Social engineering

Social engineering is a trick used by hackers to fool people into giving away important information, like passwords or bank details. Instead of hacking computers directly, they "hack" people by pretending to be someone they trust—like a friend, boss, or company.

They might send fake emails, call you pretending to be tech support, or even try to sneak into a building by following someone inside. The goal is to make you do something that helps them, like clicking a bad link or sharing private info.

Social engineering is dangerous because it targets people, not just computers—so it's important to stay alert and think before you click or share anything.

Phishing

Phishing is a type of social engineering attack where an attacker pretends to be a trustworthy entity to trick victims into revealing sensitive information such as usernames, passwords, credit card numbers, or installing malware**.**

List of **14 types** of phishing attacks:

- Basic (Email, Spear, Whaling)
- Mobile (Smishing, Vishing)
- Technical (Pharming, MitM)
- Social/Platform-specific (Clone, Angler, Social Media, Calendar, BEC)
- Trick-based (SEO, Cloud document spoofing)

1. **Email Phishing**
    - The most widespread type. Victims receive emails that appear to be from legitimate sources (banks, companies, etc.) with fake links or attachments.
    - Example: "Your account is locked. Click here to reset your password."
2. **Spear Phishing**
    - Targeted phishing aimed at a specific individual or organization.
    - More personalized and harder to detect.
    - Often uses info from social media or previous data breaches.
3. **Whaling**
    - Aimed at high-profile targets like CEOs, CFOs, or other executives.

- Often involves urgent business-related requests like wire transfers or login credentials.

4. **Smishing (SMS Phishing)**
    - Delivered through SMS messages.
    - Example: “Your package is held. Click this link to verify your address.”
5. **Vishing (Voice Phishing)**
    - Involves phone calls.
    - Attacker pretends to be from tech support, a bank, or a government agency.
6. **Pharming**
    - Redirects users from legitimate websites to fake ones via DNS poisoning or malware, without user interaction.
7. **Clone Phishing**
    - An attacker creates a near-identical copy of a legitimate email previously sent to the victim, replacing links or attachments with malicious versions.
8. **Angler Phishing**
    - Happens on social media platforms where attackers impersonate customer support accounts to trick users into giving up personal info.
    -
    9. **Business Email Compromise (BEC)**
        - A form of spear phishing where attackers impersonate a company executive or trusted vendor to trick employees into sending money or sensitive info.
    10. **Man-in-the-Middle Phishing (MitM)**

    - Involves intercepting communication between the user and a website, often on public Wi-Fi, to steal login credentials in real-time.

    11. **Search Engine Phishing (SEO Poisoning)**

    - Attackers create fake websites with high-ranking search engine results to lure users searching for services like tech support, banking, etc.

    12. **Social Media Phishing**

    - Fake profiles or messages trick users into sharing personal info, clicking malicious links, or downloading infected files.

    13. **Calendar Phishing**

    - A newer tactic where attackers send fake calendar invites with malicious links or urgent meeting topics to trigger curiosity or fear.

    14. **Dropbox/Google Docs Phishing**

How AI is Used in Scams: Deepfakes, Phishing, and Social Engineering

Deepfakes: What They Are

- • AI-generated fake media: Deepfakes are fake images, videos, or audio created by AI. For example, AI can put one person's face on another body, or make a recording of someone saying words they never said. Deep learning models "learn" from lots of real pictures and sounds, then generate convincing fakes.
- • Training on data: To make a deepfake, AI needs many real photos or recordings of the person. The AI studies how that person looks and sounds, and then creates a new fake clip.
- • Can be very convincing: A good deepfake can fool your eyes and ears. You might see a video of a famous person talking, but it's actually AI-made. The face and voice match so well you might not notice it's fake.

Deepfakes are dangerous because they make lies look real. Imagine seeing a video of a political leader saying something shocking that they never actually said. People might believe it and panic. In scams, deepfakes can be used to trick victims. For example, criminals have cloned a CEO's voice to trick a company into sending money. Because deepfakes can copy anyone, they make it hard to trust audio or video.

Why Deepfakes Are Dangerous

- • Spreading misinformation: Fake videos can be used to spread rumors or false news.
- • Tricking victims: Scammers use deepfake videos or voices to pretend to be trusted people.
- • Emotional manipulation: Seeing and hearing someone real makes scams feel more urgent.

Because deepfakes look and sound real, they're hard to spot. Even experts say AI scams combine phishing techniques with social engineering, plus the power of AI.

AI in Phishing

- • Fake emails and websites: Phishing attacks are when scammers send fake emails or create fake websites to steal personal info.
- • AI writes better phishing emails: With AI, scammers can generate phishing emails quickly and in many languages.
- • Language and chat support: AI can translate phishing emails and answer in real time via chatbot.

- • Personalization: AI can scan social media and guess your interests or work.
- • Automation and scale: AI lets scammers send millions of emails easily.

Phishing is one of the most common online scams. AI just makes this trick bigger. For instance, phishers copy the behavior of legitimate sites and send fake links through spam.

AI in Social Engineering

- • Voice cloning: AI can create a fake voice that sounds exactly like someone.
- • Deepfake video calls: Attackers can do video calls with a deepfake image.
- • Fake online profiles: AI can generate realistic profile photos and details.
- • Information gathering: AI tools can scrape social media, news, and other sources.

Scammers can clone voices to call employees and pretend to be their boss, asking for urgent transfers or passwords.

Real-World Case Studies

- • Voice deepfake CEO (UK energy firm): Criminals used an AI voice clone of a German CEO to trick a UK energy company into wiring $243,000.
- • Deepfake CFO video call (Arup, 2023): British engineering firm Arup lost $25 million when scammers posed as their CFO in a video meeting.
- • Attempted scam on WPP (2024): Scammers used deepfake tech to impersonate WPP's CEO in a Teams meeting, but vigilant staff stopped it.
- • Many businesses targeted: Surveys show over half of businesses have been targeted by AI-powered deepfake scams.

These real cases prove that AI scams are not just theory. Even big companies need to be careful.

Staying Safe and Aware

- • Verify requests: Double-check weird emails or calls.
- • Look for red flags: Check email addresses and websites carefully.
- • Educate yourself: Learn about deepfakes and phishing.
- • Use tools and policies: Companies can use security tools to flag deepfake or spoofing attempts.
- • Stay skeptical: If something seems too strange or urgent, it might be a scam.

AI makes these scams tougher, but not impossible to beat. By staying alert and double-checking unexpected requests, people and businesses can avoid falling for AI tricks.

Case Studies

Global Case Study 1: UK Energy Company Deepfake Scam

- About: A UK-based energy firm (owned by a German parent company) was targeted in 2019.
- How it happened: Hackers used an AI voice-generating tool to clone the German parent CEO's voice and convinced the UK CEO to transfer funds.
- Loss: About ₹1.75 crore (US $243,000) was transferred before fraud was noticed.
- Prevention: Double-check such requests via a different communication channel (e.g., video call or direct call). Implement multi-factor authentication.
- Learnings: Always verify urgent money requests. Be aware of deepfake tech and train staff accordingly.

Global Case Study 2: WPP Deepfake Phishing Attempt

- About: WPP is the world's largest advertising and PR firm.
- How it happened: Fraudsters impersonated executives using AI video and voice in a fake Teams meeting.
- Loss: No financial loss, as vigilant staff caught the fraud.
- Prevention: Verify video meeting participants, especially during financial discussions.
- Learnings: AI deepfakes are realistic; training staff to detect fakes is essential.

Global Case Study 3: Arup Deepfake CFO Video Scam

- About: Arup is a British engineering company involved in major infrastructure projects.
- How it happened: A Hong Kong employee was tricked in a video call by AI-generated CFO.
- Loss: HK$200 million (~£20 million) was lost.
- Prevention: Use multi-layered fund transfer approvals and confirm identities by direct means.
- Learnings: Always verify financial requests, even if they seem to come from top executives.

India Case Study 1: Leading Bank AI-Driven Phishing Attack

- About: One of India's top banks was targeted in 2024.
- How it happened: Emails mimicking the CEO's style tricked execs into entering login details.
- Loss: Executive accounts were compromised; financial loss occurred but undisclosed.
- Prevention: Use AI email filters and mandatory multi-factor authentication.

- Learnings: Traditional methods don't stop AI-powered phishing. Staff training is vital.

India Case Study 2: Delhi Companies CEO Impersonation Scam

- About: Three Delhi firms faced WhatsApp impersonation scams.
- How it happened: Employees received urgent fund requests from fake MD WhatsApp accounts.
- Loss: Total loss was about ₹6.99 crore.
- Prevention: Call and verify requests via official numbers; require multi-level fund approvals.
- Learnings: Impersonation can happen on simple apps. Never act on financial requests without checks.

India Case Study 3: Bharti Executive AI Voice Clone Scam

- About: Bharti Enterprises executive in Dubai received fake voice call.
- How it happened: Scammers used AI to clone Sunil Mittal's voice.
- Loss: No loss; the employee caught the fraud.
- Prevention: Always verify voice calls that involve fund transfers.
- Learnings: Voice cloning is realistic; always double-check before acting on voice-only requests.

References

- • Abdul Basit et al., A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 2021.
- • Trend Micro (2019), Unusual CEO Fraud via Deepfake Audio Steals US$243,000 from UK Company.
- • Nick Robins-Early (2024), CEO of world's biggest ad firm targeted by deepfake scam. The Guardian.
- • Cybersecurity Dive (2024), Deepfake scams escalate, hitting more than half of businesses.
- • Mailgun Blog (2025), The golden age of scammers: AI-powered phishing.