Cybercrime’s science of deception

Description

Social engineering is the practice of influencing people into making mistakes. It’s the calculated science of deception and psychological manipulation – and cybercriminals are exploiting it.

Cybercriminals are using our cognitive biases – the mental shortcuts our brains use to quickly make decisions and judgments – to gain the upper hand.

Here are just a few of the tricks they use that we must be more aware of:

Authority bias: People tend to comply with requests from authority figures. Social engineers impersonate managers or anyone who might have legitimate reasons for requesting information or access.

Scarcity bias: “For a limited time only” is a common sales technique. A fear of missing out creates a sense of urgency, just like social engineers often do via phishing attacks and other scams.

Reciprocity bias: People often feel obligated to return favours. Attackers can leverage this by offering to help someone with a (non-existent) technical problem, thereby getting their target to reveal a password.

Turn the tables on cognitive bias

Slow down: Social engineers love catching people when they’re too busy to think clearly – hasty decisions can be costly.

Don’t assume: Impersonation is one of the key tactics of attackers. Never assume someone is who they claim to be.

Verify: If you encounter an unusual request, reach out directly to a trusted source (such as a manager) to verify its legitimacy.

Think critically: Social engineers want to gain your trust and use your emotions against you. Use critical thinking before reacting.

Category

1. Our Knowledge Centre