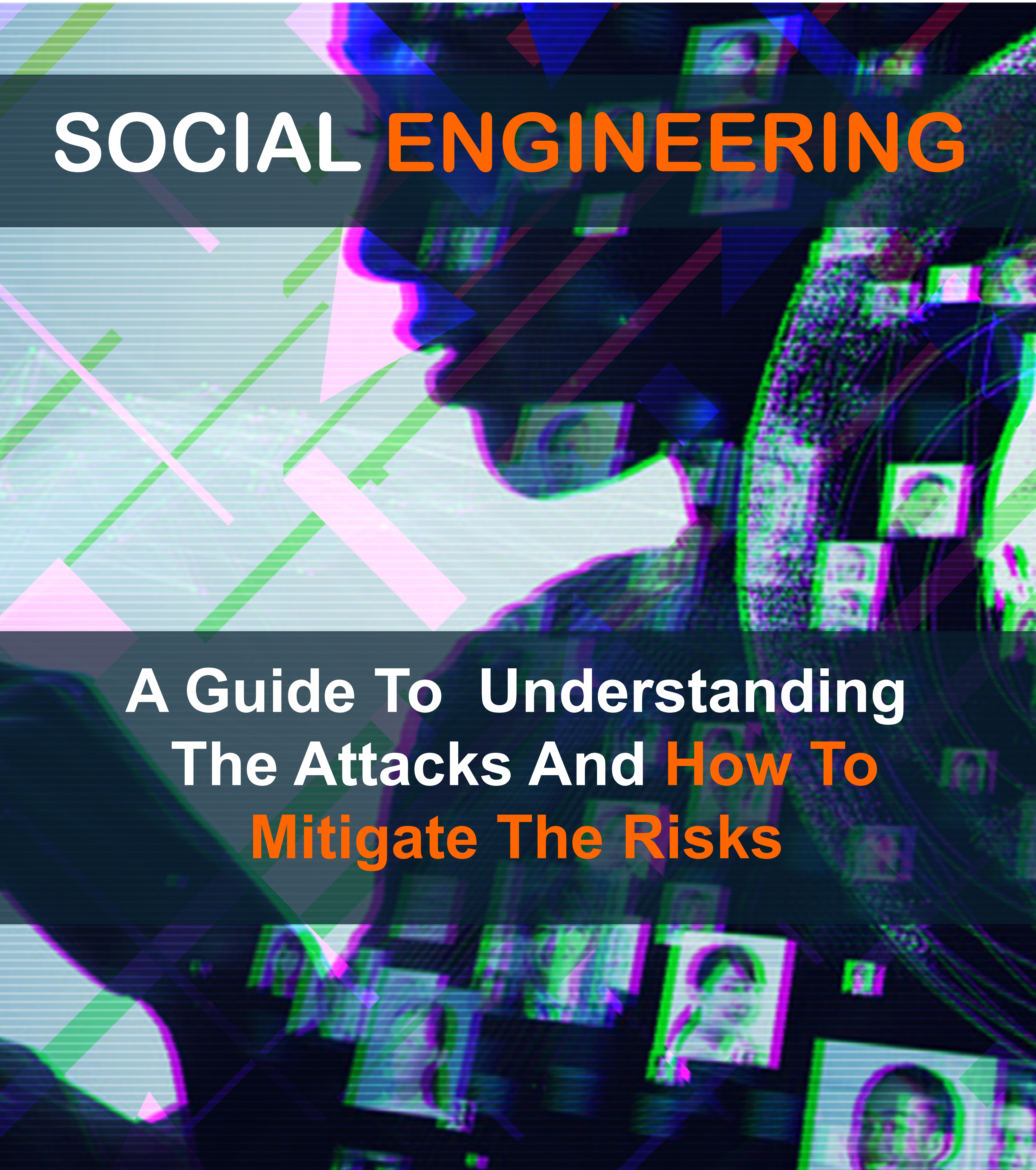
SOCIAL ENGINEERING

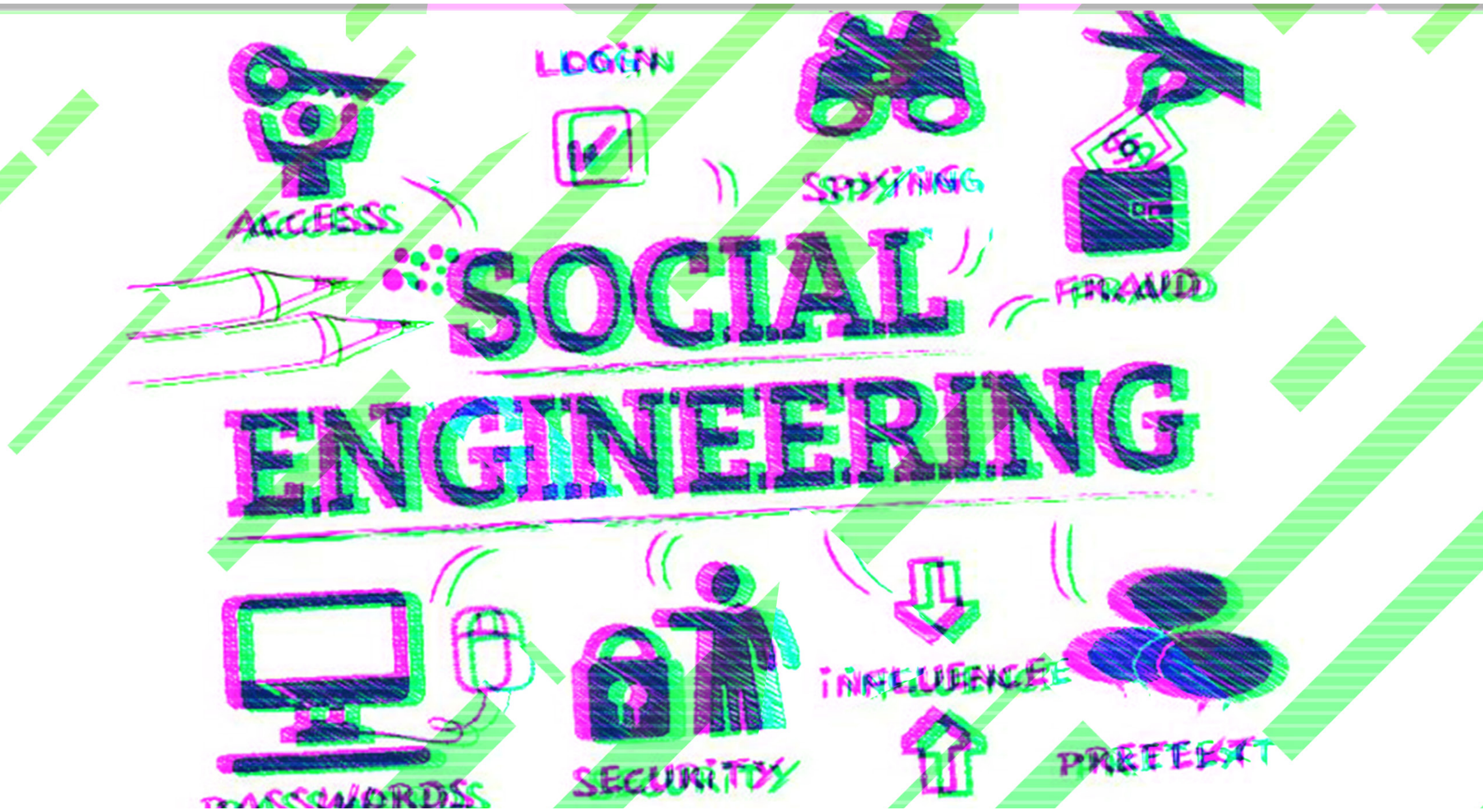
A Guide To Understanding The Attacks And How To Mitigate The Risks



> “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 continually evolving and has largely transcended the traditional methods of hacking and virus distribution. Today, social engineering attacks have emerged as one of the most insidious and effective means of attack, relying on manipulation and psychology instead of technical expertise. Modern IT systems are difficult to infiltrate from the outside but no so when you manipulate or trick someone into granting you access. In this guide, we will explore social engineering attacks, the various techniques employed by cyber-criminals, and provide practical tips on how to stay safe from these ever-evolving threats.

SOCIAL ENGINEERING

DECONSTRUCTING SOCIAL ENGINEERING

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.

Social Engineering Ranks #1 as the Top Attack Type in 2022

Social Engineering-Based Data Breaches Took 270 Days to Identify and Contain

82% of Data Breaches Involve the "Human Element"

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

47% of Social Engineering-Related Security Incidents Resulted in Data Disclosures

SOCIAL ENGINEERING OVERVIEW

PHISHING

Phishing is a type of social engineering attack that involves sending fraudulent emails or messages that appear to come from legitimate sources. The objective is to trick recipients into revealing sensitive information or downloading malware. Phishing emails will generally encourage you to take and action such as clicking on a link that appears to be legitimate but will likely lead to a compromise.

SPEAR PHISHING AND WHALING

Spear phishing is much more focused and will target an individual or small group by gleaning data from sources such as social media sites to trick the recipients. This email will be personalised and may appear to come from a legitimate bank or organisation that you are associated with. Executive Whaling is like Spear Phishing in that the cyber-criminals target individuals. In this case however, the targets are top executives

PRETEXTING

Pretexting is a social engineering technique that involves creating a false scenario to manipulate individuals into revealing sensitive information or performing certain actions. This type of social engineering attack is not exclusively online and may take place through other forms of communication, including in person.

BAITING

Baiting entices victims into revealing sensitive information or downloading malware with a false promise. Baiting attacks may leverage a free offer or a highly sought after item at a very low price to entice the user into entering their login or payment details into a fake website or some form of online portal.

QUID PRO QUO

Quid pro quo means something for something where a service or assistance in offered in exchange for sensitive information or access. Whereas baiting typically takes the form of offering goods, quid pro quo typically offers a service. The intention here is to siphon off money from accounts or steal confidential data. Personalisation and detailed knowledge of the executive and the business are the hallmarks of this type of fraud.

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.

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.

IMPERSONATION

Social engineers may pose as legitimate representatives of an organisation, a friend, or a family member to gain the trust of their targets. They may spoof the email address of a person known to you or contact you on a messaging app claiming to be a family member who has lost their phone and is using a temporary number. In this case they are trying to get you to engage with them and win your trust before dropping the hammer and making an urgent demand.

COMMON GOALS OF SOCIAL ENGINEERING

By creating a sense of urgency, social engineers can pressure their targets to act quickly without considering the potential risks. They often use authority figures or influential individuals to gain compliance from their targets. An example of this is the CEO Scam whereby, the victim receives an email purporting to be from a senior member of their organisation with an urgent demand to make a payment or send confidential information. leads to a compromise.

> “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

DETECTING AN ATTACK

RED FLAGS IN EMAILS AND MESSAGES

Be cautious of suspicious attachments, spelling errors, generic greetings, or mismatched URLs in emails or messages that could indicate a potential social engineering attack.

UNUSUAL REQUESTS AND BEHAVIOURS

It is essential to be wary of requests that seem out of the ordinary or ask for sensitive information regardless of who you believe is requesting the information.

VERIFYING THE SOURCE OF INFORMATION

Before acting on any request or sharing sensitive information, you must verify the authenticity of the source through known and trusted channels. Do not respond to the request from the contact information in the email. If the request is from a bank, then simply look up their contact number on their website and contact them directly or if it claims to come from senior member of the company, give that person a call. You should never get into trouble for carrying out due diligence.

IDENTIFYING FAKE WEBSITES AND URLS

There are several red flags that can help you identify a fake website. Check the domain name closely, it may be very similar to a legitimate one but with subtle differences. Check for poor spelling and grammar and poor website design. You should also be wary of any website that doesn't have the lock symbol to the left of the domain name.

SOCIAL ENGINEERING BEST PRACTICES

EDUCATE AND TRAIN YOUR EMPLOYEES

Regular training and cyber awareness programs can help you and your team to recognise and avoid social engineering attacks that are designed to compromise your systems and steal sensitive data.

MAINTAIN STRONG AND UNIQUE PASSWORDS

To minimise the risk of unauthorised access, everyone should use complex, unique passwords for different accounts.

MULTI-FACTOR AUTHENTICATION

Multi Factor Authentication or MFA is a security measure that requires you to provide at least two separate pieces of information before you are granted access.

BE CAUTIOUS WITH UNSOLICITED COMMUNICATION

You should always be extra cautious with unexpected emails, phone calls, or messages, especially if they request sensitive information or require you to carry out an action.

VERIFY REQUESTS THROUGH MULTIPLE CHANNELS

Confirming the legitimacy of requests through multiple channels and contacts can help individuals avoid falling victim to social engineering attacks.

KEEP DEVICES AND SOFTWARE UP TO DATE

Many software updates include patches for security vulnerabilities, so it’s important to stay current.

REGULARLY BACK UP DATA

Regular backups can help protect data in case of a successful social engineering attack or a data compromise by another method of cyber-attack.

SOCIAL ENGINEERING
RESPONDING TO ATTACKS

REPORTING INCIDENTS

You should always report suspected social engineering attacks to your IT Department for investigation and advice on the steps to take to mitigate the impact. An attack that has resulted in the compromise of company data or finances should also be reported law enforcement and regulatory agencies. In the EU there is a requirement to report data breaches within 72 hours of you becoming aware of the breach under GDPR.

ASSESSING THE DAMAGE AND TAKING CORRECTIVE ACTION

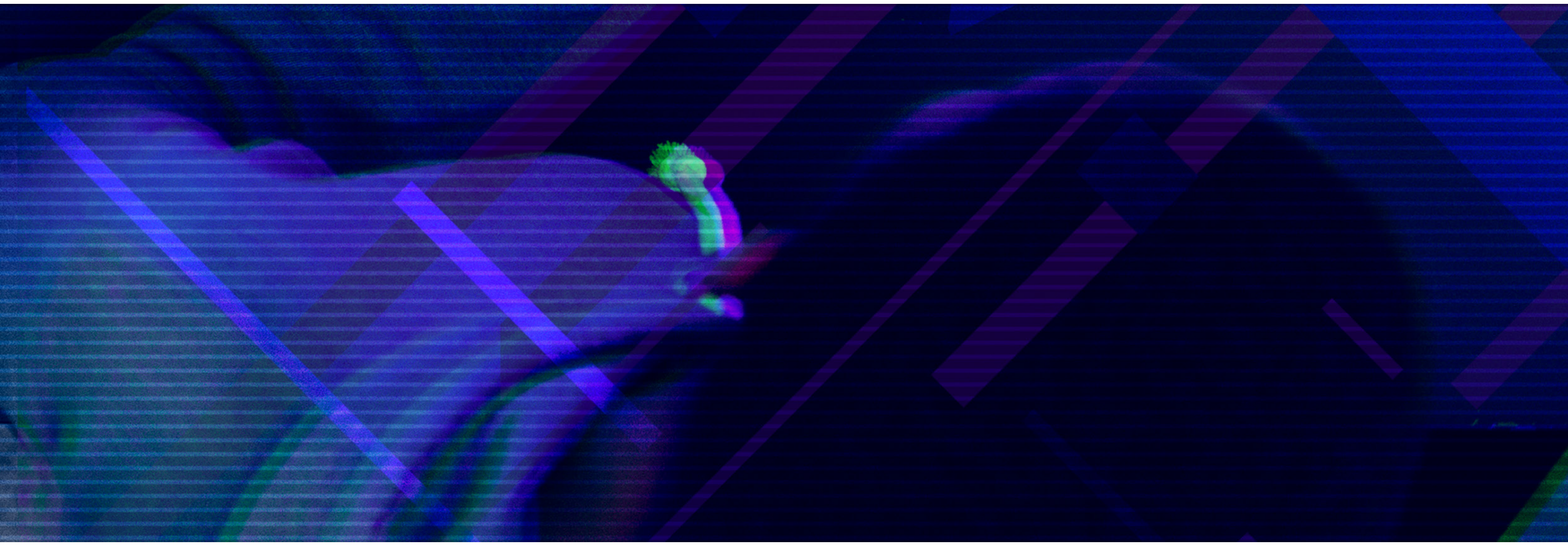
If an individual at your organisation falls victim to a social engineering attack, assessing the damage and taking appropriate corrective action, such as changing passwords or monitoring accounts for suspicious activity, can help mitigate the impact.

STRENGTHENING SECURITY POSTURE

Learning from social engineering incidents can help improve security measures and processes, making it more difficult for attackers to succeed in the future.

SOCIAL ENGINEERING Vs SOCIAL HARVESTING

Social engineering and social harvesting are two distinct practices, but they share some similarities. We now know that social engineering involves the use of psychological manipulation to deceive or exploit individuals, often through the use of fraudulent emails, phone calls or text message. In contrast, social harvesting involves the collection of personal information about individuals from various online sources, with the goal of using that information for nefarious purposes. While social engineering and social harvesting differ in their methods, they both rely on the collection and analysis of personal information to achieve their goals.



CONCLUSION

Social engineering attacks have become a prevalent threat in the cyber security landscape, targeting the human element as the weakest link in the security chain. These attacks utilise various techniques, such as phishing, pretexting, and emotional manipulation, to deceive individuals into compromising their security. To stay safe from these ever-evolving threats, it is crucial to educate yourself and your employees on best practices, maintain strong and unique passwords, implement multi-factor authentication, and be cautious with unsolicited communication. Additionally, verifying requests through multiple channels, keeping devices and software up to date, and regularly backing up data can provide further protection. In the event of a social engineering attack, prompt reporting, assessing the damage, and taking corrective action are essential steps to mitigate the impact and strengthen security measures for the future. IT.ie have been helping businesses throughout Ireland protect their sensitive data since 2004. If you would like to know more about how to protect your business from a cyber-attack, talk to our team of experts 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