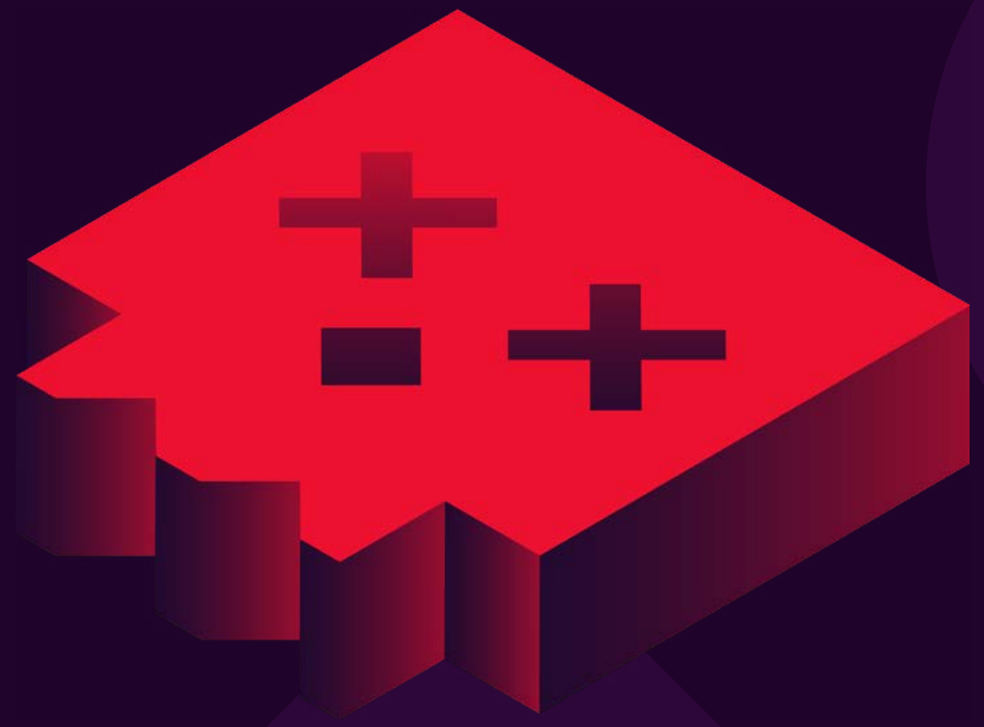
FourNet®

Quick Guide on

Socially Engineered Attacks

Enter Guide



Copyright 2022®

Welcome to our Quick Guides to Cyber Security Series.

These five guides have been created to give you an overview of the key pillars and solutions needed to overcome the challenges arising from Cyber threats.

Other guides in our security series:

Secure Infrastructure | Quick Guide to Edge/Perimeter Security

Secure Infrastructure | Quick Guide on Endpoint Security

Secure Infrastructure | Quick Guide to Cloud Security

Secure Infrastructure | Quick Guide to Data and Compliance

Secure Infrastructure | Quick Guide to Socially Engineered

In these guides, we outline all the major risks and threats, security trends, common challenges, and impacts. Finally, we consider the best ways to calculate and mitigate the risks to your organisation, the key measures which should be introduced, and outline how FourNet's best-in-class security solutions can help.

If you take one concept from this series, it is that effective cyber security requires a layered approach to be successful. Also be mindful that compliance does not make an organisation secure and relying solely on technology to provide the solution won't combat the inherent risks posed by humans.

Building the right security culture and strategy is like Lego, needing many pieces to intersect and interplay to help mitigate the increasing level of risk our organisations face.

Most successful cyber-attacks start with a human, yet many organisations overlook this network of employees in security practices. In this guide, we provide insight and context into how social engineering is used to breach cyber defences and the steps you can take to build a resilient and cyber aware workforce.

Copyright 2022®

Contents

01 Cyber Security and The Human Challenge

02 Common Types of Socially Engineered Attacks

03 Overcoming the Human Challenge

04 How FourNet Can Help

Copyright 2022®

01 Cyber Security and The Human Challenge

02 Common types of socially engineered attacks

03 Overcoming the Human Challenge

04 How FourNet Can Help

Cyber Security and The Human Challenge

Whilst technology can deliver protection and intelligence against many types of threats. Humans can very quickly undermine investment and efforts within your organisation.

It is commonly accepted that the human element of your organisation poses a significant risk as humans can be coerced into taking actions they knowingly wouldn't do.

The truth is that social engineering is at the heart of most successful attacks. Social engineers use manipulation tactics to obtain and use information and credentials from individuals within an organisation. These tactics range from spear phishing to using fake Wi-Fi connections to trick or otherwise confuse their way into your private data.

While it may seem like social engineering is the "long way" around for threat actors (those with nefarious intent), **98% of cyber-attacks rely on social engineering.** Whether the goal is to harvest credentials, install malware or commit fraud, it's accepted that a human will be coerced into taking action at some point.

Several areas are specifically targeted by threat actors, which are increasingly being used to manipulate individuals, which include social media, web applications and deep fakes.

In the **Social Engineering report from Proofpoint**, it was noted that threat actors have been using increasingly involved and sophisticated ways to engage with victims over the last year.

Threat actors are now holding extended conversations with victims, building greater trust.

Using 'Trusted Companies' to deliver effective attacks has increased.

Threat actors are making use of existing conversation threads between colleagues to deliver attacks.

Attacks continue to leverage topical, timely and socially relevant themes.

"Social engineering is defined in the context of information security as "The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."

Types of Social Engineered Attacks

Several common types of attacks use social engineering, and staff within your organisation will undoubtedly have already been exposed to one or more.

These include Spear Phishing emails, Quid Quo Pro, Baiting and whaling.

Many organisations have been hit by cybercrime, and recent figures put the costs to the United Kingdom economy at an estimated **£27 billion**. Phishing is the prime culprit in launching successful attacks, and it doesn't help that nearly **97% of users don't recognise a phishing email and only 3% report attacks to their IT security teams**. It's also widely accepted that 85% of all organisations have succumbed to an attack of this nature at least once.

The Anti-Phishing Working Group, or APWG, has released its Phishing Activity Trends Report for the **second quarter of 2022. The report reveals that in the second quarter of 2022, there were 1,097,811 total phishing attacks— a new record and the worst quarter the APWG has ever observed**. The report also revealed an upward surge in ransomware attacks targeting healthcare and transportation.

In a recent report from security vendor Sophos, attackers, on average, are in the network for 11 days before being identified. However, much information can be siphoned off during this time, and malicious activity occurs.

Copyright 2022®

01 Cyber Security and The Human Challenge

02 Common types of socially engineered attacks

03 Overcoming the Human Challenge

04 How FourNet Can Help

Common Types of Socially Engineered Attacks

Executive Whaling

Whaling emails are often more sophisticated than generic phishing emails as they often target specific high-level executives and contain personalised information about the individual or the organisations. These often are of an urgent nature to increase the likelihood of the recipient acting.

In some cases, attackers will sit undetected on the network, intercepting communications, especially around financial transactions, and payments.

There are two common ways in which an attack is launched. The first is name spoofing. During an attack of this nature, the threat actor uses the name of a CEO or senior leadership team member but with a tweaked email address, often similar to the company's domain.

Using this method, the attacker hopes the recipient will not notice the incorrect sender address and will rush to respond. These can also be engineered to be sent when the recipient may be under pressure and not thinking, such as at the close of business on a Friday. A further challenge is that some email and mobile clients do not display the sender address by default, making these even harder to detect.

Another form is name and email spoofing, where the attacker uses both the CEO's name and their correct sender address. In this form of the attack, the attacker typically uses a reply-to address that is different from the sender's address so that your response to the email will go to them.

Examples of Whaling

- A request for sensitive information such as Payroll information about current and past employees.
- Intercepting and interrupting an unencrypted conversation to divert payments into a fraudulent bank account.
- Setting up fictional meetings with malware links disguised as a zoom meeting.

Phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Quid Pro Quo

A quid pro quo attack is a lower-level form of socially engineer attack. For example, this could see an attacker calling you, pretending to be from a service provider offering support. The attacker will help of some kind, but only works if you are already experiencing some difficulty. The aim is to be allowed access to your device or computer to plant malware. These types of attack are less common in business, but on the rise in our personal lives.

Baiting

Baiting is a common method of spreading malware. It involves leaving an open device, such as a CD or flash drive, in an open location to tempt a victim into seeing what's on it. When the victim opens files on the media, it executes a malware program that releases a virus or leads to personal and financial information being exposed to hackers.

The infection can spread and propagate if the victim uses a network. Flash drives are a common medium used for such an attack as these are rarely encrypted, and most of their contents aren't password protected; they're easy for hackers to access and use as bait for spreading malware.

In a recent study that looked at 50 organisational USB drives, none were found to be encrypted, and no files were password protected. This is a major area of risk with laptops and flash drives commonly lost or stolen. This can be rectified by introducing tighter control and policy measures across the organisation.

Copyright 2022®

01 Cyber Security and The Human Challenge

02 Common types of socially engineered attacks

03 Overcoming the Human Challenge

04 How FourNet Can Help

Overcoming the Human Challenge

Whilst humans can be your weakest link, they can also learn and become a resilient and dependable firewall to your organisation.

Clearly steps can be implemented from a technological standpoint to try and minimise exposure to socially engineered threats. These include email filtering and ensuring that two-factor authentication is used, which can all help mitigate some risks.

Things can become a little trickier when it comes to the human element. We are raised from childhood to be helpful to other human beings, and often pre-programmed to be trusting of those around us. There is therefore a defined need for reprograming us to be vigilant and aware within the digital world.

In addition, users don't always have a vested interest in the bigger organisational picture and often can adopt an attitude of 'self' rather than the team.

In our modern workplaces we also have a mix of generations, The baby boomers, who had to learn to embrace technology, and Generation X, who grew up both with and without the internet, two large groups that are not by age digitally native.

This poses a problem regarding staff's awareness, abilities, and knowledge to identify and protect against engineered attacks. Organisations have also been slow to recognise the threat levels posed by socially engineered attacks and have failed to take steps to empower and boost the human defences within the organisation.

"The hardest part of preventing social engineering is overcoming the human instinct to be helpful"

Top cybersecurity training topics

Critical topics that should underpin your security awareness training.

- Phishing Attacks
- Password Hygiene
- Social Engineering Attacks
- Secure Remote Work Practices

Copyright 2022®

01 Cyber Security and The Human Challenge

02 Common types of socially engineered attacks

03 Overcoming the Human Challenge

04 How FourNet Can Help



Building Your Human Defences

Organisations need to develop a culture of security throughout every facet of the business. This needs to start at the top with Senior leadership buy-in and permeate through every aspect of operations.

This culture needs to resonate at all levels and should be reinforced regularly, but in the right ways, so as not to create a negative perception of the need to learn and adopt a security minded approach.

This requires a strategic plan and policy to help educate and drive security into the everyday working practices of the organisation. For example, look to develop a community of security advocates within the business that understands the risks, pushing and leading the organisation to take the appropriate steps to secure the vulnerable areas, and mentor staff and teams.



Train, Test and Train

A fundamental step in creating a security culture is to train staff to identify and act within secure parameters in the workplace. Staff Cyber Awareness Training supports this drive.

Organisations must invest in building knowledge and awareness around the differing risks, which helps to create a workforce and culture that can defend and repel cyber-attacks.

However, it is crucial that this training is informative, engaging and fun as no one can get enthusiastic about something that they feel is uninteresting and forced upon them.

Security training also allows testing this human firewall with automated phishing attacks, which can quickly identify individuals or departments that may require additional focus or attention. It can also enable organisations to benchmark their current security posture and measure this over time with simulated phishing attacks.

The investment in this area alone can deliver a considerable return and, in conjunction with other key



Investing can yield a positive ROI

The monetary impact of downtime for an organisation, department or individual has a tangible measurement, but what can be the unknown is the impact of reputational damage and the cost of remediation should the worst happen. Staff awareness training has been proven to deliver a positive ROI, and at a very basic level, can be calculated by taking the average cost of an incident and multiplying that number by how many incidents a business might experience in a given time frame.

Copyright 2022®

01 Cyber Security and The Human Challenge

02 Common types of socially engineered attacks

03 Overcoming the Human Challenge

04 How FourNet Can Help

How FourNet Can Help

Our clients benefit from our experience working with some of the biggest names in government, healthcare, and finance. We have delivered solutions that have been recognised as Best of Breed by industry bodies such as Government Digital Service (GDS).

At FourNet, our solutions are designed to always protect your organisation from downtime - whether it's network failure or an attack on your infrastructure - so you can concentrate on what matters most: keeping people safe.

Trusted by Mission Critical Organisations

FourNet are trusted by some of the most secure and mission critical organisations in the UK including Whitehall, Downing Street, Cheshire Fire and Rescue, South Coast Ambulance Service, and others. Offering a diverse portfolio of solutions for both public sector and private enterprise with cloud solutions like ANTENNA and Agile Cloud.

We also provide highly available contact centre solutions delivering 999 & 111 services to the public and back-office solutions to support a flexible, agile workforce and have highly accredited and security cleared engineers and consultants.

Helping You to Understand Security Posture

FourNet's security specialists are here to help your organisation detect, defend, and repel threats from whatever threat vector they emerge. Our team of experts will work alongside you to identify and remediate areas of concern or risk. We work with you to build a business case to demonstrate ROI and payback periods based on your current costs and KPIs. Get in touch to schedule an initial discovery call.

Managed Security to Remove the Worries

We offer a range of managed solutions from the world's leading security vendors, all underpinned by SC and DV level security cleared engineers and consultants. Our best-in-class security cleared service management from our dedicated secure Service Desk, FourNet, provides a Security Operations Centre (SOC) with 24/7 phone support and multi-factor authenticated ITSM access.

Whether you want to secure and control access to critical systems or outsource security to a managed SOC, we can help. We work with you to understand your organisation and provide the help, solutions, and support where it is needed most.

Copyright 2022®

01 Cyber Security and The Human Challenge

02 Introduction

03 Overcoming the Human Challenge

04 How FourNet Can Help

Get Started with a Free Simulated Phishing Campaign

Discover what percentage of your employees would respond to a phishing email and discover how your organisation ranks against others. This is an effective way to get an understanding of how to achieve best practice to patch your last line of defence

How the Phishing Test Works

- Start your test for up to 100 users
- Select from 20+ languages and customise the phishing test template based on your environment
- Choose the landing page your users see after they click
- Show users which red flags they missed, or a 404 page
- Get a PDF emailed to you in 24 hours with your Phish-prone % and charts to share with management
- See how your organisation compares to others in your industry

Understanding your current Phishing score can also be an effective way to make a business case to secure budget for investment. Talk with us to book your simulated phishing campaign today.

Trusted by Mission Critical Organisations

FourNet are trusted by some of the most secure and mission critical organisations in the UK including Whitehall, Downing Street, Cheshire Fire and Rescue, South Coast Ambulance Service, and others. Offering a diverse portfolio of solutions for both public sector and private enterprise with cloud solutions like ANTENNA and Agile Cloud.

We also provide highly available contact centre solutions delivering 999 & 111 services to the public and back-office solutions to support a flexible, agile workforce and have highly accredited and security cleared engineers and consultants.

Managed Cyber Security Awareness Training

We offer a range of both standalone and managed Training solutions from the award-winning vendors. Offering simulated Phishing campaigns and engaging online training, we work with you, to develop an awareness program tailored to your organisational needs and structure.



Copyright 2022®

FourNet®

Manchester Office (HQ)
3 Scholar Green Road,
Cobra Court,
Manchester. M32 0TR
Tel: 0845 055 6366

London Office
83 Victoria Street,
London. SW1H OHW
Tel: 0203 503 0003

Burton Office
First Floor, Unit 10 Barberry Court,
Burton-on-Trent,
Staffordshire. DE14 2UE
Tel: 01283 519020

Scarborough Office
Unit 2, Lora Court
Wykeham Business Centre
Scarborough,
YO13 9QP
Tel: 0333 344 8971

FourNet PR & Media Office
Tim Reid
e-mail: treid@fournet.co.uk

0161 864 5130
sales@fournet.co.uk
www.fournet.co.uk

Copyright 2022®