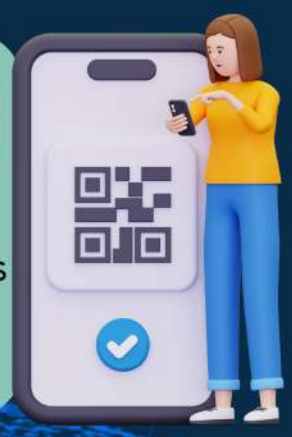
ESTAFAS POR QR

GIC (Gestión e Investigación en Ciberseguridad)
Lines - UTN La Plata

01 VERIFICA LA AUTENTICIDAD DEL QR

Antes de escanear un código QR, asegúrate de que proviene de una fuente confiable. Los estafadores pueden crear códigos QR falsos que parecen legítimos, pero que en realidad te llevan a sitios web maliciosos o te piden información personal.



02 NO ESCANEES CÓDIGOS QR DESCONOCIDOS

No escanees códigos QR que encuentres en lugares públicos, como en la calle, a menos que estés seguro de que son legítimos. Los estafadores pueden colocar códigos QR falsos en lugares públicos para atraer a víctimas.

03 NO PROPORCIONES INFORMACIÓN PERSONAL

Nunca proporciones información personal, como números de tarjeta de crédito o contraseñas, después de escanear un código QR. Los estafadores pueden utilizar esta información para robar tu identidad o realizar compras no autorizadas.

04 UTILIZA UNA APLICACIÓN DE ESCANEO DE QR SEGURA

Utiliza una aplicación de escaneo de QR que tenga buenas reseñas y que esté diseñada para detectar códigos QR maliciosos. Algunas aplicaciones de escaneo de QR pueden alertarte si un código QR parece sospechoso.

05 REVISA LA URL ANTES DE ACCEDER

Antes de acceder a un sitio web después de escanear un código QR, revisa la URL para asegurarte de que sea legítima. Los estafadores pueden crear sitios web que parecen legítimos, pero que en realidad son falsos y están diseñados para robar tu información personal.

Quishing: utiliza un mensaje de texto o correo electrónico que incluye un enlace o un número de teléfono.
Qphishing: utiliza un código QR que dirige al destinatario a un sitio web malicioso o a una aplicación.
QRhishing: combina el phishing con el uso de códigos QR, enviando un mensaje de texto o correo electrónico que incluye un código QR que el destinatario debe escanear.