Social engineering is a manipulation technique used by cybercriminals to trick people into giving up confidential information or performing certain actions that may compromise security. Instead of hacking systems or using software vulnerabilities, attackers exploit human psychology to gain access to sensitive data such as passwords, bank details, or personal information.

Some common social engineering tactics include:

1. **Phishing**: Sending emails or messages that appear to be from a legitimate source (e.g., a bank or employer) to deceive individuals into sharing sensitive information.
2. **Pretexting**: Creating a fabricated scenario to obtain sensitive information. For example, pretending to be a company representative or authority figure to gain trust.
3. **Baiting**: Luring victims with promises of something enticing (like free software, gifts, or movie downloads) to get them to click on malicious links or hand over personal details.
4. **Tailgating**: Physically following someone into a secure area without proper credentials or permission, often by exploiting common courtesies like holding the door open for someone.
5. **Impersonation**: Pretending to be someone else to gain access to restricted information or systems, often by mimicking authority figures or trusted individuals.

The goal of social engineering is to bypass security measures by exploiting human vulnerabilities, making it a dangerous and effective tool for cybercriminals.

1. Twitter Bitcoin Scam (2020)

In July 2020, a major social engineering attack targeted high-profile Twitter accounts, including those of Elon Musk, Bill Gates, and Barack Obama. Hackers gained access to internal Twitter tools by convincing employees to hand over credentials through a phone phishing attack. They then posted fraudulent tweets

offering to double any Bitcoin sent to a specific wallet. Many people fell victim to this scam, sending thousands of dollars to the attackers.

2. Target Data Breach (2013)

The 2013 Target breach, which exposed the personal and financial information of millions of customers, involved social engineering. Attackers gained access to Target's systems by tricking a third-party vendor into clicking on a malicious email link. Once the vendor's network was compromised, the attackers used those credentials to infiltrate Target's payment systems.

3. Ubiquiti Networks Scam (2015)

In 2015, Ubiquiti Networks, a networking technology company, fell victim to a Business Email Compromise (BEC) scam. Fraudsters impersonated company executives and convinced employees to transfer over $46 million to overseas accounts. The attackers used email spoofing techniques and posed as higher-level executives to create urgency and pressure the employees into making the transfers.

4. Robinhood Customer Service Scam (2021)

In November 2021, Robinhood, the stock trading platform, experienced a data breach where attackers used social engineering tactics to trick a customer support employee into giving them access to internal systems. The hackers were able to obtain sensitive information, including the names and email addresses of about 7 million customers. Although the incident didn't compromise financial data, the stolen personal information could be used for future scams.

5. Google and Facebook Fraud (2013-2015)

From 2013 to 2015, cybercriminals successfully scammed both Google and Facebook out of $100 million by using social engineering tactics. The fraudsters impersonated a supplier, sending fake invoices to the companies for products that were never delivered. They used phishing emails and fake identities to convince accounting departments to process payments to overseas bank accounts.

These examples demonstrate how attackers can use social engineering to manipulate individuals and exploit companies by preying on trust, urgency, and fear. Such attacks can have significant financial and reputational consequences.