Caso Práctico 3

1. Cinco permisos sospechosos y por qué lo serían

1. Acceso a los contactos: Si la app solo sirve para descuentos o reservas, no debería necesitar ver mi lista de contactos. Podría estar recopilando datos personales para fines no legítimos.

2. Acceso al micrófono: No es coherente con la funcionalidad anunciada. Este permiso podría usarse para escuchar conversaciones sin consentimiento.

3. Permiso para enviar SMS: Muy peligroso, ya que puede usarse para enviar mensajes sin autorización, suscribirme a servicios premium o robar códigos de verificación.

4. Acceso al almacenamiento completo: Si solo debería mostrar ofertas, no necesita acceder a todos mis archivos. Podría extraer fotos, documentos o información sensible.

5. Permiso para modificar la configuración del sistema: Un riesgo grave, ya que podría cambiar ajustes de seguridad, conectividad o instalar más malware.

2. Cuatro formas de protegerse ante posibles QRs maliciosos

1. Utilizar un lector de QR que muestre la URL antes de abrirla: Esto permite ver si el enlace dirige a un sitio legítimo o sospechoso, evitando redirecciones ocultas o peligrosas.

2. Verificar que el QR provenga de una fuente confiable: Si el QR está en un cartel impreso y no dentro de un canal oficial (como una web verificada o app oficial), es mejor desconfiar.

3. Evitar instalar apps fuera de Google Play o Apple Store: Las tiendas oficiales tienen controles de seguridad. Si el QR lleva a una APK externa, hay más riesgo de malware.

4. Comprobar los permisos antes de instalar una app: Revisar si los permisos solicitados se corresponden con la función esperada. Si algo no cuadra, no instalarla.

Bibliografía

Agencia Española de Protección de Datos. (2022). Riesgos de seguridad derivados del uso de códigos QR. https://www.aepd.es/es/documento/guia-qr.pdf

ENISA – Agencia de la Unión Europea para la Ciberseguridad. (2021). Threat Landscape for Mobile Devices.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-mobile-devices

OWASP Foundation. (n.d.). Mobile Security Testing Guide.
https://owasp.org/www-project-mobile-security-testing-guide/