केनरा बैंक Canara Bank
सिंडिकेट Syndicate

SOCIAL ENGINEERING ATTACKS

TARGET THE WEAKEST LINK IN SECURITY: HUMAN ASSETS

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. Using phone calls and other media, these attackers trick people into giving away to sensitive information which is used for stealing money or performing malicious activities.

Common Types of Social Engineering Attacks

PHISHING ATTACKS

Phishing is the most common form of social engineering attack that is typically in the form of an email, chat, web ad or website that has been designed to impersonate a real system, person, or organisation.

Phishing messages are designed to deliver a sense of urgency or fear with the end goal of capturing an end user's sensitive data.

BAITING ATTACKS

Baiting is very similar to phishing. It involves offering something captivating to an end user, in exchange for login information or private data.

It may be in the form of a movie download or gift coupon, which once accessed or downloaded, malware gets delivered to user's device and hackers get access to the device.

QUID PRO QUO

Similar to baiting, quid pro quo involves a hacker requesting the exchange of critical data or login credentials in exchange for a service.
For example, an end user might receive a phone call from the hacker who, posed as a technology expert, offers free IT assistance. The most recent ones are scams claiming to update your expired KYC with a Bank or office via fake apps which steal your financial data

PRETEXTING ATTACKS

Hacker creates a false sense of trust between themselves and the end user by impersonating a co-worker or manager.
An example of this type of scam is an email to an employee from what appears to be from Manager or CEO. Also other examples are creating fake ID of your friend in social media and requesting for urgent fund expecting you to send them money.

Best Practices to protect yourself from Social Engineering Attacks

- Never respond to a request for financial information or passwords. Legitimate organisations will never send a message asking for personal information.
- Never follow unknown links present in emails/SMS/ chat messages, etc. or download attachment within.
- Protect your digital space with anti-virus software, firewalls, and email filters.
- Always be alert and never share OTP, CVV number, Credit/ Debit Card details, PIN number, etc to strangers.
- Do not download applications in your device from untrusted software.

INFORMATION SECURITY SECTION, RISK MANAGEMENT WING