

¡Alerta! Qué hacer si te estafan y cómo actuar con seguridad

Itziar Castro de la Hoz

Objetivo

Aprender aspectos básicos de ciberseguridad para evitar riesgos que nos puedan afectar tanto a nivel personal como profesional.



Índice

¿Qué vamos a aprender?



1.

Un poco de contexto antes de profundizar

2.

Riesgos y amenazas que encontramos en la Red

3.

Buenas prácticas

4.

Más información y ayuda

Contexto



Sociedad digital hiperconectada

- ❖ Conectados entre sí.
- ❖ Instantáneo.
- ❖ Evolución rápida y creciente de las tecnologías.
- ❖ Más conciencia en ciberseguridad.



2. Riesgos y amenazas que encontramos en la Red

SIN EMBARGO, NO ESTAMOS EXENTOS DE AMENAZAS



2. Riesgos y amenazas que encontramos en la Red



PRINCIPALES AMENAZAS 2024

- ❖ Ransomware.
- ❖ Malware.
- ❖ Ingeniería Social.
- ❖ Amenazas contra los datos.
- ❖ Denegación de servicio.
- ❖ Manipulación de la información.
- ❖ Ataques a la cadena de suministro.

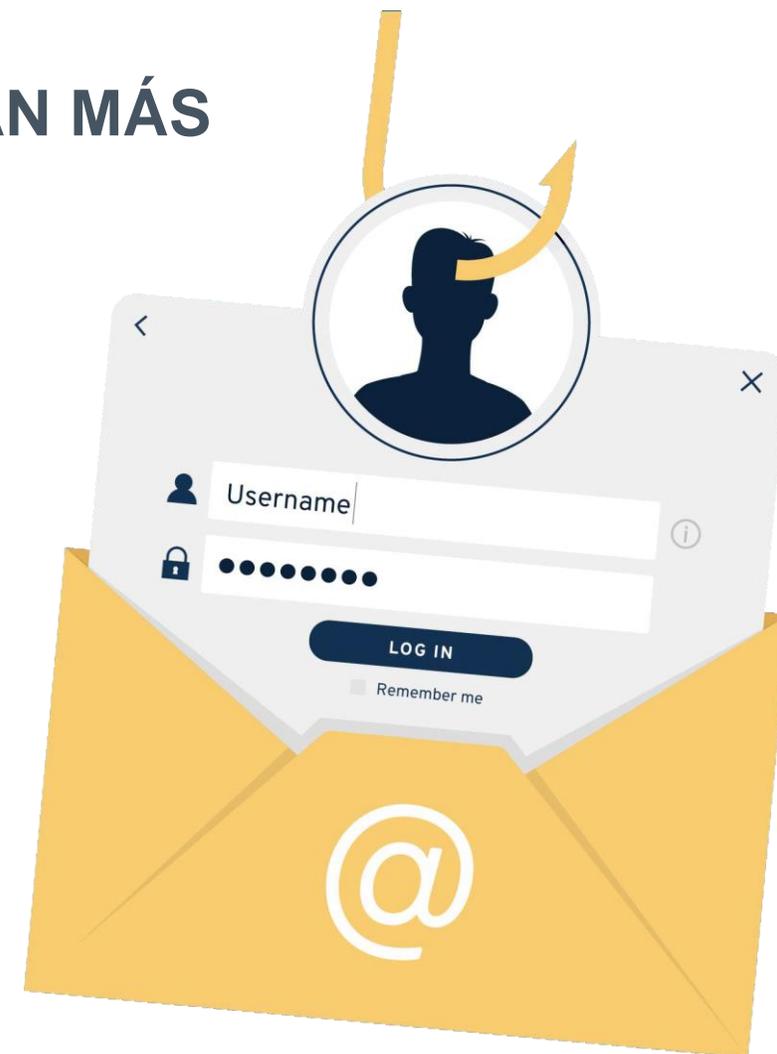
*Fuente de los datos: [*Informe de ENISA Panorama de Amenazas de 2024](#)

2. Riesgos y amenazas que encontramos en la Red

¿QUÉ TIPO DE ATAQUES NOS AFECTAN MÁS COMO USUARIOS?



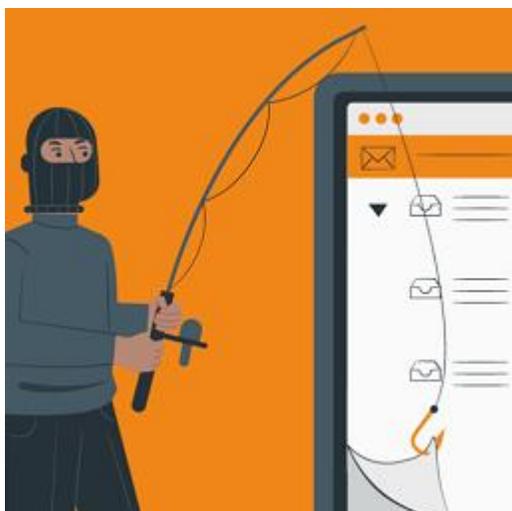
Sobre todo, aquellos que se apoyan en técnicas de **Ingeniería social**.



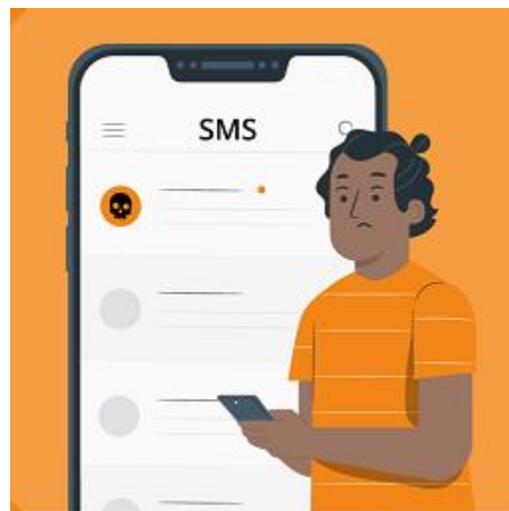
2. Riesgos y amenazas que encontramos en la Red

Phishing, vishing y smishing

El correo electrónico, los SMS, las redes sociales y Whatsapp son los canales más utilizados por la ingeniería social.



Phishing



Smishing



Vishing

Smishing: Caso real

INICIO / CIUDADANÍA / Avisos / Cuidado si recibes un SMS de la DGT para el pago de una multa

Cuidado si recibes un SMS de la DGT para el pago de una multa

← DGT

16:43

Sede Electronica , tiene una multa impagada de 35 euros, que se incrementara en 24 horas si no recibimos el pago:



← ⌂ Dangerous | aā 🔍 🔊 ☆ 📄 ⌵ 🗑️ 🔄

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR DGT Dirección General de Tráfico

Pago de sanciones

Pagos

PAGO DE SU MULTA N°164357371274

Confirme su identidad

Apellido *	Nombre *
<input type="text"/>	<input type="text"/>
Fecha de nacimiento *	Dirección postal *
<input type="text" value="JJ/MM/AAAA"/>	<input type="text"/>
Código postal *	Ciudad *
<input type="text" value="XXXXX"/>	<input type="text"/>
Email *	Número de teléfono *
<input type="text" value="correo2@dgt.es"/>	<input type="text" value="+34"/>

Continuar

¿Cómo reconocer un phishing, o un smishing?

¿QUÉ ES EL SMISHING?

El remitente es un número de teléfono desconocido.

Solicitan datos personales, credenciales o bancarios bajo alguna excusa.

Fraude que consiste en suplantar a entidades y servicios a través del envío de SMS cuyo objetivo es robar tus datos o infectar tus dispositivos.

El mensaje es importante, urgente o llamativo que lleva a la acción.

A veces, invitan a descargar una supuesta aplicación oficial en el móvil.

¿Recibiste un SMS sospechoso? ¡No pulses en ningún enlace ni proporciones información!

Se facilita un enlace, generalmente acortado, para proceder con la gestión.

¡Corre, no esperes más!

Descarga nuestra app: www.smhising.com

¡Enhorabuena!!!
Acaba de ganar 500 euros en nuestro sorteo, para reclamar tu premio indica tus datos personales en nuestra app.

Desconocido
+34 600 000 000

¡Recuerda que esto no es una buena práctica!

Si ya es tarde y han conseguido engañarte:

- 1 Cambia tus contraseñas de inmediato. También en aquellos sitios online en los que utilices esa misma clave.
- 2 Contacta con tu entidad bancaria si tus datos bancarios pueden estar comprometidos. ¡Ellos te ayudarán!
- 3 Contrasta la información con la empresa que supuestamente te está contactando a través de sus canales oficiales.
- 4 Reporta el SMS malicioso a INCIBE (incidencias@incibe-cert.es)
- 5 Interpón una denuncia en las Fuerzas y Cuerpos de Seguridad del Estado aportando las evidencias.
- 6 Y si aún tienes dudas, contacta con Tu Ayuda en Ciberseguridad de INCIBE, llamando al 017, o a través de WhatsApp (900 116 117) o Telegram (@017INCIBE).

017

Remitente

1 SocialNet <info@socialneet.es>
para mi

Mensaje

2 Estimado usuario de SocialNet

3 SocialNet

4 Redacción

5 Enlaces

6 Adjuntos

Factura.doc

http://social.net/do/trkln.php?

Factura.doc

Factura.doc

Factura.doc

incidencias@incibe-cert.es



Vishing : Caso real

INICIO / INCIBE / Tu Ayuda en Ciberseguridad / Casos Reales / Nueva variante del robo de cuenta de WhatsApp suplantando al soporte técnico

Nueva variante del robo de cuenta de WhatsApp suplantando al soporte técnico

Fecha de publicación 10/09/2024



Otros fraudes

CAMISETA COMITE OLIMP. PORTUGAL BLANCO M/C

€4 €14

SERVICIO

10% DCTO. EN EL PRIMER PEDIDO
¡CREA UNA CUENTA Y RECIBE UN CUPÓN
ENVÍO GRATIS MÁS DE €35

Tallas

4XS-3XS

[GUÍA DE TALLAS](#)

Cantidad

1

AÑADIR AL CARRITO



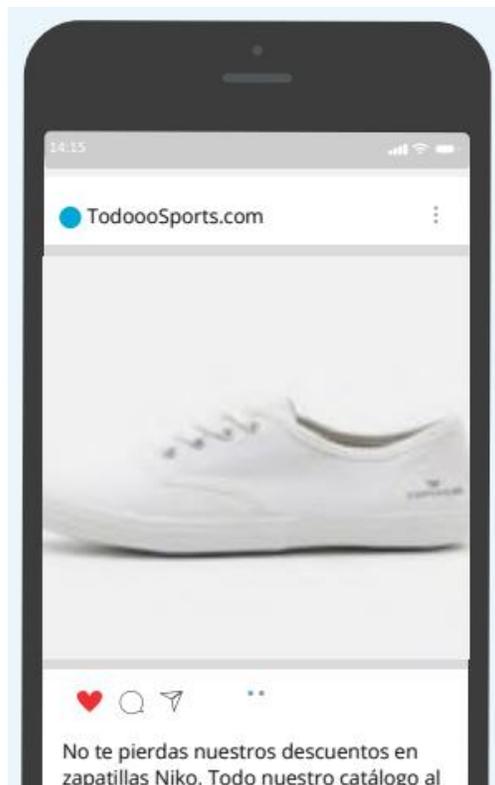
ENVÍO EXPRESS

Envío dentro de 24 horas



DEVOLUCIÓN GRATIS

Las devoluciones son gratis **hasta 365 días**
envío



Cámara Visión Nocturna

Four Seasons - 5 de marzo de 2014
Entretenimiento

Instalar **Añadir a la lista de deseos**

i Esta aplicación es compatible con tu dispositivo.

★★★★☆ (267) **g+** +220



NIKE **OFERTA 79%**

Zapatillas NIKE 578

★★★★★
Color innovador modelo clásico y materiales son impecables.

Perfecta Buena oferta.
Nos ha parecido correcto, buen producto.
Hoy recibí el producto. Bien atención.

11'34 EUR ~~54'00 EUR~~

COMPRAR

Dependiendo del stock y la demanda es posible que se apliquen costes adicionales.



¿Qué más podemos hacer?



3. Buenas prácticas

1. PON A PUNTO TUS DISPOSITIVOS



Instala una herramienta antivirus



Actualiza el sistema operativo, así como el resto de programas



Crea cuentas de usuario diferentes

3. Buenas prácticas

2. HAZ COPIAS DE SEGURIDAD

5 Razones
por las que hacer copias de seguridad

COPIANDO 75%

Todos tenemos información que queremos **proteger, guardar y preservar en el tiempo**. Para ello, lo mejor es crear copias de seguridad.

1 Estás prevenido en caso de deterioro del dispositivo

2 Proteges la información

3 La preservas en el tiempo

4 Liberas espacio

5 La proteges de ti mismo

DISCO EXTERNO (F:)

1,2 GB disponibles de 100 GB

¿ESTÁ SEGURO?
BORRAR TODO
ACEPTAR

3. Buenas prácticas

3. SE CAUTO CON LAS REDES A LAS QUE TE CONECTAS

WiFi Pública

3. Comprueba que la red gratuita disponible es la oficial del lugar en el que estás.



4. ¡En cualquier lugar público hay mirones! Protege tu pantalla de miradas indiscretas.



1. Evita la conexión automática y elimina los accesos a las redes WiFi una vez haya finalizado su uso.



2. Evita realizar compras online o intercambiar información sensible.



5. Sé precavido y mantén actualizados tus dispositivos y sus aplicaciones.



6. Siempre que estén disponibles, conéctate a páginas con certificado de seguridad, con https://



3. Buenas prácticas

4. NO COMPARTAS FOTOS DE TU DNI

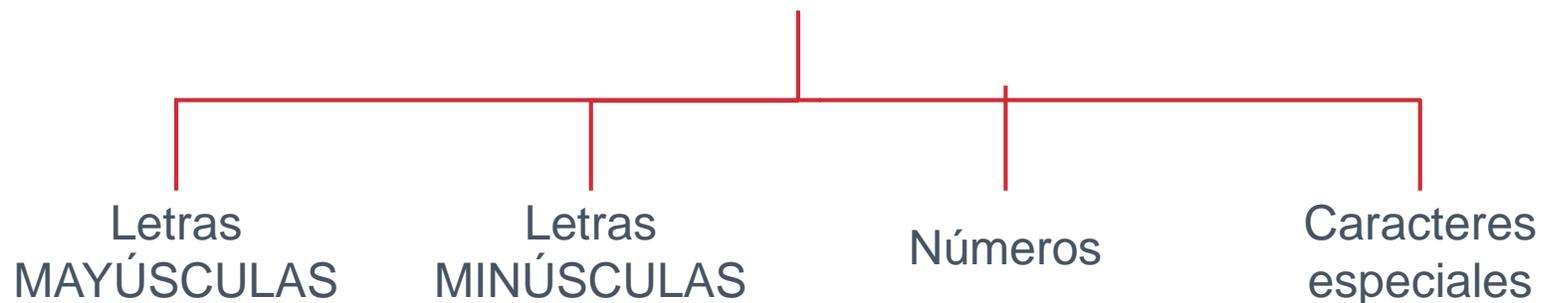


- ❖ Suplantación de identidad.
- ❖ Pérdida de control de la información.
- ❖ Vulnerabilidades en las comunicaciones.
- ❖ Mala configuración en redes sociales y sobre exposición de información.
- ❖ Almacenamiento de información en la nube y compartir por error.

3. Buenas prácticas

5. GESTIONA CORRECTAMENTE TUS CONTRASEÑAS

Al menos 12 caracteres



No reutilizar contraseñas, usa contraseñas diferentes para distintos servicios.



Dependiendo de la criticidad de la información que maneje el servicio, se establecerá una mayor o menor periodicidad para el cambio de contraseña.

3. Buenas prácticas

5. GESTIONA CORRECTAMENTE TUS CONTRASEÑAS

¿SABÍAS QUE EXISTEN HERRAMIENTAS PARA COMPROBAR SI UNA CLAVE ES ROBUSTA?

¡COMPARTO ALGUNOS EJEMPLOS!



ES FAQ

Comprueba tu contraseña

Tu contraseña no es segura si puede ser averiguada mediante un ataque de fuerza bruta o se encuentra en una base de datos de contraseñas filtradas.

No recopilamos ni almacenamos las contraseñas. [Más información](#)



- <https://password.kaspersky.com/es/>
- <https://password.es/comprobador/>
- <https://howsecureismypassword.net/>

3. Buenas prácticas

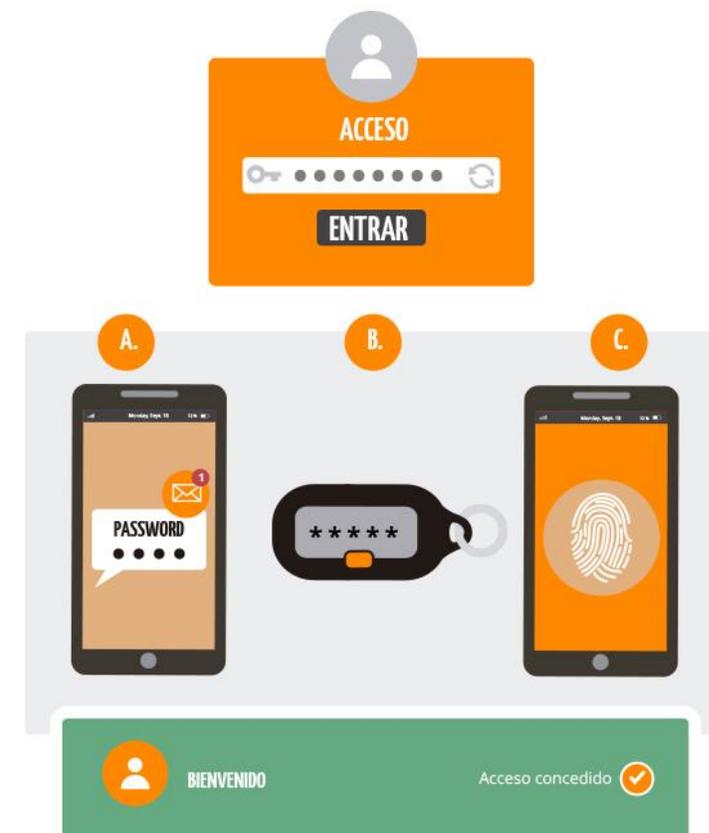
5. GESTIONA CORRECTAMENTE TUS CONTRASEÑAS

SISTEMAS DE DOBLE VERIFICACIÓN = DOBLE AUTENTICACIÓN = DOBLE FACTOR = VERIFICACIÓN EN DOS PASOS

Google authenticator



Microsoft authenticator



3. Buenas prácticas

OTRAS CUANTAS

- ❖ Comprueba si la web es fiable
- ❖ Revisa las Apps y los permisos
- ❖ Configura tu privacidad
- ❖ Piensa antes de publicar



DESCARGA

En tiendas oficiales

Las plataformas Google Play o AppStore cuentan con medidas de seguridad para evitar aplicaciones fraudulentas.

1. **Revisa quién es el desarrollador de la app.**
Las empresas o desarrolladores conocidos en teoría ofrecen más garantías de seguridad. Chequea que redirigen a un sitio seguro y profesional.

2. **Echa un vistazo a los comentarios.**
Si tiene pocos comentarios y todos positivos, o si tiene muchos y negativos... ¡Desconfía!

3. **Comprueba el número de descargas.**
Una app famosa con pocas descargas puede significar que nos encontremos ante una copia de la misma poco fiable.

7,5
Más de 100 mil Descargas

QUÉ DATOS

no debes compartir nunca en Internet

¡Ajusta bien los niveles de privacidad!

Configura la privacidad de tu perfil para que no quede **abierto** y tu **información disponible para cualquiera**.

Nivel de privacidad alto 😄	Nivel de privacidad medio 😞	Nivel de privacidad bajo 😞
Controlaremos en todo momento quién puede ver nuestra información y publicaciones.	Solo aquellas personas que tengamos agregadas podrán visualizar nuestra información y publicaciones (algunas podrán ser privadas si así quisiésemos).	Cualquier persona fuera de nuestro "círculo de contactos" puede tener acceso a toda nuestra información publicada en la Red social.

017 TU AYUDA EN CIBERSEGURIDAD

Dónde encontrar más información y soporte

Servicio gratuito y confidencial, disponible de 08:00 am a 11:00 pm los 365 días del año.



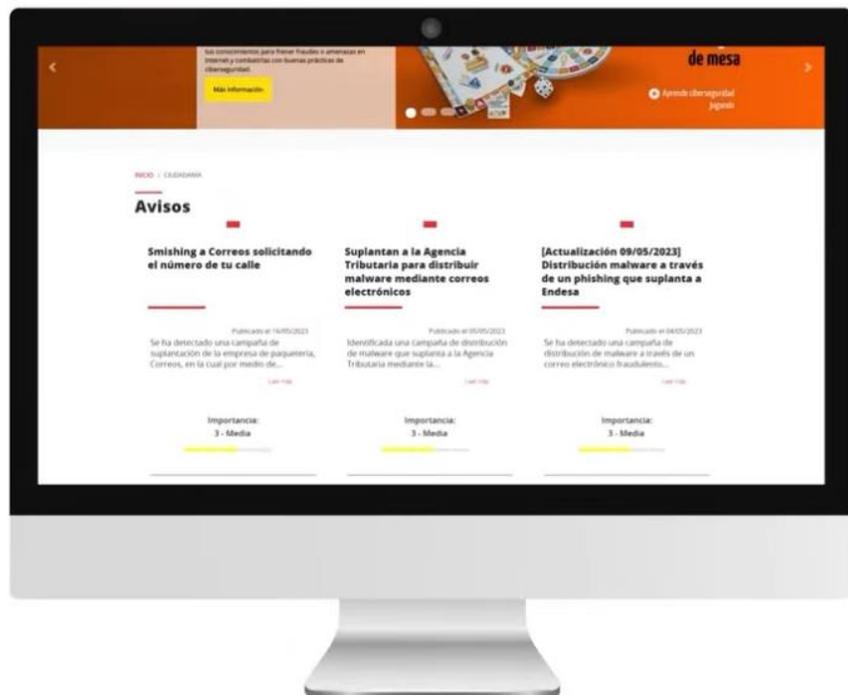
TU AYUDA EN CIBERSEGURIDAD

-  **017**
Teléfono 017
-  WhatsApp 900 116 117
-  Telegram @INCIBE017
-  Formulario web
-  Atención presencial



www.incibe.es/linea-de-ayuda-en-ciberseguridad

OFICINA DE SEGURIDAD DEL INTERNAUTA



❖ Servicios de avisos y blog



❖ Recursos didácticos y divulgativos



❖ Iniciativas formativas



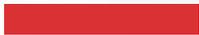
❖ Redes sociales



www.incibe.es/ciudadania



INSTITUTO NACIONAL DE CIBERSEGURIDAD



GOBIERNO DE ESPAÑA

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

