



Centro Nacional de Inteligencia
Avda. Padre Huidobro, 14
28023 MADRID
620 10 43 58
913725419
usedi@cni.es



COMUNICACIÓN CON BARRERAS

- Ten especial cuidado con los **enlaces web** que recibas, pueden albergar **código dañino** e infectar y comprometer nuestro dispositivo móvil.
- Aplica el **sentido común**, fíjate en cualquier síntoma o patrón fuera de lo considerado normal (urgencia, redacción errónea, otros idiomas...)
- **Elimina las previsualizaciones** de mensajes de aplicaciones como WhatsApp.
- Cuando navegues, verifica que la **conexión es segura** (el navegador mostrará un candado y/o el prefijo "https" en la barra de dirección).
- No aceptes un **mensaje de error del navegador** web asociado a un certificado digital inválido. Cancela la conexión.



DIME CON QUIÉN TE CONECTAS Y...

- **Desactiva conectividades** (Wi-fi, Bluetooth, NFC...) y servicios adicionales (GPS, sincronización con la nube...) **cuando no los utilices**. Aumentan la superficie de ataque sobre el dispositivo.
- No conectes el dispositivo móvil a **redes Wi-Fi públicas abiertas** (o hotspots Wi-Fi) que no implementan ningún tipo de seguridad. Si no tienes otra opción, **usa un servicio de VPN** (Virtual Private Network, o red privada virtual) para cifrar todo el tráfico transmitido a través de la red Wi-Fi.
- **Deshabilita el uso de redes 2G**. No utilizan mecanismos de seguridad.

¿ES APPsolutamente NECESARIO?

- No otorgues **permisos innecesarios** o excesivos a las apps.
- **Limita los datos** y la funcionalidad a la que éstas tendrán acceso: cámara, micrófono, ubicación...
- Mantén **actualizadas** las aplicaciones que usas habitualmente y **desinstala** cualquier aplicación que no utilices o no sea necesaria.
- No confíes en **aplicaciones descargadas en foros o redes sociales**.

DISPOSITIVOS MÓVILES

Los teléfonos inteligentes

Son dispositivos que están permanentemente conectados y expuestos a internet y con ellos, la información que contienen: tus contactos, cuentas de correo, tus mensajes y conversaciones, los sitios web que visitas, las compras que realizas o recibes, las aplicaciones que utilizas o tus cuentas bancarias...

Actualizaciones

Mantén el **terminal a punto**, descarga las actualizaciones recomendadas por el fabricante. Del mismo modo, actualiza las aplicaciones que usas habitualmente.

Evita pérdida de los datos

Evita la pérdida de los datos, realiza copias de seguridad periódicas, conserva, preferiblemente de forma local a través de USB con tu ordenador personal.

Autenticación de doble factor

Activa la autenticación de doble factor (2FA) en todas tus cuentas.

Bloqueado

Mantén el **teléfono bloqueado** (pantalla y acceso al dispositivo). Configura un PIN robusto (6-8 dígitos) o el acceso mediante huella dactilar.

Dispositivo Cifrado

Si almacenas información sensible para tu vida personal, o tu trabajo, cifra el dispositivo.

Puertos USB

No conectes el teléfono a puertos USB desconocidos (aeropuertos, servicios públicos...) o de confianza.

Informa

Si has observado alguna conducta extraña, comunícalo. El CNI está para ayudarte (usedi@cni.es)

