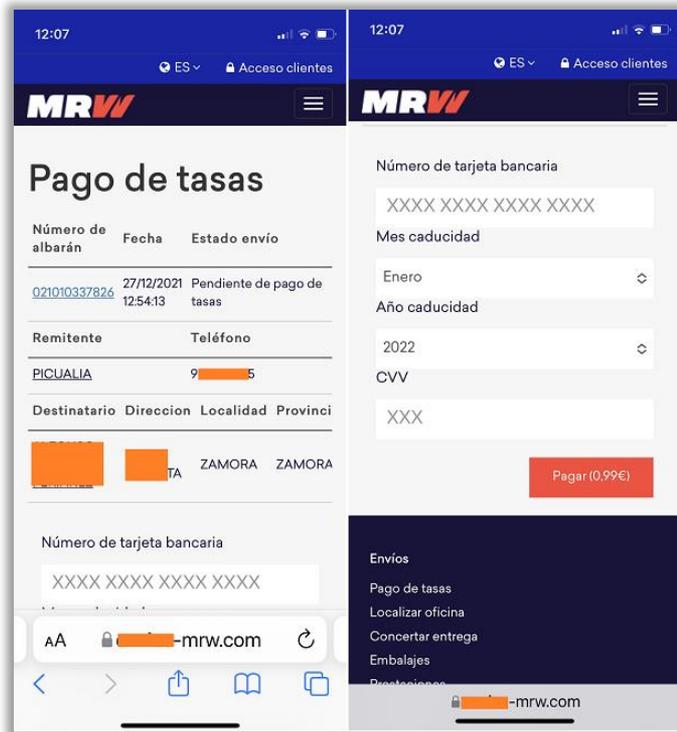
# Ingeniería social



## Smishing

- Mediante mensajes SMS

# Ingeniería social



## Smishing

- Mediante mensajes SMS

# Ingeniería social



## Spear phishing

- El ataque se centra en una persona en concreto. Recaban información sobre ella previamente

## Medidas de prevención



- Detectar errores gramaticales
- Enlace del sitio al que apunta o de la web oficial
- Comprobar remitente
- No descargar archivos adjuntos
- No contestar al mensaje y eliminarlo



## Baiting o Gancho

- USB infectados con malware para robar datos y/o tomar el control del dispositivo
- Anuncios y webs de promoción de concursos y premios (descarga software malicioso)

# Ingeniería social

## Detección de virus y otras amenazas

### Antivirus y cleaners



¿Necesitas una herramienta que detecte y elimine virus y otras amenazas en tiempo real? Lo que buscas es una herramienta antivirus. Si sospechas que tu dispositivo ya está infectado, entonces, lo que necesitas es un cleaner.

### Analizadores de URL y archivos



Para comprobar si un archivo que recibes es malicioso o una página web es fraudulenta, esta herramienta es lo que buscas. Detecta rápidamente cualquier tipo de amenaza antes de que te afecte, así evitarás muchos problemas.

## Mecanismos para proteger tus cuentas

### Doble factor de autenticación



Si quieres dotar de mayor seguridad a tus cuentas de usuario para que tú y sólo tú puedas acceder a ellas, esta es la herramienta que necesitas. Además de la contraseña, necesitarás un código que sólo tú recibirás a través del teléfono móvil.

### Gestores de contraseñas



Herramienta muy útil para que puedas almacenar todas tus contraseñas robustas y cifradas de tal forma que sólo tengas que memorizar una, la que te da acceso al resto de contraseñas guardadas.

## Baiting o Gancho

- Evitar conectar dispositivos desconocidos
- Mantener actualizados los dispositivos (software, programas, aplicaciones)
- Herramientas de protección activadas y actualizadas (antivirus)

[www.osi.es/es/herramientas](http://www.osi.es/es/herramientas)

# Ingeniería social



## Shoulder surfing

- Mirando “por encima del hombro” desde una posición cercana
- Verificar que no hay personas cercanas, verificación en dos pasos, filtros anti-espía



# Ingeniería social



[Servicio gratuito de Google para encontrar dispositivos](#)

@cyldigital

## Dumpster Diving

- Buscar en nuestra “basura” para encontrar información comprometida.
- Grandes empresas: documentos con información valiosa y sensible (datos personales, números de tarjeta de crédito, etc)
- Dispositivos electrónicos desechados que contengan información
- Prevención: eliminación segura de la información



# Ingeniería social



## Spam

- Envío de grandes cantidades de mensajes o envíos publicitarios sin haber sido solicitados. MENSAJES NO DESEADOS
- Fines comerciales
- Pueden contener algún tipo de malware

# Ingeniería social



## Spam

- Correo electrónico o cualquier otro medio que permita envío de mensajes (mensajería instantánea o redes sociales)
- Objetivos: robo de datos (phishing) o infección equipos (malware)



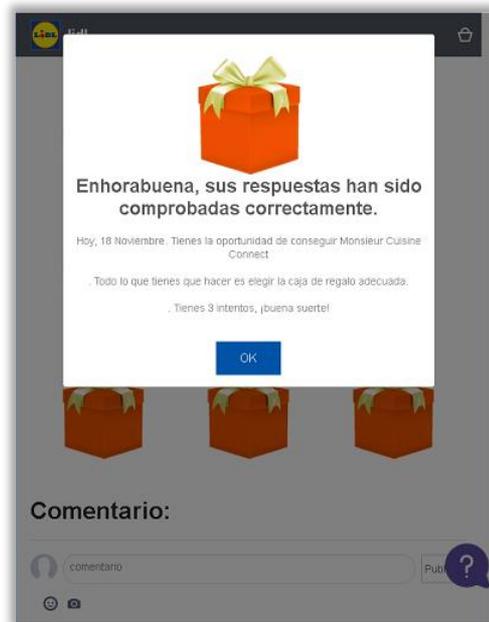
## Spam

- Usar cuenta de correo alternativa para registrarse en ofertas o promociones.
- Configurar filtro antiSpam.
- Configurar filtros antisпам en redes sociales.

# Ingeniería social



## Fraudes online



# Ingeniería social

## Fraudes online

Todos los nuevos clientes participan en el sorteo del premio del producto de la campaña que se muestra. Si eres el ganador afortunado, nos pondremos en contacto directamente por correo electrónico. Esta oferta especial incluye un periodo de prueba de 3 días de un servicio de suscripción como afiliado, tras el cual se te cargará automáticamente en tu tarjeta de crédito la comisión de suscripción (33 EUR cada 14 días). Si por cualquier motivo el servicio no te satisface, puedes cancelar tu cuenta en un plazo de 3 días. El servicio se renovará cada 14 días hasta que se cancele. Esta campaña concluirá el 31 de diciembre de 2021. Si deseas participar, ¡regístrate para una prueba de 3 días para realimentar, envía un correo electrónico a [procesaaw@qualtrics.com](mailto:procesaaw@qualtrics.com).

### El procesador para cocinar alimentos Monsieur Cuisine Connect de Silvercrest

No te pierdas esta oferta fantástica. Participa en el concurso antes de que sea demasiado tarde.



Accesorios para cocer al vapor

Volumen de cocción: 3 litros

Ajuste de temperatura de 37 a 130 °C

Báscula integrada

Lleva incorporado un sistema Cooking pilot con 213 recetas preinstaladas

Triturar 800 W

SÓLO 3€

#### Nuestra opinión

- Facilidad de uso ★★★★★
- Nivel de ruido ★★★★★
- Consumo de energía ★★★★★
- Opiniones de los usuarios ★★★★★

#### Introduce tus datos

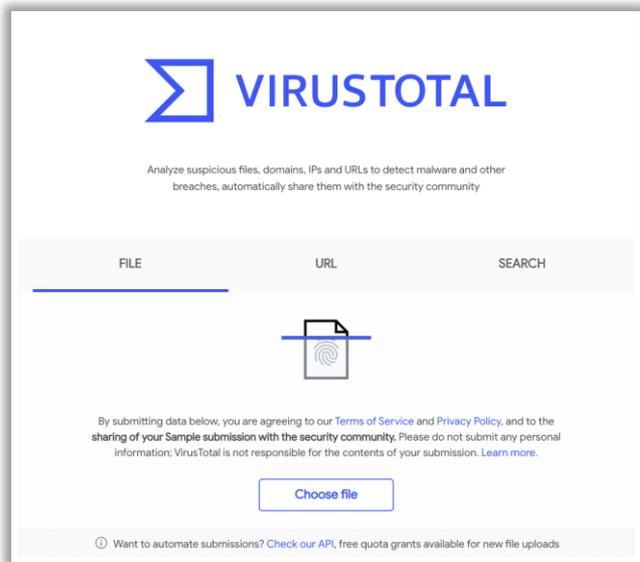
Nombre  Apellidos

Dirección

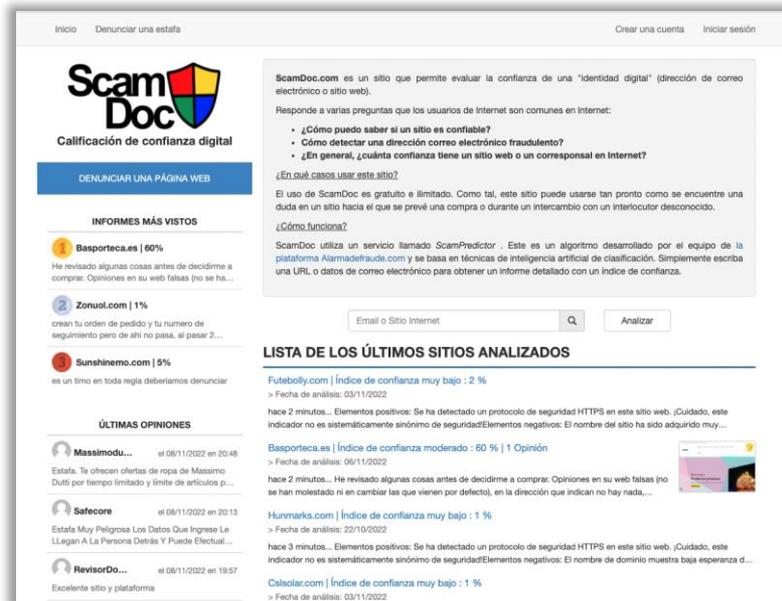
Código pi  Ciudad

Correo electrónico  N.º de teléfono

# Ingeniería social



[www.virustotal.com](http://www.virustotal.com)



[www.scamdoc.com/es](http://www.scamdoc.com/es)

# Ataques a las conexiones



## Redes Trampas

- Creación de redes wifi falsas: wifis gemelas a otras legítimas y seguras con nombre similar (ej: biblioteca\_gratis)
- Comprobar si usa protocolo https

[www.osi.es](http://www.osi.es)

# Ataques a las conexiones

## IP Spoofing

- Falso de la dirección IP para hacerla pasar por una distinta y saltarse las restricciones del router y, por ejemplo, hacer llegar un paquete con malware.
- Prevención: configuración del router.



[Guía www.osi.es](http://www.osi.es)

@cyldigital



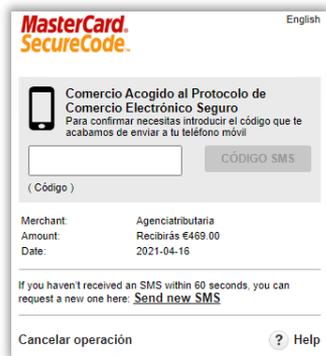
# Ataques a las conexiones



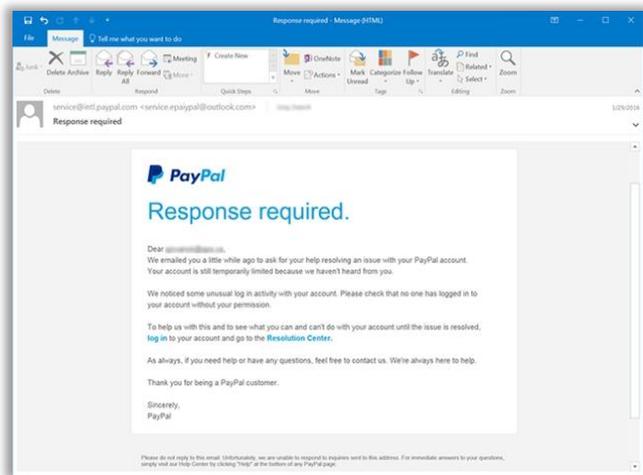
## Web Spoofing

- Suplantación de una página web real por otra falsa.
- Prevención:
  - Comprobar URL
  - Comprobar https (aunque no es señal inequívoca de que sea segura)

X  $\chi$



# Ataques a las conexiones



## Email Spoofing

- Suplanta la dirección de correo de la persona o entidad de confianza
- Prevención: Utilizar firma digital o cifrado al enviar emails.

# Ataques a Cookies



## Concepto

- Las cookies pequeños ficheros que contienen información de:
  - Páginas web que hemos visitado
  - Anuncios vistos
  - Idioma, zona horaria
  - Información de correo electrónico, contraseñas, etc.

# Ataques a Cookies



- Robo de cookies o modificación (envenenamiento) de información almacenada en una cookie a través de diferentes técnicas y malware.
- Prevención:
  - Mantener actualizado el navegador
  - Eliminar cada cierto tiempo los datos de navegación
  - Intercambio de información sensible a través de ventana de incógnito

# Malware

## Virus

- Diseñados para copiarse así mismos y propagarse a tantos dispositivos como les sea posible.
- Prevención:
  - Mantener activas y actualizadas las herramientas de protección: antivirus
  - No descargar archivos sospechosos o de origen poco fiable.



# Malware

## Spyware



- Se instala en nuestros equipos y comienza a recopilar información, supervisando toda actividad para compartirlo con un usuario remoto.
- Prevención:
  - Ignorar anuncios y ventanas emergentes, archivos o enlaces de sitios poco fiables.

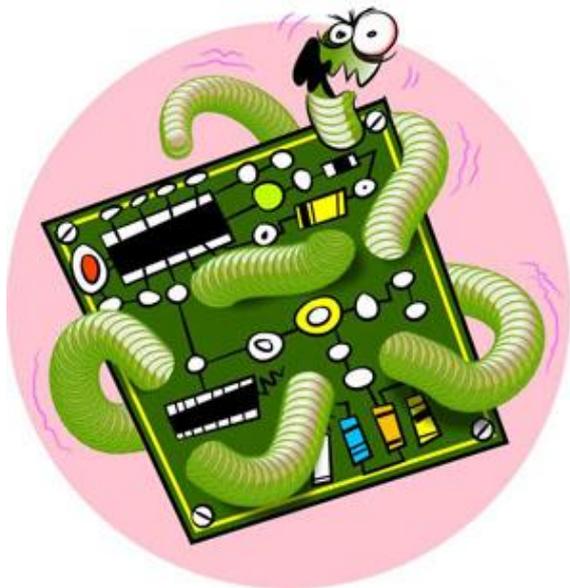
# Malware

## Troyanos



- Se camuflan como un software legítimo para infectar nuestros equipos o a través de ingeniería social.
- Prevención:
  - Mantener equipos y programas actualizados
  - Medidas de protección activas (antivirus)

# Malware



## Gusanos

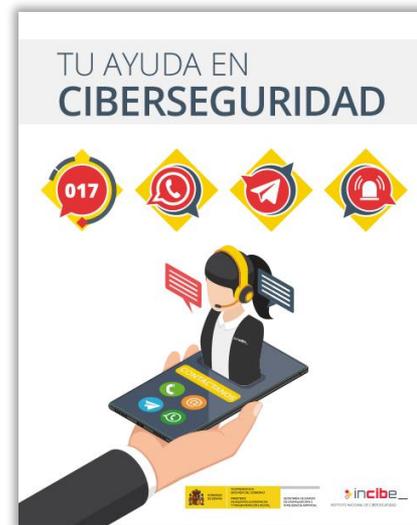
- Una vez ejecutado en un sistema puede modificar el código y características de éste.
- Prevención:
  - Mantener equipos y programas actualizados
  - Medidas de protección activas (antivirus)

# Recomendaciones

## El mejor antivirus eres tú

- Usar antivirus
- Mantener equipos actualizados: software y programas
- Utilizar contraseñas robustas y doble factor
- Desconfiar de archivos adjuntos
- Descargar de sitios oficiales
- Evitar conectarse a wifis abiertas o desconocidas
- No compartir información personal
- Hacer copias de seguridad

@cyldigital



[www.incibe.es/linea-de-ayuda-en-ciberseguridad](http://www.incibe.es/linea-de-ayuda-en-ciberseguridad)



# ¡¡Muchas Gracias!!

[www.cyldigital.es](http://www.cyldigital.es)



[@cyldigital](https://twitter.com/cyldigital)