Phishing

Phishing is the crime of tricking people into sharing confidential information such as passwords and credit card numbers. There are several techniques to trick people into falling for these types of attacks, but the most common is phishing. Victims receive an email or text message that imitates being a trusted person or organization. When the victim opens the email or text message, they will find a message that can scare them. Normally, the message demands that the victim go to a website and act immediately or they will have to face the consequences.

Types of phishing

- Whaling: This type of phishing focuses on specifically attacking senior executives and company managers, seeking to gain access to valuable information or commit high-level fraud.
- Smishing: It is done through SMS messages (text messages). They usually include malicious links or request personal information through text messages.
- Pharming: This is the most sophisticated phishing technique, as the attacker manipulates the DNS system to redirect users to fake websites, even if they type the correct web address into their browser.
- SIM Swapphig: This is one of the most modern variants. It consists of duplicating someone's SIM card to impersonate them and thus access their bank credentials.
- Spear phishing: This is usually carried out by sending an email or social media message, and is a highly targeted and personalized form of phishing to individuals or companies.
- Vishing: This is done through fake phone calls.
- QRshing: This seeks to adapt to current trends, in this case simulating a QR code from a supposed brand or business but which links to a fraudulent website.