



Avoid Becoming a Social Engineering Victim

Four Questions to Ask Yourself

Social engineering is a scam where a cybercriminal attempts to trick someone into taking an action against their own best interests. Usually, the action results in the victim providing confidential information (like their login information) or installing malware on their computer.

Most social engineering attacks have four common traits, which signal a far higher likelihood of a scam if all are present. Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, advises asking yourself these four questions to help you avoid becoming a victim.



If you answer yes to all of them, you should go out of your way to confirm the request is legitimate. Use a trusted method like calling or texting the sender before taking any action.

Not every message with these four traits is absolutely a social engineering scam. Our email inboxes, voicemail and postal mailboxes are full of unexpected requests; that is life. But when these four traits are present, **stop, look, and think** before you act!