BBVA

Creating Opportunities

Resource guide

Social engineering: What is it and how can you protect yourself

The definition of social engineering

When used in reference to cybercrime, social engineering is the act of deceiving or manipulating someone into providing personal information.

Common types of social engineering

***Phishing*:** Deceptive emails, websites, chat or text messages designed to trick people into giving out personal information or infect their computer with malware.

***Spear phishing*:** While regular phishing emails are typically sent to a mass audience, spear phishing targets an individual or specific group.

***Vishing** and **smishing*:** These are phishing attacks via voice call (vishing) and SMS texts (smishing).

***Scareware*:** Communications that misled the victim into believing their computer is infected, then offer to remove the bad software for a fee.

***Baiting*:** Emails, texts, chats and web ads that offer a prize or reward for clicking a link or download an attachment. Baiting can be used to get the victim to provide information or infect their computer with malware.

***Quid Pro Quo*:** Like baiting, these communications request information in exchange for a service or benefit.

***Pretexting*:** With pretexting, the hacker posed as an authority figure, such as a police officer or investigator. If the victim responds, the hacker will then make some kind of request for information.

How to protect yourself from social engineering schemes

Aggressively protect your personal information. Always be overly cautious when it comes to sharing your personal or financial information.

Be suspicious of all electronic communications requesting information or asking you to perform a task.

Keep your software updated. Many software updates include security upgrades, so it's wise to install the updates when they are available.