

GUÍA DE CIBERSEGURIDAD

Para Usuarios Particulares

Todo lo que necesitas saber para proteger tus dispositivos y tu vida digital

💡 ¿Para quién es esta guía?

Escrita en lenguaje sencillo, sin tecnicismos. Te explica qué riesgos existen en tu día a día digital y qué acciones concretas puedes tomar para estar más protegido/a. No hace falta ser informático/a.

🔑 1. CONTRASEÑAS: Tu primera línea de defensa

⚠️ ¿Sabías que...?

El 80% de los ciberataques exitosos se producen porque las contraseñas son demasiado sencillas o se reutilizan en varios servicios. Una contraseña robada en una web puede abrir la puerta a tus cuentas de banco, correo o redes sociales.

✅ HAZLO	❌ EVÍTALO
✅ Usa contraseñas largas (+12 caracteres)	❌ Usar '123456' o 'password'
✅ Mezcla letras, números y símbolos	❌ Poner tu nombre o fecha de nacimiento
✅ Una contraseña diferente para cada servicio	❌ La misma contraseña en todos los sitios
✅ Usa un gestor de contraseñas (Bitwarden, 1Password...)	❌ Guardar contraseñas en papel junto al ordenador
✅ Activa la verificación en dos pasos (2FA)	❌ Compartir contraseñas por WhatsApp o email
✅ Cambia contraseñas si hay una brecha de seguridad	❌ Ignorar avisos de inicio de sesión sospechoso

📱 ¿Qué es la verificación en dos pasos (2FA)?

Es como poner un segundo candado. Aunque alguien robe tu contraseña, necesitaría también tu móvil para entrar. Actívala en tu banco, correo y redes sociales. Apps recomendadas: Aegis o Authy.



2. REDES WIFI: No todo lo que brilla es seguro



En casa: Cambia el nombre de tu WiFi y la contraseña que viene de fábrica en el router. La de fábrica es fácilmente hackeable.



Usa cifrado WPA2 o WPA3 en tu router (se configura en la web del router). Evita WEP, es muy antiguo e inseguro.



Crea una red WiFi de invitados para las visitas. Así no acceden a tus dispositivos principales.



Las redes WiFi públicas (cafeterías, aeropuertos, hoteles) son peligrosas. Cualquiera puede interceptar lo que envías.



En redes públicas: nunca accedas a tu banco, no hagas compras y no introduzcas contraseñas si puedes evitarlo.



Actualiza el firmware (software interno) de tu router cuando haya actualizaciones disponibles.



Red WiFi pública = Riesgo real

Los atacantes pueden crear redes WiFi falsas con nombres como 'WiFi_Hotel_Gratis' o 'AeropuertoFree'. Tu móvil se conecta automáticamente y ellos ven todo tu tráfico. Si te conectas a una red pública, usa siempre una VPN (ver sección siguiente).



3. VPN: Un túnel seguro para tu conexión

¿Qué es una VPN?

Una VPN (Red Privada Virtual) es como un túnel cifrado entre tu dispositivo e Internet. Todo lo que envías pasa por ese túnel, y nadie de fuera puede ver el contenido. Es especialmente útil en redes WiFi públicas.



Úsala siempre que te conectes a una WiFi pública (aeropuertos, cafeterías, hoteles, centros comerciales).



También sirve para proteger tu privacidad en general: tu proveedor de internet no puede ver qué páginas visitas.



VPNs de pago recomendadas: ProtonVPN, Mullvad, NordVPN, ExpressVPN. Ofrecen mejor privacidad que las gratuitas.



Cuidado con VPNs gratuitas desconocidas: algunas venden tus datos o inyectan publicidad. Si es gratuita, el producto eres tú.



Instálala también en el móvil, no solo en el ordenador. Usamos el móvil más y en más redes distintas.

4. PUNTOS DE CARGA PÚBLICOS: El 'Juice Jacking'

⚠️ ¡Peligro en los puertos USB públicos!

'Juice Jacking' es el nombre del ataque donde conectar tu móvil a un puerto USB público (en aeropuertos, hoteles, centros comerciales) puede permitir a los atacantes robar tus datos o instalar software malicioso. Un cable USB transmite tanto energía como datos.

- Usa SIEMPRE tu propio cargador enchufado a la red eléctrica. Es lo más seguro.
- Lleva un 'condón USB' o bloqueador de datos: un adaptador pequeño que solo deja pasar la corriente, no los datos. Cuestan menos de 5 euros.
- Lleva una batería portátil (powerbank) propia. Es la solución más práctica cuando viajas.
- Si no tienes otra opción: en iOS aparece un aviso preguntando si confías en el dispositivo. Elige 'Solo carga'. En Android activa el 'Modo de carga' si está disponible.
- Nunca uses cables USB que encuentres olvidados o te regalen en eventos. Pueden ser cables trampa con chips maliciosos integrados.

5. BLUETOOTH: Cuando lo invisible ataca

Ataques comunes por Bluetooth







- Bluejacking: envío de mensajes no solicitados. Molesto pero generalmente inofensivo.
- Bluesnarfing: robo de datos (contactos, mensajes, fotos) a través de Bluetooth. Más peligroso.
- Bluebugging: control remoto de tu dispositivo. El más grave. Puede hacer llamadas o leer mensajes.
- Tracking: rastreo de tu ubicación mediante Bluetooth sin que lo sepas.

☑️ HAZLO	❌ EVÍTALO
☑️ Apaga el Bluetooth cuando no lo uses	❌ Dejar el BT siempre encendido en zonas públicas
☑️ Pon tu dispositivo en modo 'no visible'	❌ Aceptar solicitudes de emparejamiento desconocidas
☑️ Acepta solo conexiones de personas conocidas	❌ Emparejar dispositivos en lugares concurridos
☑️ Actualiza el software de auriculares y altavoces BT	❌ Ignorar notificaciones extrañas de Bluetooth
☑️ Revisa los dispositivos emparejados y elimina los que no reconozcas	❌ Usar BT abierto en hoteles o aeropuertos

6. NFC: Pagos contactless y más

¿Qué es el NFC?





El NFC (Comunicación de Campo Cercano) es la tecnología que permite los pagos con el móvil (Google Pay, Apple Pay) y acercar tarjetas para pagar. Funciona a muy corta distancia (menos de 10 cm) pero tiene sus riesgos.




-  Activa el NFC SOLO cuando lo vayas a usar. Ve a la configuración de tu móvil y desactívalo en el día a día.
-  Usa billeteras digitales (Google Pay, Apple Pay) en vez de la tarjeta física: son más seguras porque no transmiten tu número real de tarjeta.
-  Existe el 'skimming NFC': alguien con un lector puede intentar leer tu tarjeta. Las fundas y carteras con protección RFID/NFC lo evitan.
-  Cuidado con pegatinas NFC desconocidas en carteles o mesas (en restaurantes, por ejemplo). Podrían redirigirte a webs maliciosas.
-  Si tienes NFC activo, bloquea la pantalla cuando no la uses. Los pagos NFC requieren pantalla desbloqueada en la mayoría de móviles.
-  Revisa periódicamente los movimientos de tu banco para detectar cargos no autorizados.

7. TUS DISPOSITIVOS: Mantenlos al día

La actualización más aburrida es la más importante

El 60% de los ataques aprovechan fallos de seguridad que ya tenían solución disponible. Actualizar no es opcional: es la vacuna de tus dispositivos. Configura las actualizaciones automáticas y verás que casi nunca tienes que hacer nada.

-  Activa las actualizaciones automáticas en todos tus dispositivos: móvil, tablet, ordenador, incluso smart TV.
-  Instala un antivirus. En Windows, el Windows Defender (ya incluido) es suficiente para la mayoría. En Mac, el sistema tiene protecciones, pero un antivirus extra añade seguridad.
-  En Android: descarga aplicaciones solo de Google Play. En iPhone: solo de App Store. Desconfía de aplicaciones que piden permisos extraños (¿por qué necesita tu linterna acceso a tus contactos?).
-  Activa el PIN, huella o reconocimiento facial en todos tus dispositivos. Si pierdes el móvil, que nadie pueda acceder.







-  Desinstala las aplicaciones que ya no uses. Menos aplicaciones = menos puertas de entrada para ataques.
-  Haz copias de seguridad regularmente: fotos, documentos importantes. Usa la nube (Google Photos, iCloud) o un disco externo.
-  Revisa los permisos de tus aplicaciones periódicamente (configuración > aplicaciones > permisos). Retira lo que no sea necesario.

8. CORREO Y PHISHING: El gran engaño

El phishing es el ataque más común del mundo

El 'phishing' consiste en hacerse pasar por tu banco, Correos, la Agencia Tributaria u otras entidades para que hagas clic en un enlace falso e introduzcas tus datos. Es el método de ataque número 1 a nivel mundial.

Señales de alerta en un email sospechoso:

-  Te piden que actúes **URGENTEMENTE**: 'Tu cuenta será bloqueada en 24 horas!'. La urgencia es una trampa.
-  El remitente tiene un email raro: 'banco@servicio-seguro-notificaciones.com' en vez de '@caixabank.es'.
-  El enlace lleva a una web con un nombre extraño. Pasa el ratón por encima del enlace SIN hacer clic para ver a dónde va.
-  Hay errores de ortografía o el texto suena extraño, como traducido de otro idioma.
-  Te piden descargar un archivo adjunto que no esperabas. Nunca abras archivos adjuntos de remitentes desconocidos.
-  Te piden datos bancarios, contraseñas o números de tarjeta por email. Ninguna empresa legítima lo hace.



9. WHATSAPP Y SMS FALSOS: La estafa que llega al móvil

Smishing: el phishing por mensaje

El smishing es el mismo engaño que el phishing por correo, pero llega por SMS o WhatsApp. Un mensaje de 'Correos', de tu 'banco' o incluso de tu 'hijo/a' que ha perdido el móvil y necesita dinero urgentemente. Muy común y muy efectivo.



Desconfía de cualquier mensaje con un enlace, aunque parezca venir de una empresa conocida. Si tienes dudas, llama directamente a la empresa por un número oficial.



Tu banco NUNCA te pedirá la contraseña, el PIN o códigos de seguridad por SMS o WhatsApp. Si lo hace, es una estafa.



La estafa del hijo/a: 'Mamá, he perdido el móvil, escríbeme aquí'. Compruébalo siempre llamando al número habitual de tu familiar antes de enviar nada.



SMS de Correos o de empresa de mensajería: 'Tu paquete está retenido, paga 1,99 €'. Accede siempre a la web oficial, nunca por el enlace del mensaje.



Bloqueo y denuncia: en WhatsApp y en cualquier app de mensajería puedes bloquear y denunciar números sospechosos fácilmente.



Activa el filtro de spam de tu móvil para los SMS. En iOS: Configuración > Mensajes > Filtrar remitentes desconocidos. En Android: Mensajes > Menú > Bloquear números.










PIN de WhatsApp: actívalo ahora mismo

WhatsApp tiene un PIN de verificación en dos pasos que impide que alguien active tu cuenta en otro dispositivo, aunque consiga tu número de teléfono. Actívalo en: WhatsApp > Configuración > Cuenta > Verificación en dos pasos. Elige un PIN de 6 dígitos que recuerdes bien. Es gratuito y tarda menos de un minuto.

10. COMPRAS EN LÍNEA: Compra seguro/a, compra tranquilo/a

Cómo identificar una web falsa o peligrosa

-  Comprueba que la web empiece por 'https://' y que haya un candado en la barra del navegador. Sin candado, no introduzcas datos de pago.
-  Verifica bien el nombre del dominio: 'amaz0n.es', 'amazon.com' o 'amazon-ofertas.net' NO son Amazon. Los estafadores imitan nombres reales con pequeños cambios.
-  Paga preferiblemente con tarjeta virtual o de prepago para compras en línea. Algunos bancos las generan desde la app. Así limitas el saldo expuesto.
-  Lee las opiniones y comprueba el tiempo que lleva la web en funcionamiento. Desconfía de precios muy por debajo del mercado: si es demasiado bueno para ser verdad, probablemente no lo es.
-  Guarda siempre el correo de confirmación de la compra y el número de pedido. Son tu prueba en caso de reclamación.
-  Comprueba la política de devoluciones antes de comprar. Una tienda legítima siempre la tiene clara y visible.
-  Nunca hagas compras en línea conectado a una WiFi pública. Hazlo siempre desde tu red de casa o con los datos móviles.

Truco rápido para saber si una web es de fiar

Busca el nombre de la tienda en Google añadiendo la palabra 'estafa'. Por ejemplo: 'TiendaXYZ estafa'. Si hay víctimas, las encontrarás en foros y redes sociales en cuestión de segundos.

11. DISPOSITIVOS INTELIGENTES EN CASA: El hogar conectado

Tu hogar puede ser una puerta de entrada para hackers

La Smart TV, el altavoz inteligente, la cámara del timbre, el robot aspirador... Cada dispositivo conectado es una puerta potencial. Muchos salen de fábrica con contraseñas por defecto que nunca se cambian, y los atacantes lo saben.



Smart TV: actualiza el firmware regularmente, desactiva el micrófono si no usas el control por voz, y revisa qué aplicaciones tienes instaladas.



Altavoces inteligentes (Alexa, Google Home): siempre están escuchando. Desactiva el micrófono físicamente cuando no los uses y borra el historial de voz periódicamente desde la app.



Cámaras IP y timbre inteligente: cambia la contraseña por defecto INMEDIATAMENTE. Una cámara sin contraseña cambiada es accesible desde internet para cualquier persona.



Enchufes y bombillas inteligentes: conéctalos a la red de invitados del router, separada de tus ordenadores y móviles. Si se comprometen, no podrán acceder a los dispositivos principales.



Robot aspirador: muchos hacen mapas de tu casa y los envían a la nube. Lee la política de privacidad y desactiva el envío de datos si puedes.



Regla de oro: cambia siempre la contraseña de fábrica de CUALQUIER dispositivo que conectes a internet, el mismo día que lo pones en marcha.



12. COMPRUEBA SI TE HAN ROBADO DATOS

Las filtraciones de datos: cuando ocurre sin que lo sepas

Cada año, miles de empresas sufren filtraciones de datos. Tus correos, contraseñas o datos personales pueden estar circulando por internet sin que tengas ni idea. Aquí tienes cómo comprobarlo.



Visita haveibeenpwned.com: introduce tu correo electrónico y te indica si ha aparecido en alguna filtración conocida. Es gratuito y seguro.



Activa las alertas gratuitas en haveibeenpwned.com para que te avisen por correo si tu email aparece en futuras filtraciones.



Si tu correo ha aparecido en una filtración: cambia la contraseña de ese servicio inmediatamente y, si era la misma en otros sitios, cámbialas todas.



Google Alerts (alerts.google.com): configura una alerta con tu nombre completo entre comillas. Recibirás un correo si tu nombre aparece en nuevas páginas web.



Muchos gestores de contraseñas (Bitwarden, 1Password) te notifican automáticamente si alguna de tus contraseñas ha sido comprometida en una filtración.









Tu banco probablemente tiene un servicio de alertas por SMS o app. Activa las notificaciones de cualquier movimiento, por pequeño que sea. Es la manera más rápida de detectar un fraude.



Compruébalo ahora mismo





















Abre el navegador, ve a haveibeenpwned.com e introduce tu correo principal. Tarda menos de 30 segundos. Si aparece en alguna filtración, cambia la contraseña de ese servicio hoy mismo.

13. REDES SOCIALES Y PRIVACIDAD

-  Revisa la configuración de privacidad de tus redes sociales. ¿Quién puede ver tus fotos? ¿Tu fecha de nacimiento? ¿Tu ubicación?
-  Desactiva la geolocalización en las fotos. Las fotos con ubicación pueden revelar dónde vives o dónde están tus hijos.
-  No aceptes solicitudes de desconocidos. Los perfiles falsos se usan para el robo de información y estafas.
-  No publiques información sensible: número de teléfono, dirección, cuándo te vas de vacaciones (invitas a robar en casa).
-  Cuidado con los tests y encuestas virales ('¿Cuál es tu nombre de pirata?'). Recopilan información personal.
-  Piénsalo dos veces antes de publicar fotos de tus hijos. Una vez publicadas, pierdes el control sobre ellas.

CHECKLIST: ¿Estás protegido/a?

Marca lo que ya tienes hecho. ¡Cuantas más, mejor!

	<input type="checkbox"/> Contraseñas largas y diferentes para cada servicio
	<input type="checkbox"/> Verificación en dos pasos activada en el correo y el banco
	<input type="checkbox"/> Gestor de contraseñas instalado
	<input type="checkbox"/> Contraseña y nombre del WiFi de casa cambiados
	<input type="checkbox"/> WPA2 o WPA3 activado en el router
	<input type="checkbox"/> VPN instalada para redes públicas
	<input type="checkbox"/> Bluetooth desactivado cuando no lo uso
	<input type="checkbox"/> NFC desactivado cuando no lo uso
	<input type="checkbox"/> No uso puertos USB públicos para cargar
	<input type="checkbox"/> Actualizaciones automáticas activadas en todos los dispositivos
	<input type="checkbox"/> Antivirus instalado
	<input type="checkbox"/> Copia de seguridad reciente de mis datos
	<input type="checkbox"/> Sé identificar un correo o SMS de phishing
	<input type="checkbox"/> PIN/huella activados en el móvil y la tablet
	<input type="checkbox"/> PIN de verificación en dos pasos activado en WhatsApp
	<input type="checkbox"/> Privacidad revisada en las redes sociales
	<input type="checkbox"/> Sé cómo verificar si una tienda en línea es segura
	<input type="checkbox"/> Contraseñas de fábrica cambiadas en los dispositivos inteligentes de casa
	<input type="checkbox"/> He comprobado mi correo en haveibeenpwned.com
	<input type="checkbox"/> Alertas de movimientos bancarios activadas

 **¿Has sido víctima de un ataque? ¿Tienes dudas?**

Denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado. También puedes consultar el INCIBE (Instituto Nacional de Ciberseguridad) en incibe.es o llamar al 017, la línea de ayuda en ciberseguridad. ¡Es gratuita y confidencial!

Recuerda: la ciberseguridad no es cosa de informáticos. Es cosa de todos.