



Castilla-La Mancha

Píldoras Formativas de Ciberseguridad

Consejos para protegerse mientras viajamos

Agosto 2026



Los ciberdelincuentes no descansan y somos especialmente vulnerables cuando nos encontramos de viaje, por esta razón debemos continuar alerta ante posibles riesgos y seguir estas recomendaciones:

Cuidado con el Juice Jacking.

¿Necesitas cargar el móvil en un aeropuerto, estación o centro comercial? Algunos puntos de carga USB públicos pueden ser manipulados para extraer información de tu dispositivo o instalar software malicioso.

Recomendaciones:

- Utiliza tu propio cargador y enchufe siempre que sea posible.
- Lleva una batería externa (power bank).
- Si debes usar un puerto USB público, utiliza un bloqueador de datos ("USB data blocker").

Shoulder Surfing: miradas indiscretas

En aviones, trenes, cafeterías o salas de espera, alguien podría observar tu pantalla o el teclado cuando introduces credenciales, accedes al correo o realizas operaciones sensibles.

Recomendaciones:

- Evita introducir contraseñas en espacios muy concurridos.
- Utiliza filtros de privacidad para la pantalla.
- Bloquea la pantalla cuando no estés usando el dispositivo.
- Activa métodos de autenticación biométrica.

Evil Twin: WiFi falsas imitando a legítimas

Los ciberdelincuentes pueden crear puntos de acceso WiFi con nombres muy similares a los de un hotel, aeropuerto o cafetería (por ejemplo, Hotel_Wifi_Free).

Cuando el usuario se conecta, todo el tráfico puede pasar por la infraestructura controlada por el atacante.

Recomendaciones:

- Verifica el nombre exacto de la red con el establecimiento.
- Evita introducir credenciales o datos sensibles sin VPN.
- Desconfía de los portales cautivos que solicitan información excesiva.

Utiliza una VPN en redes WiFi públicas

Las redes WiFi gratuitas de hoteles, aeropuertos o cafeterías pueden no ser seguras. Un atacante podría intentar interceptar información transmitida a través de la red.

Recomendaciones:

- Conéctate únicamente a redes WiFi legítimas.
- Utiliza una VPN corporativa o de confianza.
- Evita acceder a aplicaciones críticas o realizar operaciones sensibles si no es imprescindible.
- Mantén desactivada la conexión automática a redes WiFi.

Códigos QR fraudulentos (Quishing)

Los QR están presentes en restaurantes, hoteles, aparcamientos, medios de transporte y puntos turísticos. Los atacantes pueden sustituir un QR legítimo por otro que dirija a una web fraudulenta diseñada para robar credenciales o datos bancarios.

Recomendaciones:

- Verifica la URL antes de acceder.
- Desconfía si solicita credenciales corporativas o información financiera.
- Utiliza aplicaciones que muestren el destino antes de abrir el enlace.

