Phishing

Es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Existen varias técnicas para hacer que las personas caigan en este tipo de ataques, pero el más común es el phishing. Las victimas reciben un mensaje de correo electrónico o un mensaje de texto que imita ser una persona u organización de confianza. Cuando la víctima abre el correo electrónico o el mensaje de texto se va a encontrar un mensaje que lo puede llegar asustar. Normalmente el mensaje exige que la víctima vaya a un sitio web y actúe de inmediato a un tendrá que afrontar las consecuencias.

Tipos de phishing

- **Whaling**: Este modo se phishing se centra en atacar específicamente a altos ejecutivos y directivos de empresas, buscando obtener acceso a información valiosa o realizar fraudes de alto nivel.
- **Smishing**: Es realizado a través de mensajes SMS (mensajes de texto). Suelen incluir enlaces maliciosos o solicitar información personal a través de mensajes de texto.
- **Pharming**: Es la técnica de phishing más sofisticada ya que el atacante manipula el sistema DNS para redirigir a los usuarios a sitios web falsos, incluso si escriben la dirección web correcta en su navegador.
- **SIM Swapphig**: Es una de las variantes más modernas. Consiste en el duplicado de la tarjeta SIM de alguien para suplantar su identidad y acceder así a sus credenciales del banco.
- **Spear phishing**: Se ejecuta normalmente el envío de un email o mensajes de redes sociales, es una forma de phishing altamente dirigido y personalizado a individuos o empresas.
- **Vishing**: Se realiza por medio de llamadas telefónicas falsas.
- **QRshing**: Busca adaptarse a las tendencias actuales, en este caso simulando ser un código QR de una supuesta marca o comercio pero que enlaza a un sitio web fraudulento.