Cyber fraud

The Corporate Finance Manager's guide to protecting your business

BARCLAYS

Contents

Introduction

Falling victim to a cyber fraud attack can result in major financial losses, while data breaches can severely damage customers' trust in a company. Fraudsters can monetise stolen information by selling it online, and the impact of this on a business' reputation can be critical.

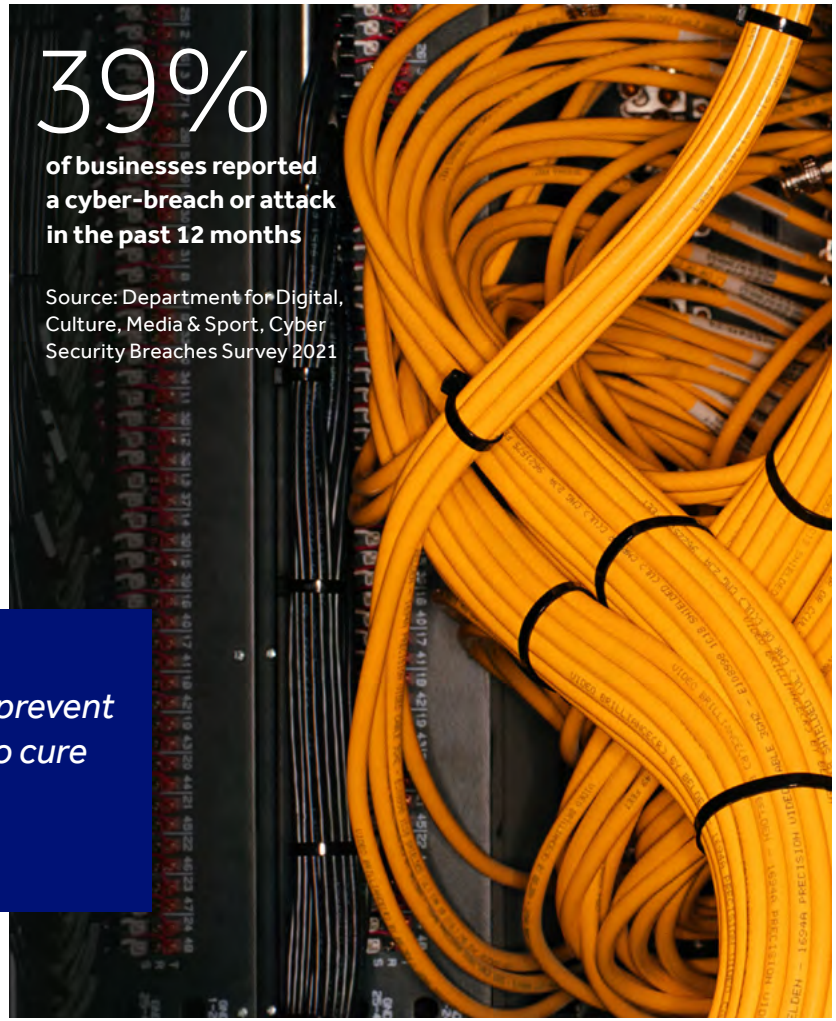
Fraud often takes place over many different jurisdictions, with victims, beneficiaries and fraudsters potentially located in different countries. Cybercriminals operating online through software, emails and internet-based communications are exceptionally difficult to identify and track down.

This makes it difficult to investigate fraud and, crucially, very hard to recover funds. For this reason, businesses must look to prevent fraud, rather than hope to cure its consequences. At Barclays, we are dedicated to helping you protect your business from the risks of cyber fraud attacks.

This guide aims to outline some of the key threats your business may face today, and offer guidance on how to mitigate those risks. We can't cover every fraud risk your business may be exposed to in a single document, so this guidance is intended as a supplement to your own fraud risk management.

B.Chance

Ben Chance
Barclays International,
Fraud Transaction Cycle Lead



> *"Businesses must look to prevent fraud, rather than hope to cure its consequences"*

Social engineering

90%

of cyber data breaches in 2019 were caused by human error

Source: Cybsafe

The threat of cyber fraud is difficult to combat, as the software used by fraudsters can be complex. However, it is important to remember that most cyber fraud attacks depend heavily on human interactions – fraudsters have long known that the easiest way to breach an organisation's defences is to target its people, not its systems.

Social engineering is the method by which fraudsters aim to trick people into breaking normal security procedures. Fraudsters are usually looking for the victim to give up sensitive information, such as bank login details, or for them to enable malicious software to be installed onto their device. They may also trick the victim into carrying out a fraudulent payment themselves.

Fraudsters in social engineering cases often use thorough knowledge of the company to help them to build trust with the victim. They may be aware of regular payments that are due, or of the structure of teams within your company, enabling them to impersonate internal employees.

Chapter 1: Social engineering

The most common forms of social engineering for corporate clients are:

- Invoice fraud
- CEO impersonation
- Phishing
- Vishing and Smishing

The Covid-19 pandemic has presented new opportunities for cybercriminals to attack organisations. Fraudsters have been impersonating government departments, charities and online communication companies with Covid-19 themed invoices, and impersonation frauds focused on items in short supply, such as Personal Protective Equipment (PPE) and medical equipment.

Verbal checks

As fraudsters employ new tactics to try to trick you into sending them money, it's important to always remember to check any new payment requests.

It's vital that you conduct verbal checks before making a payment. Read more on checking payee details here.

Invoice fraud

***Invoice fraud* is when a fraudster notifies your company that supplier payment details have changed and provides alternative details in order to defraud you.**

Invoice fraudsters are often aware of the relationships between companies and their suppliers, and will know the details of when regular payments are due. The fraud may only be discovered when the legitimate supplier follows up on non-payments.

Fraudulent letters and emails sent to companies are often well-written, meaning the fraud can be difficult to spot without strong operating processes and controls in place. Email addresses are unfortunately quite easy to spoof, or in the case of malware-infected PCs, criminals can access genuine email addresses. The process of changing the bank details of someone you are paying should always be treated with extreme caution, and appropriate processes should be followed to ensure the details are authentic.

What would you do?

Claire* received an email purporting to be from a known supplier notifying her of a change in account details and requesting a payment of £234,000.

The payment was made and was held by the bank for additional security checks. Claire told the bank that verbal checks had been performed and asked for the payment to be released. The bank strongly recommended that the details were checked through a known and trusted phone number.

Claire followed the bank's advice and the genuine supplier confirmed the payment request as fraudulent. She later explained that due to employees working from home, the company's normal process of conducting verbal checks had not been followed in the first instance.

* Names changed to protect anonymity

Protecting your business against invoice fraud

- Always check the details of any new/amended payment instructions verbally by using details held on file, and do not solely rely on the new instruction. Fraudsters can imitate email addresses to make them appear to be from a genuine contact, including someone from your own organisation.
- If you are suspicious about a request made by phone, call them back on a trusted number. Fraudsters will attempt to pressure you into making mistakes – take the pressure off by taking control of the situation.
- Consider removing information such as testimonials from your own or your suppliers' websites or social media channels, as these can help fraudsters identify your suppliers.
- Look carefully at every invoice and compare it to previous ones received that you know to be genuine – particularly the bank account details, wording used and the company logo. When making a payment, ensure your invoices quote the full legal or 'trading as' name.
- Consider setting up single points of contact with the companies you pay regularly.
- Apply the same principles to requests from within your own organisation.
- Always pay attention to Confirmation of Payee (CoP) alerts. CoP is an industry initiative designed to target Authorised Push Payment (APP) fraud in the UK, particularly impersonation fraud, invoice redirection and new payment fraud. The service enables you to check the name of an account against the sort code and account number and confirm whether or not the account details and account name match.
- Regularly conduct audits on your accounts.
- Fraudsters will look for opportunities to exploit any vulnerabilities in your processes. Therefore it is crucial to ensure staff are regularly educated, particularly those that are responsible for making payments.
- While working remotely, ensure you and your colleagues remain vigilant and adhere to relevant checks and processes.

CEO impersonation

84%

year-on-year increase in impersonation fraud in the first half of 2020

Source: UK Finance

***CEO impersonation*, also known as Business Email Compromise (BEC), is a form of social engineering. Fraudsters pretend to be a senior manager – often the CEO – in order to persuade a staff member to make a payment.**

The payment request is often made via email, apparently from a senior person in the company, normally to the accounts department, requesting an urgent payment to a supplier or partner.

The fraud attempt sometimes occurs when the senior person is out of the office, and the request may outline that the transaction is confidential and sensitive in order to discourage further verification.

For instance, the fraudster may try to convince the victim that their company is about to acquire another business and the payment is needed as a down-payment for the confidential deal.

What would you do?

Richard* received an email instruction purporting to be from the company's Finance Director requesting a payment for £23,945 to be made.

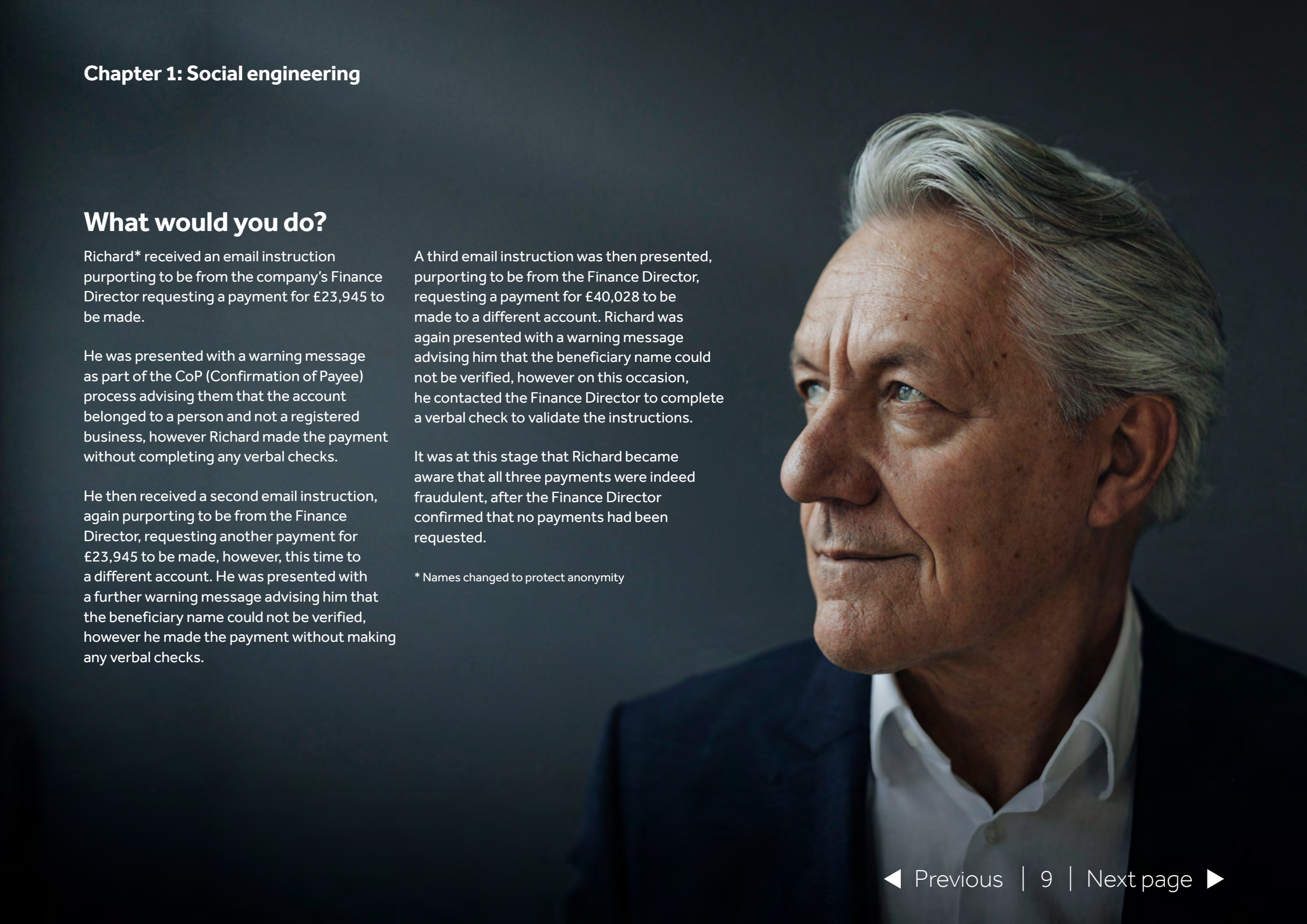
He was presented with a warning message as part of the CoP (Confirmation of Payee) process advising them that the account belonged to a person and not a registered business, however Richard made the payment without completing any verbal checks.

He then received a second email instruction, again purporting to be from the Finance Director, requesting another payment for £23,945 to be made, however, this time to a different account. He was presented with a further warning message advising him that the beneficiary name could not be verified, however he made the payment without making any verbal checks.

A third email instruction was then presented, purporting to be from the Finance Director, requesting a payment for £40,028 to be made to a different account. Richard was again presented with a warning message advising him that the beneficiary name could not be verified, however on this occasion, he contacted the Finance Director to complete a verbal check to validate the instructions.

It was at this stage that Richard became aware that all three payments were indeed fraudulent, after the Finance Director confirmed that no payments had been requested.

* Names changed to protect anonymity



Chapter 1: Social engineering

Protecting your business against CEO fraud

- ✓ Any payment requests with new or amended bank details received by email, letter or phone should be independently verified. This includes internal emails from senior management that contain payment requests. Fraudsters can imitate email addresses to make them appear to be from a genuine contact, including someone from your own organisation.
- ✓ Regularly conduct audits on your accounts.
- ✓ Make all staff aware of this type of fraud, particularly those that make payments.
- ✓ Ensure warning messages are understood and that appropriate checks, actions and processes are followed to ensure requests are genuine.
- ✗ Don't be pressured by urgent requests, even if they appear to originate from someone senior — remember this is a common tactic adopted by fraudsters.
- ✗ Dont' reveal too much about your company and key officials via social media platforms and out-of-office automatic replies.
- ✗ Don't share testimonials on your own or your suppliers' websites or social media channels that could help fraudsters identify your suppliers.

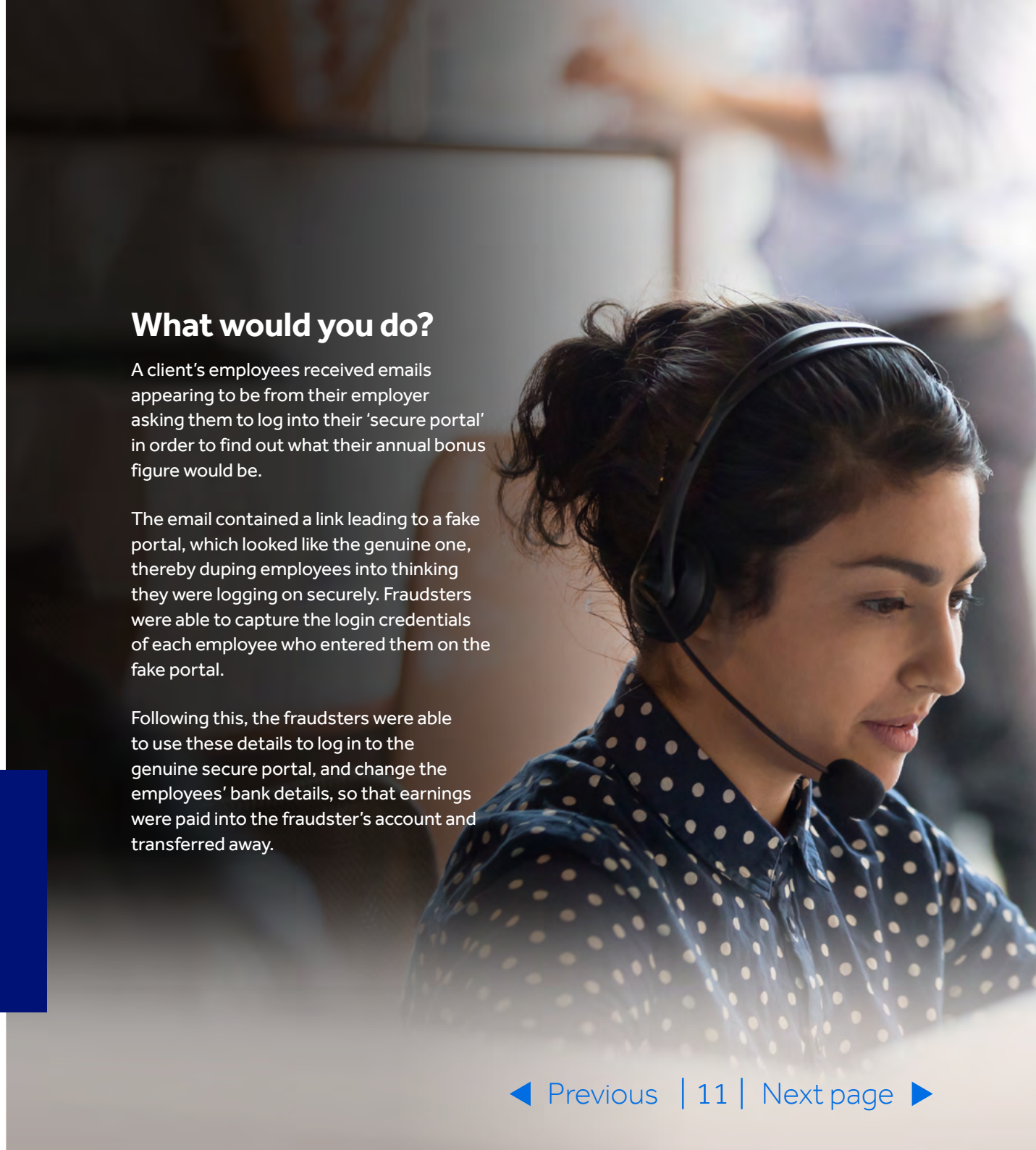
Phishing

Phishing **is a form of social engineering, which involves a fraudster posing as a legitimate source, sending emails that aim to trick people into divulging sensitive information or transferring money into other accounts. The emails typically contain a link to a fake website, which will request that you enter financial information, passwords or other sensitive information.**

Other phishing emails may contain an attachment in the form of a document, form or notification. The email may also be designed to contain and deliver malware via the attachment or a link. If the link is clicked or the attachment opened, the criminal will be able to gain access to your system.

Hackers are relying more and more heavily on the credentials they've stolen via phishing attacks to access sensitive systems and data

Source: Tessian



What would you do?

A client's employees received emails appearing to be from their employer asking them to log into their 'secure portal' in order to find out what their annual bonus figure would be.

The email contained a link leading to a fake portal, which looked like the genuine one, thereby duping employees into thinking they were logging on securely. Fraudsters were able to capture the login credentials of each employee who entered them on the fake portal.

Following this, the fraudsters were able to use these details to log in to the genuine secure portal, and change the employees' bank details, so that earnings were paid into the fraudster's account and transferred away.

Chapter 1: Social engineering

Protecting your company against phishing

- ✓ Be alert to the style, tone and grammar of emails you receive, especially if the email doesn't address you by name (e.g. "Dear Sir/Madam").
- ✓ On sites that require you to input sensitive information, look for 'https' in the website address — the 's' stands for 'secure', though be aware that this does not guarantee the website is genuine.
- ✓ Remember that Barclays may ask you for some information, but will never ask for your full password or PIN, provide you with details to make a payment, or request that you grant them access to your systems or PC.
- ✓ If you receive a suspicious email claiming to be from Barclays, forward it to internetsecurity@barclays.co.uk, then delete it straight away.
- ✓ Make all staff aware of this type of fraud, particularly those that make payments.
- ✗ Never enter any personal or security information on a site accessed through a link in an email.
- ✗ Never click on links or open attachments from senders you are unsure of.
- ✗ Do not assume a sender is genuine because they have information about you/ your company or the email address looks familiar. Fraudsters are skilled in collecting relevant information and can spoof email addresses to make them appear to be from a genuine contact, including someone from your own organisation.

Vishing and smishing

Vishing **(voice phishing) and smishing (SMS phishing) involves fraudsters calling or texting purporting to be from the bank, the police, a supplier or even an internal member of staff.**

They may claim that your account has been compromised, there has been suspicious activity on the account, or that a payment has been made by the business using incorrect bank details.

Caller IDs or numbers on display are relatively easy to change or spoof. Fraudsters have been known to convince people a call is genuine by getting them to cross-check the incoming call number with the official number of the bank, however fraudsters can use technology to spoof numbers which make them appear to be coming from a genuine source.

To make the scam more convincing, fraudsters could also use information about your company, employees or recent activities, using details that they have found online.

Smishing is similar – but is carried out through SMS text message. The text often contains a phone number, which connects you to the fraudster. As with vishing, details can be replicated, so it can seem as if the texts are coming from a legitimate source and they can even be inserted into genuine text communications with the bank.

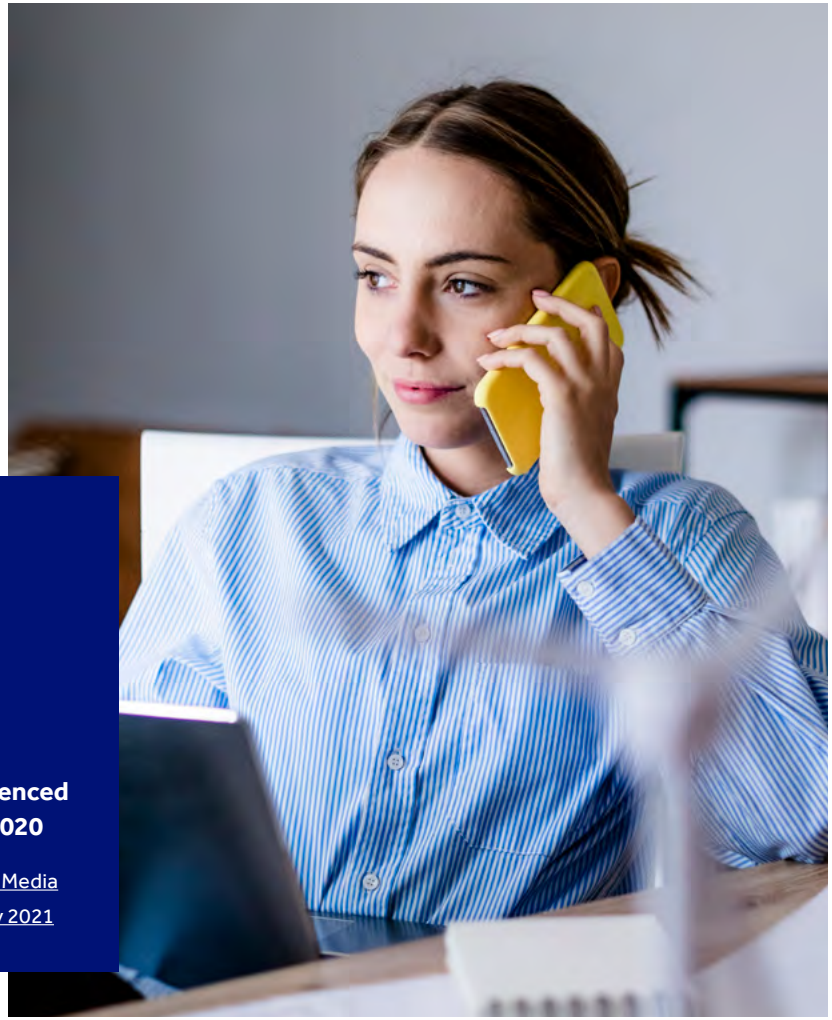
2/5

of businesses and

26%

of charities report having experienced security breaches or attacks in 2020

Source: Department for Digital, Culture, Media & Sport, Cyber Security Breaches Survey 2021



What would you do?

Mark* received a call claiming to be from Barclays. The caller's number appeared on his display as a genuine Barclays number. The caller advised Mark to use the online phone number checker to verify the call was genuinely from Barclays.

The caller told Mark that his account had been accessed from a suspicious location and advised him that he would need to block all of his accounts. They advised Mark that this would need to be done manually and instructed him to send payments with an unusual reference. Nine payments, totalling £156,000, were made by Mark following the instructions from the fraudster.

Barclays' fraud prevention team identified the unusual beneficiary names and references on four of the payments, which were held, and called Mark to ask for further details.

During the call with Mark, it became apparent that he was also on another line to the fraudster impersonating Barclays. Mark was informed of how vishing scams work, and he was advised to hang up on the other caller.

Initially Mark was understandably confused and did not know who to believe. Barclays provided relevant information so that he could independently verify the genuine call and be confident he was speaking to Barclays.

Fortunately, on this occasion this scam was averted due to the unusual reference used and the bank's internal fraud detection systems. But fraudsters have been known to be so convincing that clients have disregarded the bank's advice and demanded that payments are released.

* Names changed to protect anonymity

Chapter 1: Social engineering

Protecting your business against vishing and smishing

- ✓ To check whether or not a caller is genuine, call a trusted and known number for the organisation. Make sure you use a different phone – the fraudster can keep the original line open.
- ✓ Remember that your bank may ask you for some information, but will never ask for your full password or PIN, payment authorisation codes, provide you with details to make a payment, or request that you grant them access to your systems or PC.
- ✓ Make all staff aware of this type of fraud, particularly those that make payments.
- ✗ We will never text clients a link that leads to the online banking login page, or to ask for confirmation of account or security details.
- ✗ Never assume that the caller is genuine because they have information about you, your company, your colleagues, or even if they have the right caller ID. Sophisticated fraudsters are able to collect enough information to seem legitimate and employ advanced technology to mimic real organisations.

Malware

$2.6m

Malware attacks cost companies $2.6m on average

Source: Accenture, 2019

***'Malware',* short for 'malicious software', is used by criminals to disrupt computer operations and access confidential information.**

Malware can be installed into your computer through clicking a link in an email, opening an attachment to an email, or by downloading software from a malicious source.

Many people assume that their IT department's systems will protect them from malware, but it's very important that everyone in an organisation is aware of the risks.

Trojans

Trojan programs are a type of malware that enter your computer on the back of other software. They act as back doors to the computer, granting a fraudster remote access. Once inside your device, a trojan can give a stranger access to your personal details by taking screenshots or capturing keystrokes.

Chapter 2: Malware

When logging into online banking websites, an unexpected screen might appear, delaying you or asking you to repeatedly input data. While you are delayed by these, a fraudster could be setting up another payment elsewhere, waiting for you to unwittingly authorise it by inputting your PIN.

Trojans are hard to detect as they remain passive when not in use. Firewalls and anti-virus software help to defend against trojans but can't guarantee your protection. You should always be cautious of 'pop-ups' on your screen requesting that you put your card into the reader, input your PIN, or allow a download.

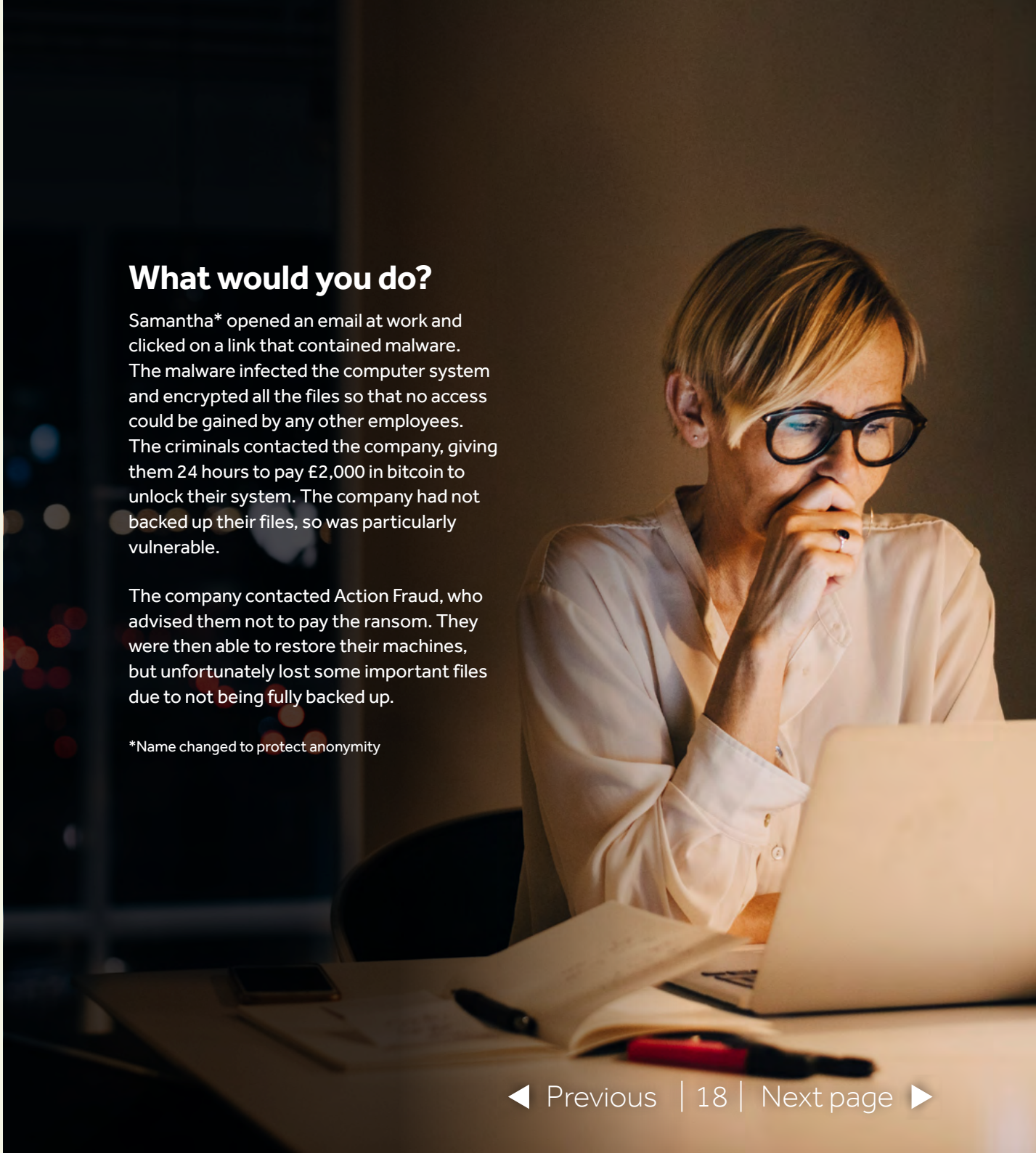
Ransomware
Ransomware enables a fraudster to gain control of your system in order to encrypt your files, demanding a fee to unlock them. Without the decryption code, it is very unlikely that you will be able to access your files again. Though in many cases the criminals will restore files when the ransom is paid, there is no guarantee this will be the case. Hackers have been known to share stolen private customer information free of charge on the web in order to punish a company for not paying their proposed ransom.

Protecting your business against malware

- ✓ Keep your firewalls and security software updated, setting updates to auto where possible.
- ✓ Install the latest updates for your internet browser and operating system.
- ✓ Only download files and software from trustworthy sources.
- ✓ Run regular security scans on your devices. It's important to check that this is functioning as expected, and the data can be accessed when required.
- ✓ Ensure you keep your important files backed up, stored off your network.
- ✓ If your computer does get infected, disconnect from the network straight away and seek professional assistance.
- ✓ Keep employees educated on how to identify phishing emails, and ensure they are aware of the initial steps to take in the event of a ransomware attack, and where to go to report fraud and scams.
- ✗ Be cautious of emails which ask you to follow a website link or open an attachment. Emails containing malware tend to have some urgency to them, pressuring the receiver into clicking a link in order to avoid adverse consequences.

Online banking – do's and don'ts

- ✓ If possible, select dual approval for making transactions, using two separate machines for setting up this authorisation
- ✓ If you notice anything unusual on your online banking screens, abandon your banking session and tell Barclays at once.
- ✗ If you have a smart card, never leave it in the reader connected to your computer
- ✗ Be wary about pop-ups for PINsentry resets when logging into online banking (your PINsentry will never need updating or resetting)
- ✗ Never remake payments to alternative account details if asked to do so
- ✗ Never enter your PIN in order to allow a download
- ✗ Never re-enter your PIN at login or while making a payment.



What would you do?

Samantha* opened an email at work and clicked on a link that contained malware. The malware infected the computer system and encrypted all the files so that no access could be gained by any other employees. The criminals contacted the company, giving them 24 hours to pay £2,000 in bitcoin to unlock their system. The company had not backed up their files, so was particularly vulnerable.

The company contacted Action Fraud, who advised them not to pay the ransom. They were then able to restore their machines, but unfortunately lost some important files due to not being fully backed up.

*Name changed to protect anonymity

Network attacks

As workforces have become more mobile, employees no longer always work on a single trusted network, making security more difficult.

Emails are the main communication method for most companies, yet businesses often forget how unsecure the communications are. An email can be thought of like a postcard – it can be read as it moves across networks.

It is therefore important that sensitive information is only sent over encrypted networks. Secure Sockets Layer (SSL) is the standard security technology for establishing an encrypted link between a web server and a browser.

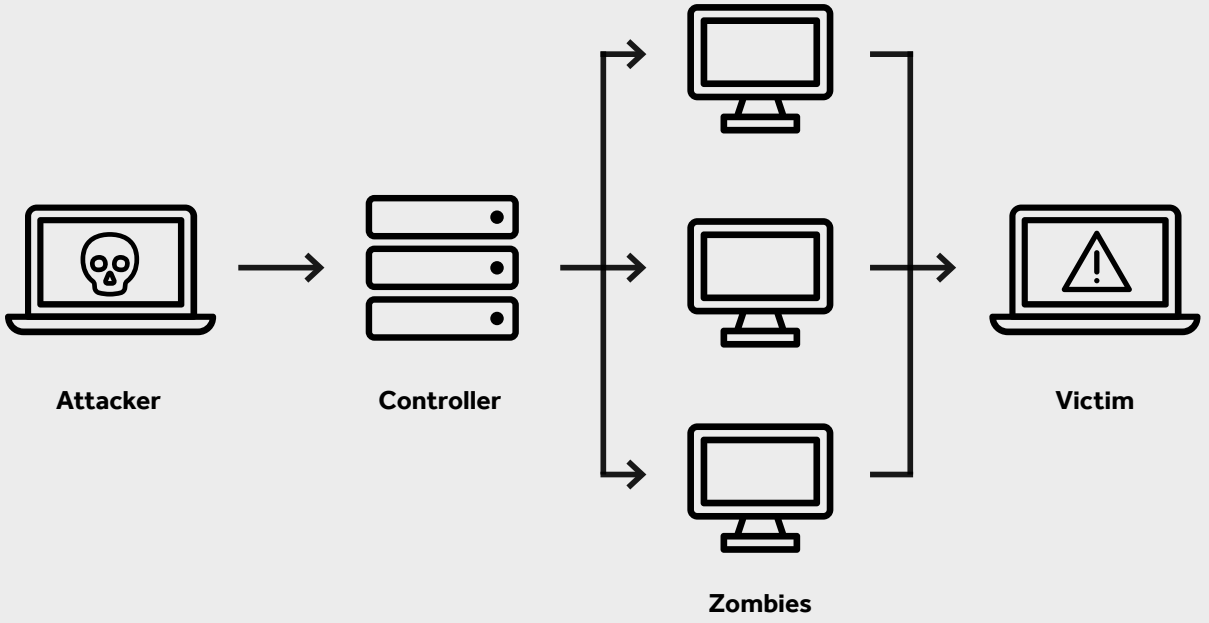
> *"An email can be thought of like a postcard – it can be read as it moves across networks"*

Man-in-the-middle attack

There are various different types of network attack, but all require the exploitation of an unsecured network. Where the network is not encrypted, an unknown third party may intercept communications that are being sent. In a 'Man-in-the-Middle attack', the attacker intercepts the network and watches the transactions between the two parties. They are then able to steal sensitive information, such as account passwords, banking details, or customer data.

A common example of a Man-in-the-Middle attack is 'active eavesdropping'. This is when the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.

Protecting your business against network attacks



Distributed denial-of-service attack

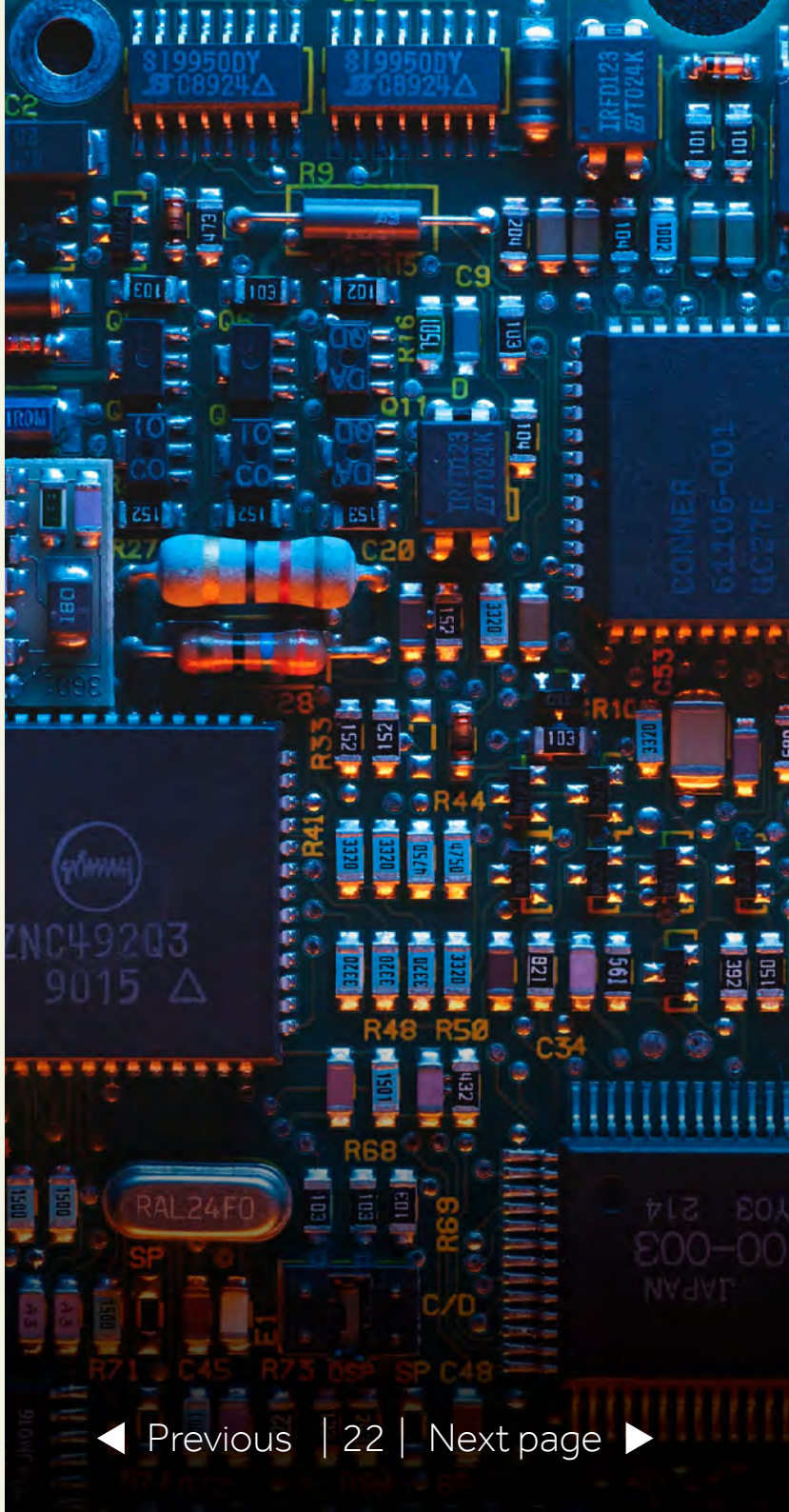
***A Distributed Denial-of-Service attack* (DDoS attack) is when a hacker tries to bombard a website with traffic from multiple sources, causing the site to become overwhelmed and crash. Attackers create a network of infected computers known as botnets by sending and spreading malware through websites, emails and social media.**

Once the malware has been distributed it allows the hacker to launch an attack remotely, sometimes using a botnet of over a million different users, without their knowledge. There are places on the Dark Web where it is possible to buy and sell botnets or individual DDoS attacks. For a small fee, a fraudster can disrupt an organisation's online operations, causing them to lose out on sales and suffer from damage to their reputation.

Chapter 3: Network attacks

Protecting your business against network attacks

- ✓ Use a Virtual Private Network (VPN) for remote access. VPNs add privacy and security to public networks and are used by corporations to protect sensitive data.
- ✓ In the absence of a VPN, avoid unknown public Wi-Fi sources and only use trusted secure connections.
- ✓ Websites should begin with 'https://' – the 's' stands for 'secure', however this only indicates that the link between you and the website owner is secure, and not that the site itself is authentic.
- ✓ Check the address for any subtle misspellings, additional words and characters, and other irregularities.
- ✓ Configure routers to halt more simple attacks by stopping invalid IP addresses.
- ✓ Use intrusion-detection systems (IDS), which can provide some protection against valid protocols being used against you in an attack.
- ✓ Invest in DDoS mitigation appliances, which can help to block illegitimate traffic to your website.
- ✓ Consider buying excess bandwidth that can handle spikes in demand. Alternatively, use an outsourced provider where you can buy services on demand, such as burstable circuits that provide more bandwidth when you require it.



Fraud awareness checklist

Support

Ensure your teams have access to training and support on your financial processes.

Remind

Issue regular reminders to your teams on how to follow important processes, and consider testing these.

Inform

Keep up to date with the latest information and resources – you could follow your bank and Actionfraud on social media to make this easier.

Train

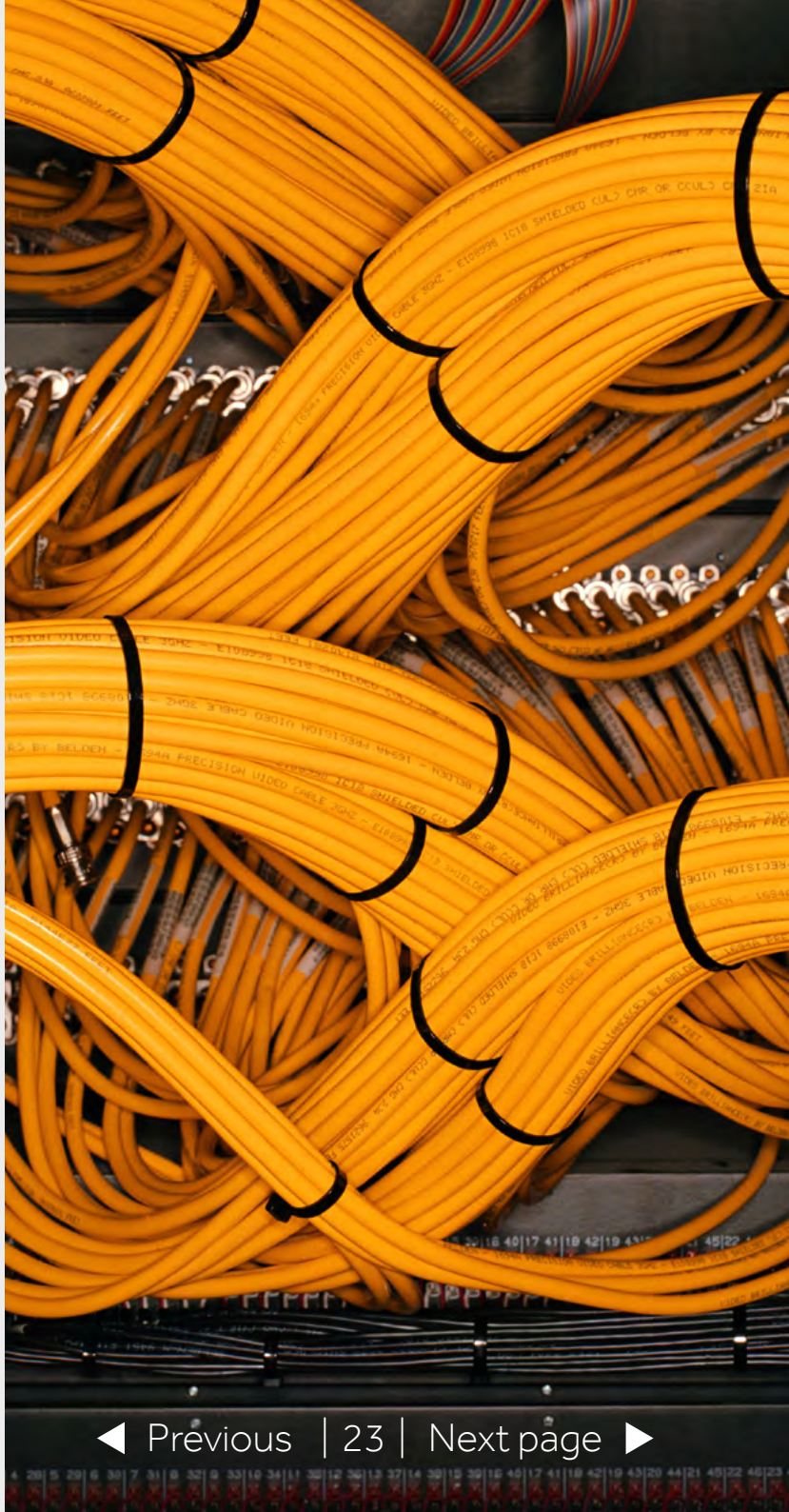
Take advantage of any training opportunities in fraud prevention and ensure that all colleagues are aware of the latest fraud attacks.

Review

Ensure that your internal prevention methods are robust and regularly reviewed.

Protect

Ensure payments requests are input, verified and authorised following adequate internal processes and controls.



Reporting fraud

- If you have any queries, please speak to your Relationship Director and ensure your company is aware of the key reporting contacts and useful links below.
- If you fall victim to fraud where payments have been sent via Barclays.Net, BACS and File Gateway, call the Online Fraud Helpdesk immediately on 0800 056 4890 (if calling from within the UK) or +44 (0) 330 156 0155 (if calling from outside the UK) (both open 24/7).
- To report fraud or any suspicious activity for all other products, including Business Online Banking, call UK Fraud Operations on 0345 050 4585 (open 24/7). To maintain a quality service, we may monitor or record phone calls.
- Fraudulent attacks, even if unsuccessful, should be reported to Action Fraud by calling 0300 123 2040 or visiting actionfraud.police.uk
- If you receive a suspicious email that appears to be from Barclays, please forward it to internetsecurity@barclays.co.uk and then delete it from your email account immediately.

Further resources

- actionfraud.police.uk
- takefive-stopfraud.org.uk
- barclayscorporate.com/fraudawareness
- getsafeonline.org
- gov.uk

Visit our Fraud Protection Hub for more resources to help you educate yourself and your employees.

barclayscorporate.com

@BarclaysCorp

Barclays Corporate Banking

Connecting you to possibility

BARCLAYS

May 2021