INSIDE THE ATTACKER'S MIND

How social engineering exploits trust, emotion, and human psychology

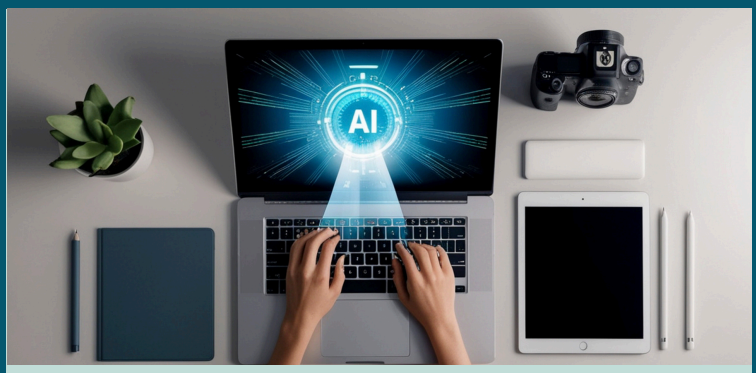
THIS MONTH'S TOPICS:

Cybercriminals don't just exploit systems. They exploit people. Social engineering attacks rely on manipulating human behavior, using trust, fear, urgency, and curiosity to bypass even the strongest technical defenses. And unfortunately, these attacks often work.

In this month's newsletter, we explore real-world social engineering incidents, examine how emotional manipulation fuels cyber attacks, and break down the psychological techniques attackers use to influence decision-making. Understanding why these attacks succeed is the first step toward recognizing and stopping them.

REAL WORLD SOCIAL ENGINEERING SCAMS AND THEIR IMPACT

Social engineering attacks are successful because they target human behavior. Instead of breaking into systems, attackers trick people into opening the door for them. From phishing emails to impersonation scams, real-world incidents consistently show that emotional manipulation and trust are often the weakest link in security.



In 2026, security researchers reported that attackers used deepfake technology to impersonate CEOs and executives during spoofed video calls. The fake executives instructed employees to run malicious troubleshooting software, which then infected internal systems with backdoors and credential-stealing malware. This attack blends social engineering with advanced AI to create realistic but fraudulent scenarios that trick even trained professionals.

In late 2025, the Noosa Council in Australia lost about $1.9 million in a business email compromise (BEC) scam. Attackers used a socially engineered email to trick employees into approving fraudulent transactions. Law enforcement noted that AI-driven social engineering tactics played a role in the deception. Even large organizations with formal procedures can be targeted by sophisticated email scams — financial transactions should require multiple layers of verification before approval.

One of the most famous social engineering cases involved Evaldas Rimasauskas, who used spear-phishing emails to impersonate vendors and trick companies into paying fraudulent invoices. Major tech companies lost millions between 2013 and 2015 before the scam was uncovered.

EMOTIONAL MANIPULATION AND CYBER ATTACKS

COMMON EMOTIONAL TRIGGERS

ATTACKERS DELIBERATELY CREATE SITUATIONS THAT...

PUSH YOU TO ACT ASAP

Attackers create artificial deadlines to pressure quick decisions.

MAKE YOU FEEL AFRAID

Messages that warn of account suspension, financial penalties, data loss, legal trouble, or security breaches are crafted to create panic.

ENCOURAGE YOU TO COOPERATE

Most employees want to be responsive and supportive, especially toward coworkers, leadership, or customers.

APPEAL TO AUTHORITY

People are conditioned to respect authority and follow instructions from leadership, IT staff, financial institutions, or well-known brands.

SPARK CURIOSITY

Messages about bonuses, refunds, confidential documents, or exclusive information tempt recipients to click before thinking.

SOCIAL ENGINEERING ATTACKS DON'T SUCCEED BECAUSE PEOPLE ARE CARELESS — THEY SUCCEED BECAUSE ATTACKERS ARE SKILLED AT MANIPULATING EMOTION.

SCAM OF THE MONTH: TECH SUPPORT SCAMS

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

It started with a pop-up that froze Jenna's screen, warning her of a critical security threat and urging her to call "Microsoft Support" immediately. Alarmed by the message and worried about potential damage to her system—or her company's network—she called the number. The person who answered sounded professional and calm, insisting that immediate action was necessary to stop an active attack.

He guided Jenna through installing a so-called security tool to fix the problem remotely. Instead of removing a virus, the software gave him full access to her computer, allowing him to install malicious programs and demand payment for "emergency services." By the time Jenna realized something wasn't right, the warning was gone—but the damage was already done.

DID YOU SPOT THE RED FLAGS?

- Legitimate tech companies don't use alarming pop-ups that freeze your screen and pressure you to call a phone number right away.
- Unsolicited requests to install tools that allow someone to remotely control your computer are a major warning sign.

HOW TO PROTECT YOURSELF

- If you see a pop-up, email, or phone call claiming there's an urgent tech issue, stop and verify it independently.
- Only allow screen sharing or remote tools when you personally contacted a verified support team and know exactly who you're working with.

PSYCHOLOGY TACTICS

TACTICS BEHIND SOCIAL ENGINEERING

01 Authority

People are more likely to comply with requests from someone they perceive as powerful or knowledgeable. We're conditioned to follow instructions from authority figures without resistance.

02 Scarcity & Urgency

When something feels limited or time-sensitive, we feel pressure to act quickly. Attackers use deadlines, expiring links, or "last chance" language to reduce critical thinking time and create fear/anxiety.

03 Social Proof

People tend to follow the behavior of others, especially in uncertain situations. Attackers may claim that "other employees have already completed this" or reference familiar names to make requests seem normal.

04 Reciprocity

When someone does something for us —or appears helpful—we feel a natural urge to return the favor. Attackers may begin with small, harmless requests before escalating to larger ones.

05 Commitment & Consistency

Once someone agrees to a small request, they're more likely to agree to larger follow-ups to remain consistent with their earlier actions. People want to appear consistent and reliable.

06 Cognitive Overload

Sometimes attackers simply overwhelm their target with information, technical jargon, or multitasking pressure. When the brain is overloaded, people rely on shortcuts instead of analysis. Mental fatigue reduces skepticism.

These techniques aren't new—they're the same principles used in sales, marketing, and persuasion. What makes them dangerous in cybersecurity is intent. Social engineers combine emotional triggers with psychological influence to create situations where reacting feels easier than verifying.