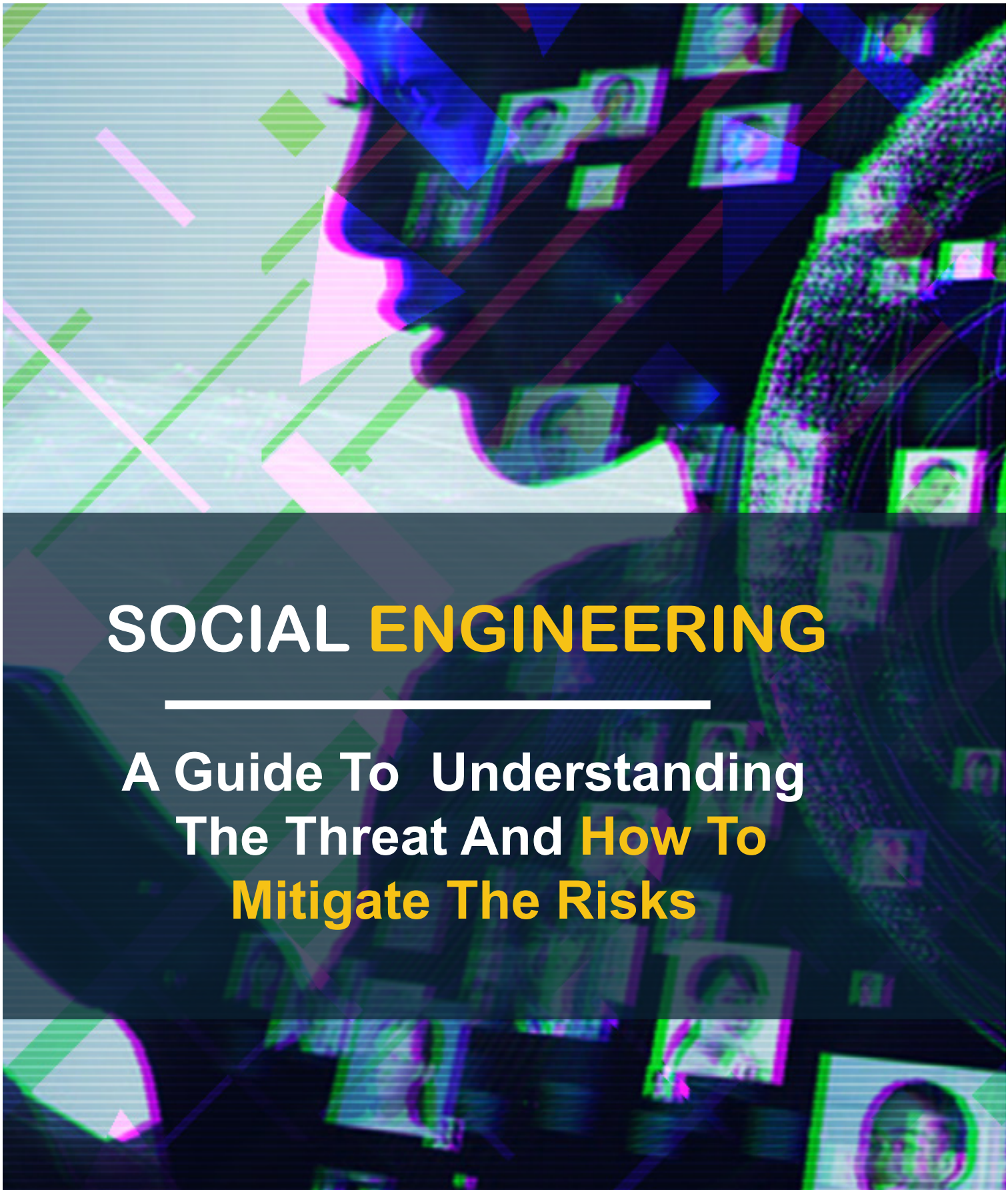
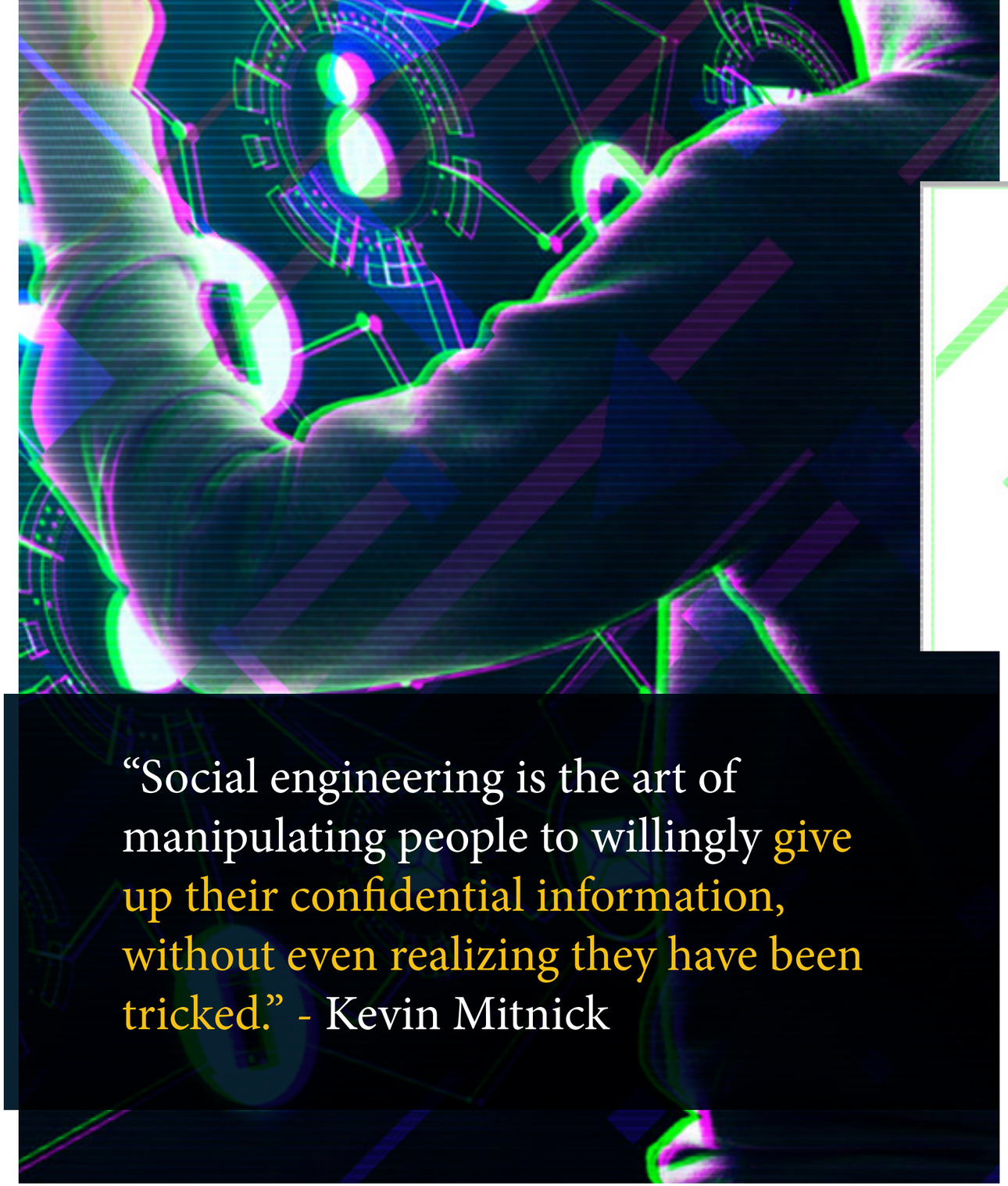


SOCIAL ENGINEERING

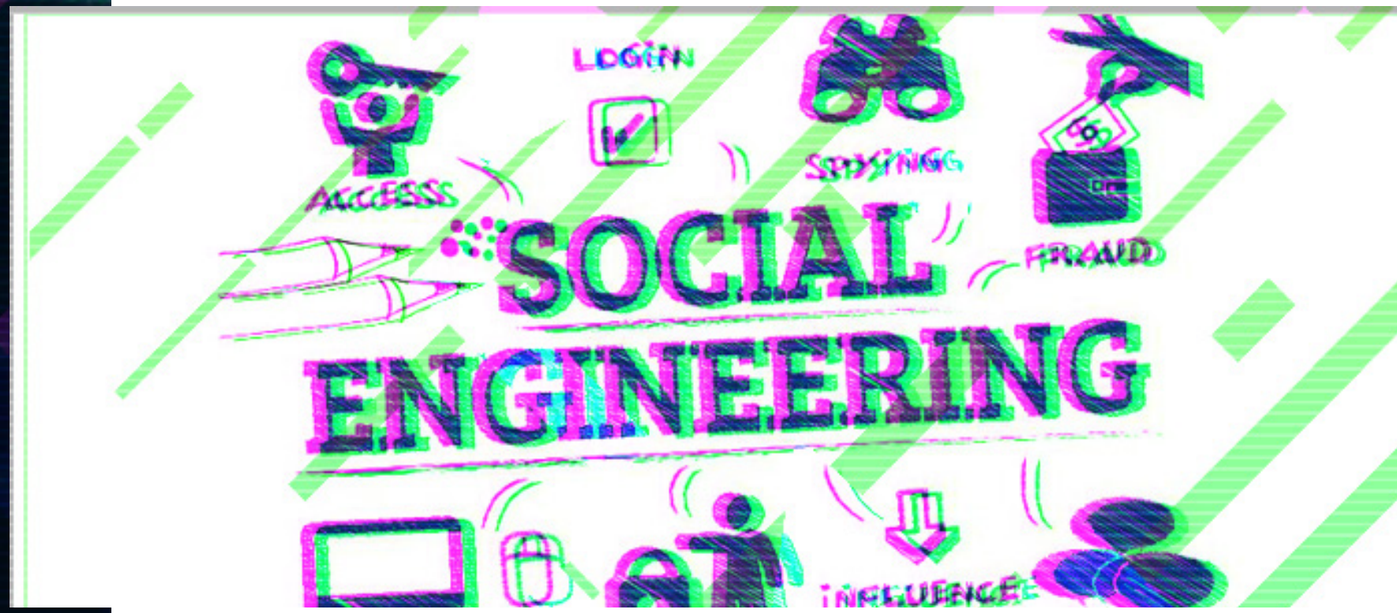
A Guide To Understanding The Threat And How To Mitigate The Risks



“Social engineering is the art of manipulating people to willingly give up their confidential information, without even realizing they have been tricked.” - Kevin Mitnick

SOCIAL ENGINEERING

INTRODUCTION



The landscape of cybersecurity threats is constantly evolving, moving far beyond traditional methods like hacking and malware distribution. Today, social engineering has emerged as one of the most effective and deceptive forms of attack, relying on manipulation and psychological tactics rather than technical exploits.

While modern IT systems are increasingly resilient to direct intrusion, cybercriminals often bypass these defences by tricking people into opening the door for them—sometimes quite literally. In this guide, we’ll explore how social engineering attacks work, the techniques most commonly used by attackers, and the practical steps you and your team can take to stay protected against these fast-evolving threats.

SOCIAL ENGINEERING DEFINED

Social engineering is the act of manipulating individuals into divulging confidential information or performing actions that compromise their security. Cyber-criminals accomplish this by exploiting human psychology, making this type of attack particularly challenging to detect.

THE HUMAN FACTOR IN CYBER SECURITY

When it comes to cyber security, human error or negligence can often lead to security breaches, making humans the weakest link in the security chain. Social engineering specifically targets this vulnerability by exploiting trust and human nature.

COMMON GOALS OF SOCIAL ENGINEERING

The goals of social engineering attacks can range from gaining unauthorised access to sensitive information, stealing credentials, spreading malware, or conducting fraud or identity theft, making this a versatile tool for cyber-criminals. The overall goal of the criminal is to manipulate you into taking an action that leads to a compromise.

98% of cyberattacks involve some form of social engineering.

68% of breaches in 2024 involved a human element, with social engineering exploiting human vulnerabilities to gain access to information.

82% of Data Breaches Involve the “Human Element”

90% of Cyber Attacks Are Targeting Your Employees Instead of Your Tech

Phishing continues to be the most common type of social engineering attack, accounting for approximately 60% of all incidents in 2023.

SOCIAL ENGINEERING

COMMON VECTORS

Social engineering attacks take many forms, but they all share a common goal: to manipulate people into compromising security, often without even realising it. Below are the most common vectors used in modern social engineering attacks, including new and evolving threats that exploit human psychology, digital habits, and even emerging technologies.

PHISHING

Phishing remains one of the most common social engineering techniques. Attackers send fraudulent emails or messages designed to trick recipients into clicking malicious links, downloading malware, or sharing sensitive information. These messages often imitate trusted brands or individuals.

Example: "Your Microsoft 365 account has been suspended – click here to restore access."

SPEAR PHISHING AND WHALING

More targeted than regular phishing, spear phishing uses information gathered from social media, public records, or previous breaches to personalise attacks. Whaling targets senior executives or high-level decision-makers, often impersonating internal stakeholders or legal authorities.

Example: A fake invoice request sent to the CFO appearing to come from the CEO.

PRETEXTING

In pretexting, attackers create a fabricated scenario to manipulate the victim. This might involve impersonating a colleague, IT technician, or vendor to gain trust and access.

Example: A caller claiming to be from the helpdesk requesting a password reset for "urgent system maintenance."

BAITING

This involves luring the target with an enticing offer – free downloads, music, or even USB devices left in public areas – which deliver malware once interacted with.

Modern variant: Cloud-based file-sharing bait (e.g., fake "shared document" links via Google Drive or OneDrive).

QUID PRO QUO

The attacker offers a service or help in exchange for information or access. For example, posing as technical support offering help to fix a fake issue, while installing remote access software.

TAILGATING

Tailgating, also known as piggybacking, is a physical form of social engineering where a person seeks to gain unauthorised access to a restricted area by following an authorised person.

VISHING (Voice Phishing)

This phone-based attack involves impersonating trusted entities—such as banks, suppliers, or IT departments—to extract information. These calls often leverage caller ID spoofing to appear legitimate.

Example: "This is your bank's fraud team. Can you verify your recent transaction by confirming your PIN?"

SOCIAL ENGINEERING
ADVANCED TECHNIQUES & TACTICS

EMOTIONAL MANIPULATION

Social engineers may manipulate their targets emotionally by using fear, sympathy, or greed, making them more susceptible to their schemes. This type of attack is particularly successful as it adds a level of urgency that is more likely compel the victim to take an action that may lead to a compromise.

Example: A message from a "family member" stuck abroad asking for an urgent money transfer.

DEEPFAKE IMPERSONATION

Attackers are now using AI-generated deepfake audio or video to convincingly impersonate senior staff. This is particularly dangerous for approving high-value transactions or sensitive data requests.

Example: A realistic voicemail from a CEO asking for an urgent wire transfer.

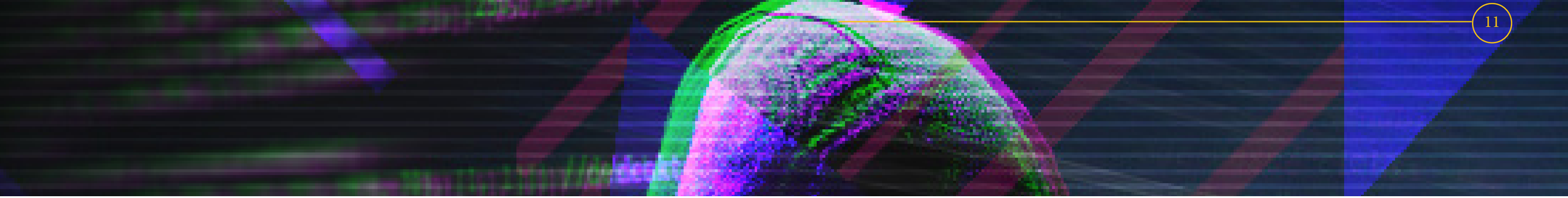
HIRD-PARTY AND SUPPLY CHAIN EXPLOITATION

Increasingly, attackers target less secure third-party suppliers as a way into larger organisations. They impersonate vendors, partners, or service providers to gain system access or credentials.

Real-world case: In 2024, Scattered Spider used social engineering to breach Marks & Spencer's internal systems via a compromised third-party supplier.

"Social engineering is not just a tactic, it is a mindset. It requires creativity, empathy, and an understanding of human behaviour to successfully manipulate people." -

Christopher Hadnagy



SOCIAL ENGINEERING

RECOGNISING THE RED FLAGS

Cybercriminals rely on subtlety and familiarity to trick victims into taking action. Learning to spot the red flags is essential for stopping social engineering attacks before they succeed.

Suspicious Emails and Messages

Look out for:

- Unexpected attachments or links
- Spelling mistakes or poor grammar
- Generic greetings like “Dear Customer”
- Urgent or threatening language
- Mismatched or spoofed email addresses and URLs

Tip: Hover over links to preview the real destination—if it looks off, don’t click.

Unusual Requests or Behaviour

Look out for:

- Requests that seem “off” or out of character
- Pressure to act quickly
- Demands for sensitive information or payments
- Messages claiming to be from executives or IT staff that bypass normal channels

Trust your instincts—if something feels wrong, it probably is.

Always Verify the Source

Never trust contact details provided in a suspicious message. Instead:

- Use official websites or internal directories to verify contact info
- Call the person directly if the message claims to be from someone you know
- Confirm requests through a separate communication channel

You won’t get in trouble for double-checking—security comes first.

Spotting Fake Websites

Cybercriminals create realistic-looking sites to steal credentials or infect devices. Key signs of a spoofed website include:

- Slight changes in the domain name (e.g., “paypaI.com” instead of “paypal.com”)
- Missing padlock icon or “HTTPS” in the URL
- Low-quality design, broken links, or odd branding
- Pop-ups asking for login details or personal info

When in doubt, don’t log in—go directly to the known site instead.

Social engineering attacks thrive on urgency, trust, and distraction. By taking a moment to pause, question, and verify, you can prevent a costly mistake. Cybersecurity isn’t just about firewalls and software—it’s about people making smart, informed decisions every day. Make vigilance part of your routine, and encourage your team to do the same. When in doubt, always check it out.

SOCIAL ENGINEERING

BEST PRACTICES FOR PREVENTION

Protecting your business from social engineering attacks starts with building a culture of security awareness and following proven preventative measures. Here's what you and your team should prioritise:

Educate and Train Continuously

Ongoing cyber awareness training is one of the most effective ways to reduce human error. Regular phishing simulations, role-based training, and scenario walkthroughs help staff recognise and respond to manipulation tactics before it's too late.

Training isn't a one-off—it should be part of your security culture.

Use Strong, Unique Passwords

Avoid reusing passwords across systems. Instead, use complex, unique passwords for each account, and consider using a secure password manager to simplify management.

Enable Multi-Factor Authentication (MFA)

MFA provides an essential extra layer of security. Even if login credentials are stolen, MFA makes it far more difficult for attackers to gain access.

Be Wary of Unsolicited Communications

Treat unexpected emails, phone calls, or messages with caution—especially if they create a sense of urgency or request sensitive information. Always think before you click, download, or respond.

Verify Through Trusted Channels

Never act on instructions or information from a message alone. Always confirm through an independent, trusted source—such as a phone call to a known contact or direct communication via company tools.

Keep Devices and Software Up to Date

Many attacks exploit known software vulnerabilities. Enable automatic updates where possible and patch all systems regularly to stay protected.

Back Up Data Regularly

Ensure critical data is backed up frequently and stored securely. Backups should be tested, encrypted, and disconnected from the main network when not in use, to safeguard against ransomware and breaches.

ADOPT A ZERO TRUST MINDSET

Trust nothing by default—verify everything. Implement access controls, monitor activity continuously, and limit permissions based on role. This reduces the risk if credentials are compromised.

By following these best practices, your organisation can build strong human defences against the constantly evolving tactics of social engineering.

SOCIAL ENGINEERING

RESPONDING TO ATTACKS

Even with strong defences in place, no system is entirely immune to social engineering. A swift and informed response can significantly reduce the impact of an incident and help prevent future occurrences.

REPORTING INCIDENTS

Suspected social engineering attacks should be reported immediately to your IT or security team for investigation and containment. Swift action limits further impact and ensures proper handling.

- Under GDPR, personal data breaches must be reported within 72 hours.
- For organisations in scope of NIS2, significant cyber incidents must be reported within 24 hours, with follow-up reports at 72 hours and one month.
- DORA applies to financial entities, requiring structured reporting of ICT-related incidents to supervisory bodies.

If financial loss or fraud has occurred, notify law enforcement and any relevant regulatory authorities.

If an individual falls victim to a social engineering attack:

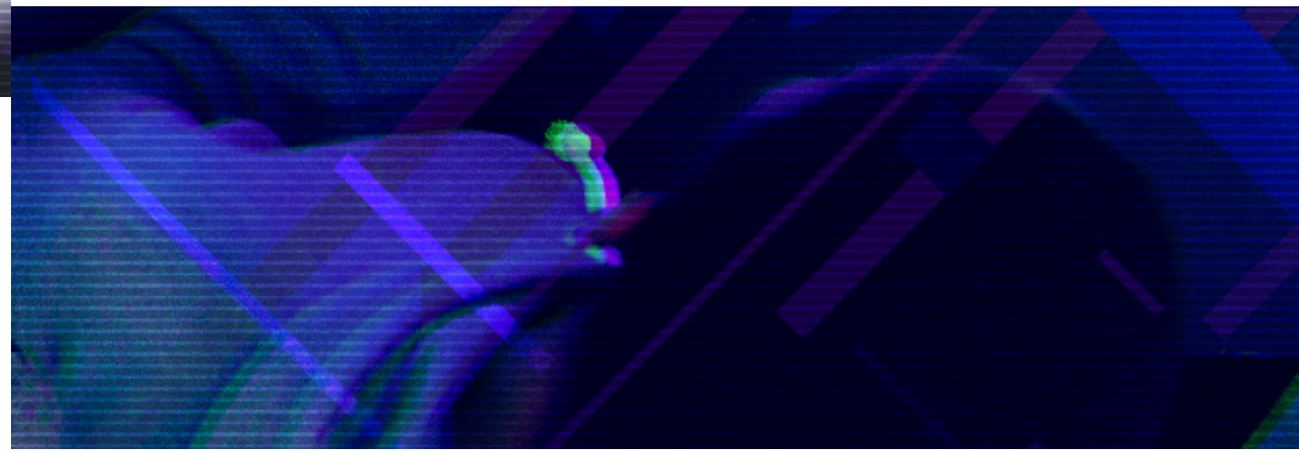
- Change affected credentials
- Monitor accounts and systems for unusual activity
- Review access logs and permissions

STRENGTHENING SECURITY POSTURE

Every incident should trigger a review of what went wrong and how to prevent recurrence. Use lessons learned to:

- Refine security policies
- Improve training and simulations
- Strengthen supplier and third-party controls

NIS2 and DORA both emphasise continuous improvement in cyber resilience—responding to incidents isn't just a best practice, it's a compliance expectation.



CONCLUSION

Social engineering remains one of the most persistent threats in today's cybersecurity landscape, exploiting the human element as the weakest link. Tactics such as phishing, pretexting, and emotional manipulation are used to deceive individuals into lowering their guard. To defend against these evolving threats, it's vital to train your team regularly, use strong and unique passwords, enable multi-factor authentication, and stay alert to unsolicited communications. Verifying requests through trusted channels, keeping systems up to date, and backing up data regularly all add vital layers of protection. If an attack does occur, swift reporting, impact assessment, and corrective action are key to minimising damage and strengthening your defences.

At IT.ie, we've been helping businesses across Ireland protect their data since 2004. Our CyberProtect User solution delivers a multi-layered defence tailored to securing your people—the front line of your business. If you'd like expert advice on protecting your organisation from social engineering and other cyber threats, get in touch with our team today.

HELLO@IT.IE

1800 353 353

DUBLIN
Unit 35, Finglas Business Centre, Jamestown Road, Finglas Dublin 11, D11 EP86

CORK
Unit P5, Marina Commercial Park, Centre Park Rd, Cork, T12 PN7F

GALWAY
Galway Technology Centre, Mervue Business Park, Galway, H91 D932