THE LITTLE BOOK OF CYBER SCAMS

It gives me great pleasure to introduce to you the latest addition to the Little Book of Big Scams brand. This is the first edition of the Little Book of Cyber Scams. Technology is rapidly evolving and whilst it provides fantastic opportunities to communicate more efficiently and effectively, enhance processes and achieve greater prosperity, it is also open to criminal abuse. This booklet has been developed to assist you to take the necessary steps to defend your business and your customers against cyber criminals.

The Eastern Region Special Operations Unit (ERSOU) Eastern ROCU, together with the forces within the Eastern region have recognised the changing face of business through the online marketplace and just as an office or warehouse requires security against intrusion so too does your presence in the online world.

To pursue online crime, units have been created regionally within ERSOU and all seven forces, it covers – Bedfordshire, Cambridgeshire, Essex, Hertfordshire, Kent, Norfolk and Suffolk. In addition there are now dedicated officers working regionally and locally on protecting victims and seeking to dramatically reduce the chances of you becoming a victim.

I hope that you find this booklet to be both useful and informative. I also hope that it encourages you to protect your business in the online world.

Trevor Rodenhurst
Detective Chief Superintendent
Eastern Region Special Operations Unit
Eastern ROCU

CONTENTS

CYBER SCAMS

INTRODUCTION

Eastern Region Special Operations Unit (ERSOU) Eastern ROCU, together with the forces within the Eastern region – Bedfordshire, Cambridgeshire, Essex, Hertfordshire, Kent, Norfolk and Suffolk are pleased to bring you the Little Book of Cyber Scams reproduced with kind permission of the Metropolitan Police Service's FALCON Protect team.

This booklet has been specifically designed to offer advice to Small and Medium Enterprises (SMEs) on staying safe in the cyber world. SMEs can be found everywhere: on the high street, on industrial estates, online or at home and are vital to the overall success of the British economy.

With limited resources and turbulent economic conditions SMEs may prioritise innovation and growth over online security and risk mitigation. These issues are often seen as expensive, burdensome and time consuming. It is important though that these areas are recognised and assessed and that companies are aware of the risks that they face from cyber criminals.

Whatever business we are in we all rely on the internet. We buy and sell on it, contact our customers on it and use it for logistical support. However with all the opportunities it brings it is important to remember the risks.

Every day thousands of computer systems all over the world are attacked. There are criminals who take advantage of the anonymity of the online world to deceive, hack and steal if the opportunity arises.

If an attack is successful it could have a devastating effect on a business. Reputational damage and financial loss may mean the failure of a company. Theft or loss of data can have a considerable effect on a company's reputation, including a loss in customer confidence, and may lead to significant fines from the Information Commissioner's Office.

PROTECT YOURSELF

This doesn't mean your business should not use the internet. Implementing a few simple security processes and making staff aware of the threats can make a significant difference to your chances of becoming the victim of a cyber criminal.

This booklet aims to identify common types of cybercrime and the ways you can protect yourself from them. It is not an exhaustive list, in what is an ever changing landscape, but by following the advice given you can improve the protection of your systems and the knowledge of your staff that use them.

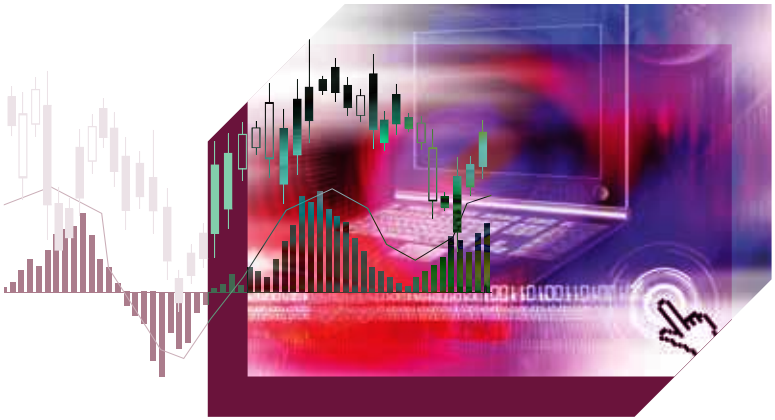
ABOUT 80% OF KNOWN ATTACKS WOULD BE DEFEATED BY EMBEDDING BASIC INFORMATION SECURITY PRACTICES FOR YOUR PEOPLE, PROCESSES AND TECHNOLOGY

Sir Iain Lobban
Director GCHQ, 2014

CURRENT CYBER FRAUD TRENDS

The UK Crime Survey shows for the first time that fraud and cybercrime are the most prevalent crimes committed against people in England and Wales, these statistics underlined that crime in this area is hugely under reported, which is evidenced by the vast difference between the numbers; 600,000 reports to the NFIB and the 248,000 reported to action fraud and the millions noted in the British Crime Survey. There are new measures in place at action fraud to increase reporting and it is anticipated that this will result in an increase to 3.5 million reports annually UK wide. That survey and assessment states there is five times more crime than reported at present.

PWC's Information Security Breaches Survey released in June 2015 reported that 90% of large organisations and 74% of SMEs had suffered a security breach, up from 81% and 60% the year before. Estimates put the costs of these breaches at between £1.46m - £3.14m for large organisation and £75k - £311k for SMEs.



CYBER SCAMS

BUSINESS RISKS

What is at risk?

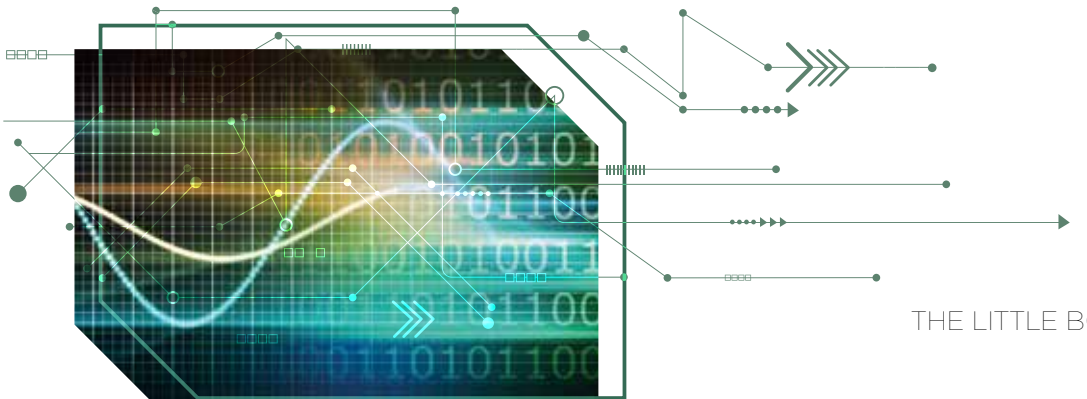
Your money, your reputation, your data, your intellectual property, your IT equipment and IT based services such as websites and payment systems are all at risk from cyber criminals.

Data can take many forms and can include client details or personal information, payment information, product details and confidential company information. There can be a risk to data wherever it is stored whether this is on company IT systems and devices or in the cloud.

An IT breach can be costly both in the cost to fix it and reputational damage. A breach could also lead to funds being stolen or fraudulently transferred from company bank accounts. A loss of data may also incur a significant fine from the Information Commissioner's Office.

Who could pose a threat?

- Criminals looking to steal from you – whether this is data or money. They may also wish to disrupt your systems so your business cannot function normally.
- Competitors wanting to obtain your confidential company data or wanting to disrupt your operations.
- Your own staff. Your employees may have access to a significant amount of confidential data and information held by your company. Disgruntled employees may steal this with the intention of passing it to competitors or to the highest bidder. Staff may also be tricked or 'socially engineered' in to providing confidential information to a cyber criminal.
- Hackers wanting to show off their skills and prove to others that they can breach your security.



CYBERCRIME PREVENTION

Cybercrime – know your business and how to protect it

SMEs face particular difficulty in balancing their cybercrime prevention activities with the resources they have available.

We recognise SMEs can not put profit at risk by implementing unnecessary and expensive 'gold standard' cybercrime control systems. Doing nothing is not an option. Instead we suggest a basic, pragmatic and practical approach.

Firstly, it is important to understand what your valuable data is and to make sure that it is protected.

Where new security issues are identified, implement new or improved procedures and controls to mitigate these problems.

Create a cybercrime prevention culture within your business. Train staff in how to spot cybercrime incidents and what to do if any are identified. Cybercrime prevention training should not be a one off activity and staff should be regularly updated in this area. All new staff should be made aware of any company cybercrime prevention policies and procedures.

Being the victim of a cybercrime incident can lead to a chain of events that can be incredibly disruptive, damaging and costly to your business. If an incident does occur it is also important to have effective plans in place that will help your business recover as quickly as possible.

If you do not have IT staff within your business you may need external help to review and update your systems, policies and procedures. There are numerous resources available to assist with this including IT security companies and websites that offer a wealth of information regarding cyber-crime prevention. Some of these are listed on pages 29 to 32 of this booklet.

Proportionality is key. Make sure the systems and processes you implement are appropriate to the type and size of your business.

Cybercrime types

It is useful to distinguish between the two categories of cybercrime:

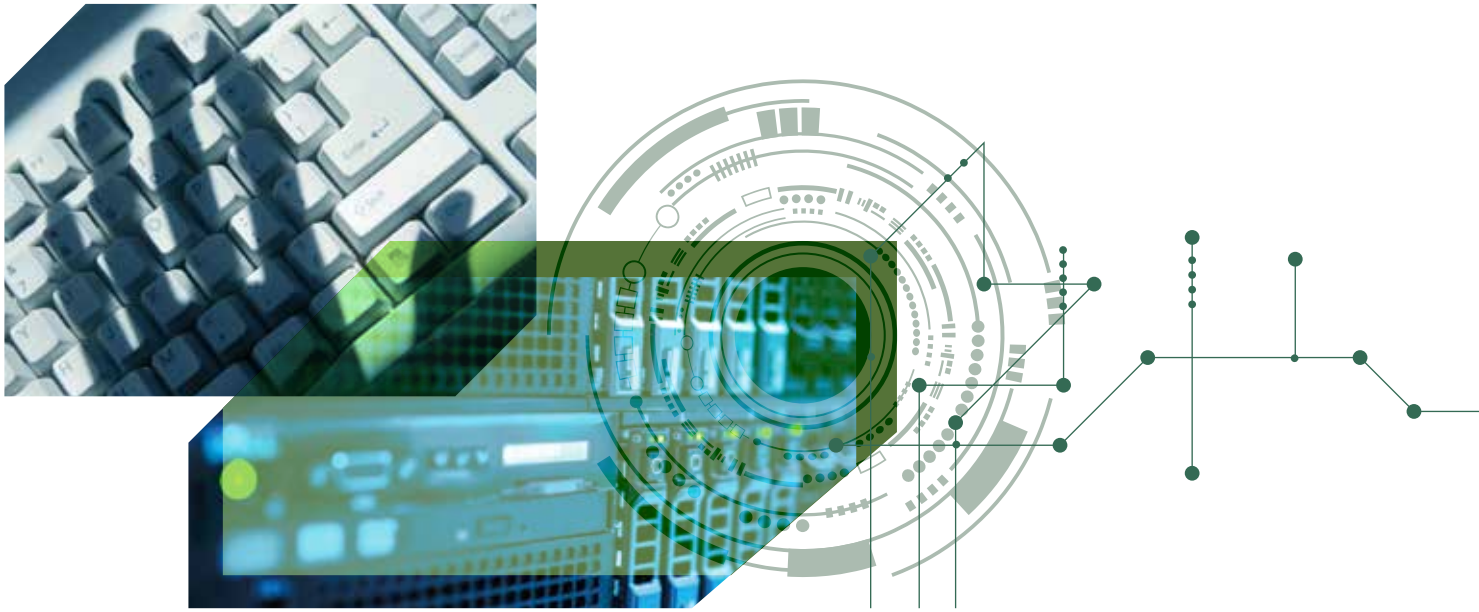
Cyber dependent

Cyber dependent crimes are offences carried out against computers, computer networks, data storage or other devices in violation of the Computer Misuse Act. These crimes involve unlawful access to a computer system or making a system unusable.

Cyber enabled

Cyber enabled crimes are traditional crimes which can be increased in their scale or reach through the use of computers, computer networks or other devices such as mobile phones and tablets.

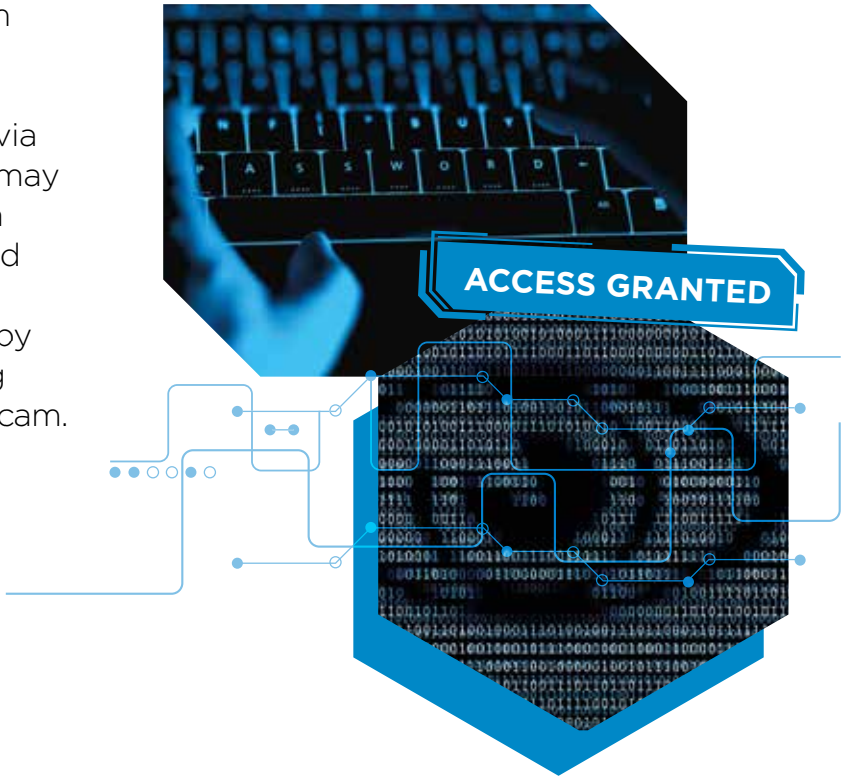
This could be where false or stolen credit card details are used to buy an item online or where a person sends funds to a criminal after receiving a fraudulent email.



CYBER DEPENDENT CRIMES

Prior to the internet, computer and network security was relatively simple as organisations only needed to secure their systems internally. Computers were only connected to others within the company and did not generally talk to other computers outside of their own network. Since the advent of the internet the challenge of securing networked computers has become significantly more difficult.

Cyber dependent crimes rely on the criminal gaining unauthorised access to a computer system or making a system unusable. If a network is connected to the internet it offers the cyber criminal an opportunity to try and gain access via this route. If access is gained a hacker may have the ability to steal or change data held on a network, control devices linked to a network, such as CCTV or printers, or view what a computer user is doing by monitoring keyboard strokes or viewing what is shown on the monitor or a webcam.



Hacking

Hacking occurs when a suspect manages to gain unauthorised access to a computer system.

There are a number of ways in which computer systems can be hacked. These include:

Password attacks

The suspect will use computer programmes that will attempt to guess the password that allows access to a system. The programme will generate passwords based on pre-defined terms and will then use these passwords to try and break in to the system. Given enough time and computing power most passwords can be cracked.

Application attacks

This involves targeting weaknesses in the computer system's applications or programmes. Often new programmes or software have vulnerabilities that can be easily exploited and allow security to be breached.

PROTECTION FROM HACKING

Use a firewall

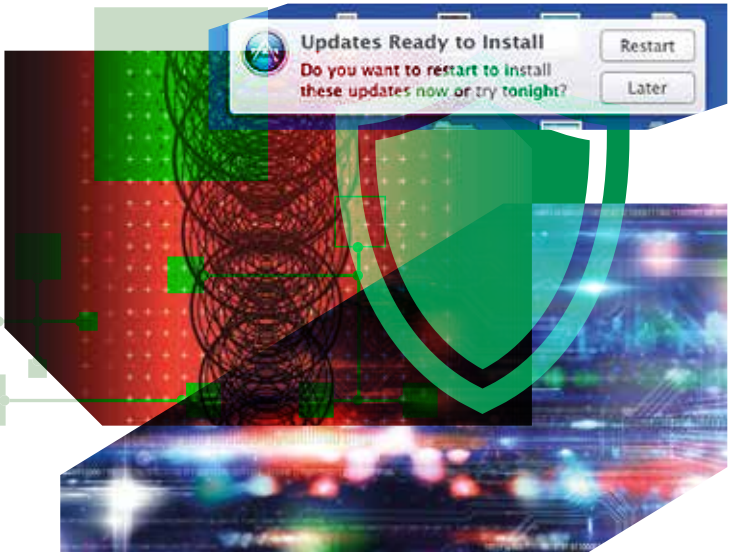
A firewall is designed to protect one computer network from another. They are used between areas of high and low trust, like a private network and the internet. Firewalls offer protection by controlling traffic entering and leaving a network. The firewall does this using a set of filters or rules that are set by the user to allow or block particular types of traffic. A firewall can help protect against hackers accessing your systems if correctly set up.

Encrypt sensitive data

Make sure all important and sensitive data is encrypted so if it is accessed or stolen it cannot be read. Encryption solutions can take many forms and are dependent on what type of data is being encrypted and how the data is being used, stored or transferred.

Keep software updated

It is important to make sure any software on your computers, systems and mobile devices is kept up to date as its designers are constantly updating it to keep it secure as new vulnerabilities are discovered. This is done by downloading updates or 'patches' from the software developer when prompted. This can often be done automatically, but you may have to select this option within the software tools. It is also important to make sure that up to date software is used as older software may be redundant and not have update support. This means that any new vulnerabilities found by cyber criminals will not be fixed leaving the software at risk of attack.



Have strong passwords

Often IT system security is breached because a default password on software or hardware, such as a router, is not changed. It is important that all default passwords are changed as soon as practicable.

There are a number of general rules regarding passwords that will make them more secure:

- Make a password as long as possible, the more characters it has the harder it is to crack.
- Use different types of characters including numbers, symbols and punctuation marks.
- Try not to include dictionary words in your password as this makes them easier to crack. If you are going to use words for ease of remembering, replace a letter with a similar symbol such as an ‘a’ with an ‘@’ or an ‘s’ with a ‘$’.
- Consider using a pass phrase with three random words together such as ‘boatcupdoctor’ or maybe lyrics from a favourite song such as ‘startspreadingthenews’.
- Use different passwords for different accounts. If one password is compromised then at least only one account can be hacked.
- Try to avoid using personal information such as birthdays, favourite sports teams or children/pet names. These can often be discovered by cyber criminals from information you have posted online, so should not be used.

DDoS

A Distributed Denial of Service (DDoS) attack is an attempt to make an internet based service, such as a website, unavailable by overwhelming it with data traffic. Usually this is achieved by sending a flood of simultaneous requests to a server which causes the server to crash as it struggles to respond to more requests than it can handle. These types of attacks are frequently carried out against websites using a network of remotely controlled computers called a botnet. The computers that are part of the botnet have usually been infected with malicious software, (*see page 13*), allowing cyber criminals control of them and the ability to direct traffic at the victim server.

DDoS attacks in themselves do not cause damage to your systems. When the attack stops, your server and attached services should return to normal. Loss of systems though, for whatever time frame, can lead to loss of sales or reputational damage.

DDoS attacks can also be used as a smokescreen to camouflage or draw attention away from other illegal activity an attacker might be committing against a company's systems, such as stealing data from the network.

Most victims of DDoS attacks are high profile organisations such as multinationals, government agencies, banks and other financial institutions. However, no organisation is immune and it is important to be aware that this type of attack can happen.

DDoS extortion

DDoS extortion involves a cyber criminal contacting a business and threatening to subject them to a DDoS attack if they do not pay them a sum of money. These threats are usually made by email and request that funds are paid by the company via a hard to trace route such as Bitcoin.

PROTECTION FROM DDOS ATTACKS

Know the signs of an active attack

Identifying that a DDoS attack is occurring allows for mitigation to be implemented at the earliest opportunity. The following symptoms could indicate a DDoS attack on your network:

- Unusually slow network performance (opening files or accessing websites)
- Unavailability of a particular website
- Inability to access any website
- A dramatic increase in the number of spam emails received

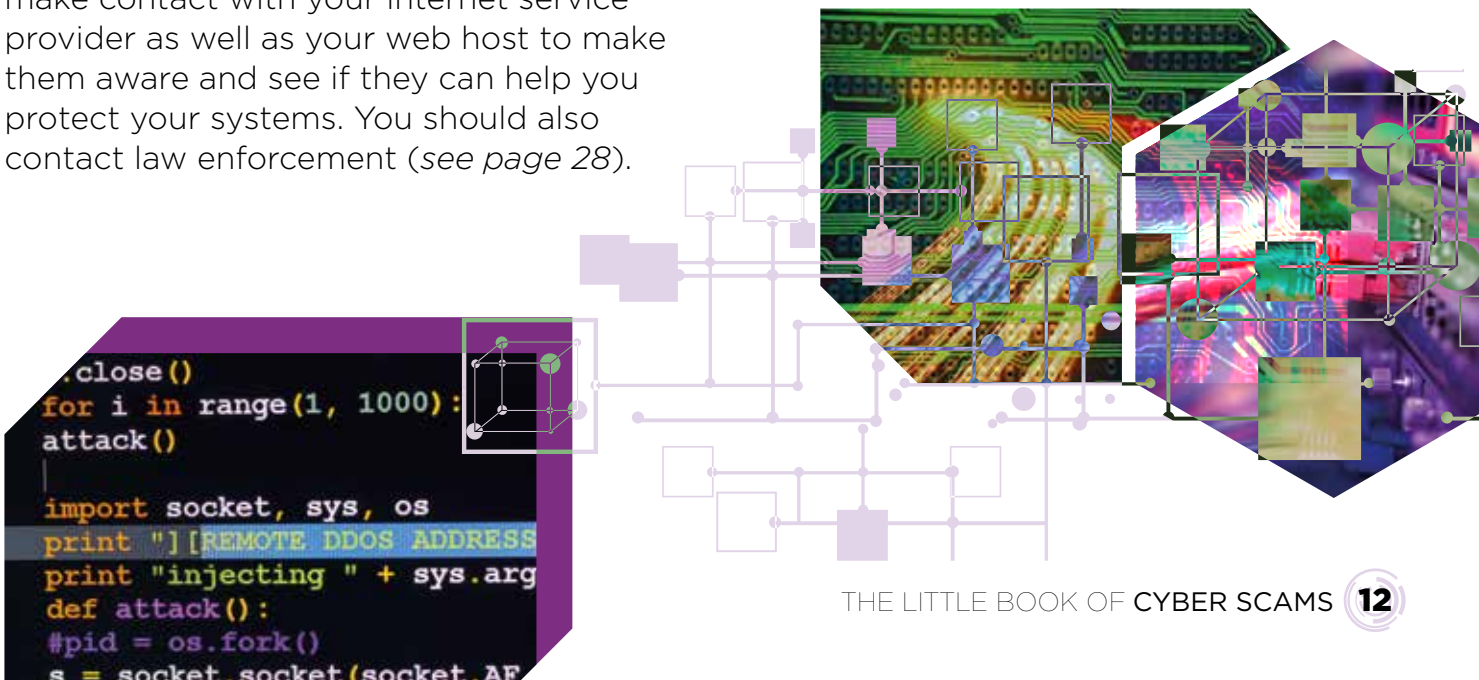
If an active attack is occurring you should make contact with your internet service provider as well as your web host to make them aware and see if they can help you protect your systems. You should also contact law enforcement (*see page 28*).

Invest in DDoS mitigation

There are numerous different DDoS mitigation applications available from various suppliers. These work by analysing data traffic and identifying rogue traffic which is then not allowed to reach the victim server.

DDoS extortion

If you are the victim of a DDoS extortion do not pay any demands. Retain any emails sent by the cyber criminal and report the incident directly to law enforcement (*see page 28*).



CYBER SCAMS

MALWARE

The term malware refers to malicious software. This is software that is designed to gain unauthorised access to computers or other connected devices, disrupt their normal operation or gather information from them.

Malware can infect a computer or network from a number of sources including:

- Contaminated email attachments.
- Infected websites, whether visiting directly or via links shown on emails or social media posts.
- From corrupt files stored on external devices such as laptops, mobile telephones or USB sticks, that are attached to the network.

Common types of malware

Spyware

Spyware is designed to steal information about your activity on a computer or other device. Spyware can perform a number of functions including recording screen shots or logging keystrokes. This enables the criminal to obtain personal information that has been input in to a computer that they can then use themselves, such as internet banking passwords. Remote Access Trojans (RATs) are a type of spyware which allows a cyber criminal to remotely connect to infected devices and control them as if they were the authorised user.

MALWARE CAN INFECT A COMPUTER OR NETWORK FROM A NUMBER OF SOURCES

Ransomware
Ransomware is a form of malware that enables cyber criminals to remotely lock down files on a computer or other connected device. This means that the operator cannot access the locked files on the computer making it unusable. Once the files have been locked the criminal will make contact with the victim and offer to unlock them for a fee, the 'ransom'. Payment is usually requested via a route which is difficult to trace such as Bitcoin.

Virus/Worm
Viruses and worms infect host systems and then spread to infect others. Once on a system, viruses and worms insert copies of themselves into programs, files, and drives. A worm also has the ability to spread onto other computers using the network it is attached to. Worms and viruses can also carry additional "payloads" designed to perform harmful activity on their hosts. This type of malware can cause damage that rapidly becomes widespread. For example worms can enable attackers to create a network of hijacked machines called a botnet which can be used in a distributed denial of service (DDoS) attack, (*see page 11*).

PROTECTING YOURSELF FROM MALWARE

Use antivirus software

Install this software on all computers, mobile devices and servers. It will monitor for malware within the device's memory, processes and storage and alert the user if any is found. Most antivirus software can remove malicious software it has detected and repair damage it may have caused.

It is important to make sure any antivirus software is kept up to date as its designers are constantly improving it as new malware programmes are discovered. This is done by downloading updates or 'patches' from the software designer. Most antivirus software can be set up to do this automatically.

Use a firewall

See page 9 for further information on firewalls.

Back up your data regularly

Make regular backups of important work and data to a separate device, such as a portable hard drive, and check that backups have been successful. Backups should be encrypted and stored in a safe place such as a fire proof safe. If your computer is infected by malware, such as ransomware, it can then be restored using the backup and any locked or lost data can be returned.

Implement device control

Prevent malware from infecting computers by restricting what devices can be connected to them such as smart phones and USB drives. These can carry malware which can transfer to the host computer when they are connected to it. Before connecting any device check it is free from malware.

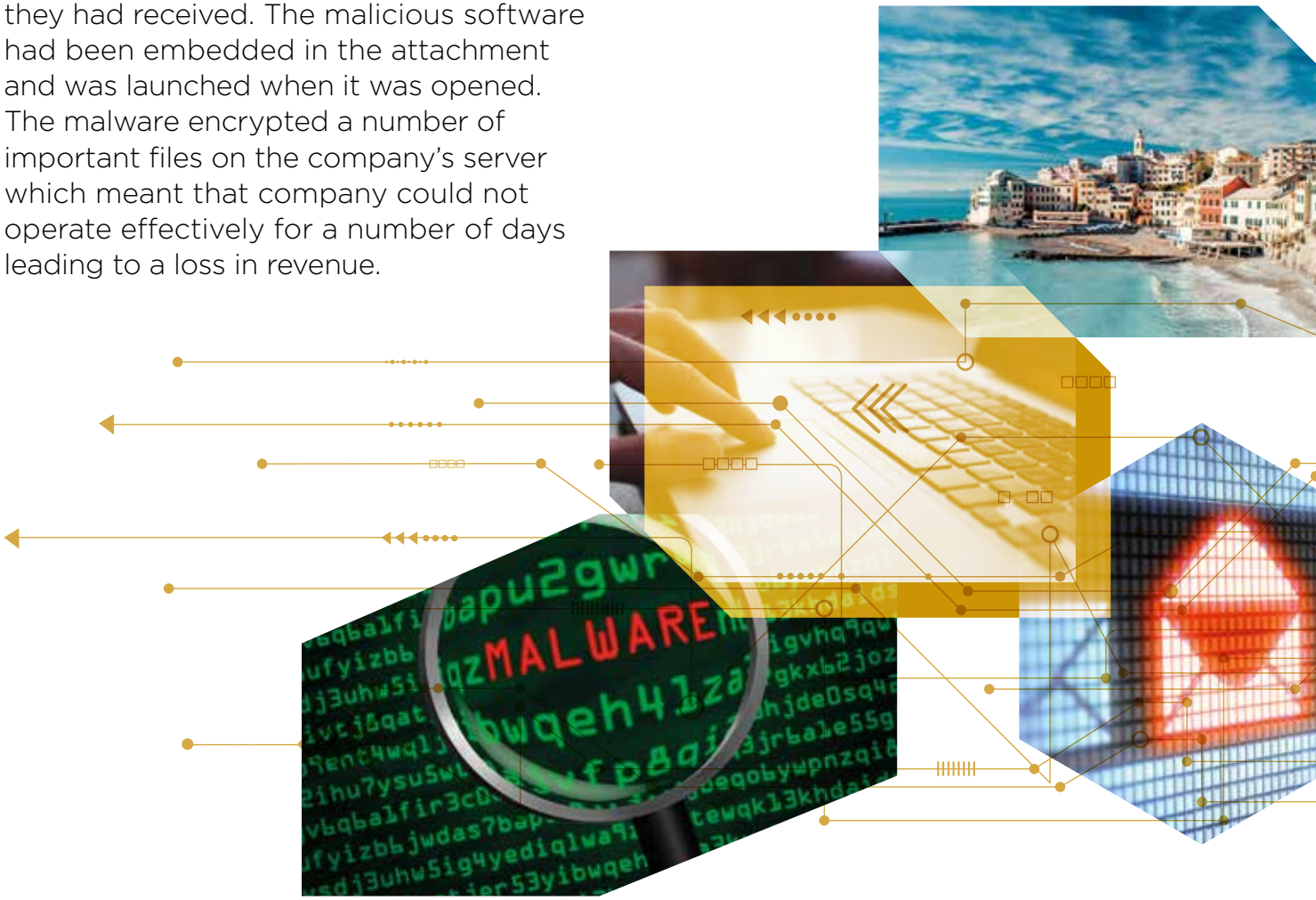
Don't follow links or open attachments in emails unless from a trusted source

Opening links and attachments in emails may allow malicious software to be downloaded on to your system or device. Malware can be concealed in email attachments, including .pdf files or Word documents, or downloaded from a malicious webpage when you connect to it.

CASE STUDY

RANSOMWARE

A small independent travel company was the victim of ransomware after a member of staff opened an attachment in an email they had received. The malicious software had been embedded in the attachment and was launched when it was opened. The malware encrypted a number of important files on the company's server which meant that company could not operate effectively for a number of days leading to a loss in revenue.



CYBER ENABLED CRIMES
SOCIAL ENGINEERING

Social engineering involves a fraudster skilfully manipulating an individual to assist their criminal activity. It may be easier to trick an employee into opening an infected email that places malware on a system than it is to directly hack the system itself. Due to this, social engineering has become more prominent and cyber criminals are finding more audacious ways to get people to undertake tasks, provide information or hand over money using the internet.

Types of social engineering

Phishing

Often cyber criminals will send emails pretending to be someone else to numerous recipients at the same time. The email may claim to come from a bank, online auction site or government department. The aim of the email is to get the recipient to do something they wouldn't usually do or to reveal confidential information to the sender.

By making the email appear to be from a legitimate source the recipient is more likely to reply or take the action requested in the email.

Software is available that can show or 'spoof' an email address in the sender line of an email so it appears the email is from someone that it is not.

The email may also be sent from an email address that is similar to the genuine sender i.e. *@met.p0lice.uk* (the 'o' has been changed to a 'zero') instead of *@met.police.uk*.

Without taking time to check the authenticity of the sender address the recipient may believe the email is from a genuine source.

Often the emails will request login details for internet banking websites. This may be under the guise of security questions to confirm the recipient's identity. Once input, these details can be harvested by the cyber criminal and used to steal from online bank accounts or make purchases from online retailers.

Phishing emails may also contain malware in attachments that you are directed to open, (*see page 13*). The email may also ask you to click on a link which leads you to a fake or malicious websites that can transfer malware to your device or harvest information you input.

Spearphishing

Spearphishing is a more direct form of phishing. Again, the cyber criminals will send an email, but on this occasion it will be targeted at a specific person and the 'sender' is often shown as a person the recipient knows. This may be a work colleague, senior employee or someone from the company IT department. Again, the sender email address is 'spoofed' to appear that it is from a known sender.

The email may also contain other information to make it appear more genuine. This may include details of where the sender is, such as at a conference or on holiday. This information can often be obtained from social media sites. It may also show information about the recipient that has been obtained from the internet such as universities attended or restaurants visited.

95% OF INTERNAL BREACHES ARE CAUSED BY HUMAN ERROR

IBM 2015 Cyber Security Intelligence Index

Spearphishing emails often ask the recipient to complete a specific action, such as, provide bank account details or to input their work computer login details. They may also request that an attached file is opened, or a link is clicked. Opening the attachment or clicking the link may lead to malware being downloaded on to your computer.

Payment fraud

Payment fraud is a specific type of spearphishing which targets businesses with the intention of getting them to transfer money to a bank account operated by the cyber criminal.

There are two main types of payment fraud, CEO fraud and mandate fraud. Both are usually targeted at staff within a company's accounts department and use spoofed sender email addresses.

CEO fraud involves an email that claims to be from a senior member of staff within a company such as a CEO or Finance Director. The email will ask the recipient to make a payment or transfer funds for an ongoing business opportunity or deal. Often the payment request is marked as urgent and pressure is applied to the recipient to make the payment as soon as possible.

Mandate fraud usually involves an email which appears to come from a known supplier. The email will request that future payments for products or services are made to a new bank account, and a reason for the change is provided. The new account will be operated by the cyber criminal and any funds paid in to it will be lost.

PROTECTING YOURSELF FROM SOCIAL ENGINEERING ATTACKS

The best defence against social engineering attacks is staff education and awareness training. By making staff aware of the issue they will be better equipped to combat it. This training should include the following:

How to check the sender email address in an email

Hover the mouse cursor over the email address shown in the sender box. If the email address has been spoofed this should show the email address the message has actually come from. Be aware though this function can be overridden and you may need to check the email header data to confirm the source email address. Viewing this data is different with each email provider and you may need to check with them regarding how to obtain it.

Also check that the email address shown is an organisation's correct email address and has not been spelt incorrectly, such as *@met.p0lice.uk* (the 'o' has been changed to a 'zero') instead of *@met.police.uk'*. Often, phishing emails will be sent from an email account similar to a genuine company email address, for example *police@gmail.com* or *police@yahoo.com,* rather than a genuine corporate account, such as *@met.police.uk*.

This offers the appearance that the email has come from a legitimate sender as the corporate name is shown in the sender email address.

What to do if a request is made to provide bank details, personal information or login details

If a request for this type of information is made, then it should be verified by making contact with the organisation or person making the request using established contact details. Do not make contact using a reply email from the one received and do not reply using any of the contact details, such as phone numbers, shown in the email. If you have no contact details already, contact the organisation using details sourced from an internet search.

How to verify requests for changes to client account information or banking details and requests for one off payments

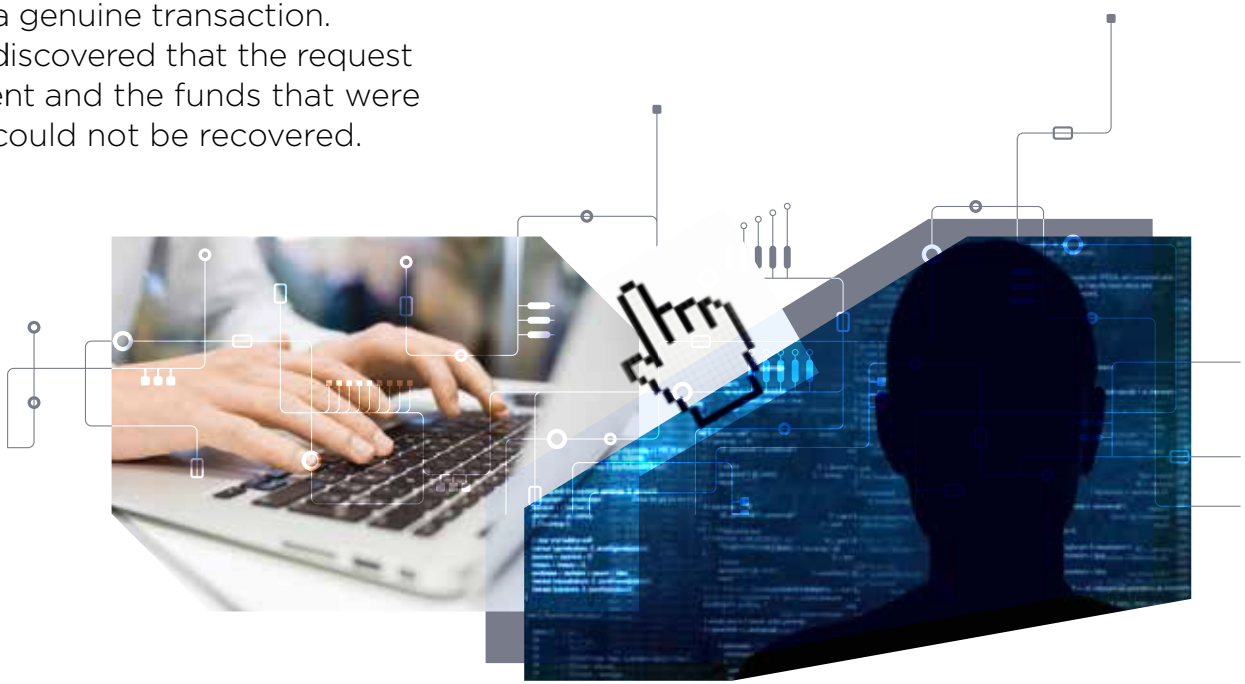
If an email is received requesting a change of bank account for payment, contact information details on an account or a one off payment, verify this by making direct contact with the organisation or person requesting the change using established contact details.

MALICIOUS SOFTWARE

CASE STUDY

The Finance Director of a small HR company received an email they believed was from the company's CEO as their email address was shown in the sender box of the email. The email directed the Finance Director to make a payment into a bank account shown in the email. Believing the request was genuine, the Finance Director transferred £30,000 to the account.
The Finance Director was contacted by the company's bank regarding the transaction, and its authenticity, and confirmed to the bank it was a genuine transaction.
It was later discovered that the request was fraudulent and the funds that were transferred could not be recovered.

Police identified that both the CEO's and Finance Director's business email addresses were shown on the company's website therefore greatly assisting the cyber criminal in creating the spearphishing email. It was also found that by hovering over the email address on the email sent by the criminal the true sender email address could be seen.



CYBER SCAMS

DATA LEAKAGE

The information you post online can be a treasure trove for a cyber criminal. Social media sites are used by millions of people every day and many people have online profiles where a significant amount of information is detailed about them, their employment, education and personal interests.

In the same way a criminal may see from a social media post you are on holiday and burgle your house, a cyber criminal may use a work contact email address or something you have posted online, such as an event you are attending, to assist in a cyber attack against you.

It is very easy for a cyber criminal to create a spearphishing email from the information gained by a simple internet search.

For example, a simple tweet about a visit to a restaurant could be used to create a spearphishing email that appears to come from the restaurant. This email may offer you the opportunity to enter a competition or claim a discount on your next visit by completing a form attached to the email. This form may contain malicious software and on opening it the malware can infect your computer.

SPEARPHISHING

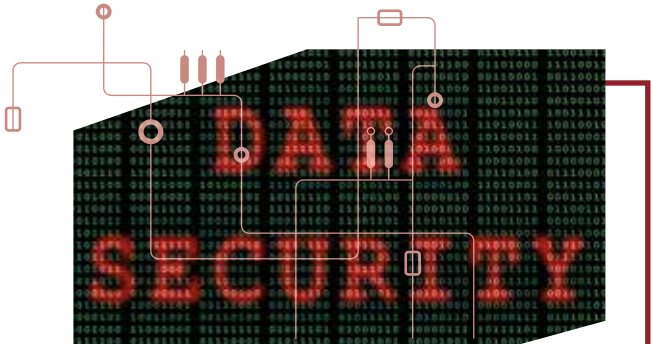
PROTECTING YOURSELF FROM DATA LEAKAGE

Be wary of what you post online

Does the information have to be in the public domain? Particular care should be taken around posting direct business contact email addresses online. These can be used by cyber criminals to create spearphishing emails. A contact@ or info@ email address is often a simple solution.

Know what information can be found about you online

Complete a simple internet search to see what data is available about you. There may be information posted by others that you are not aware of or information you did not know was posted in the public domain. If you are the director of a company a wealth of information is available about you and your business via the Companies House website and other similar websites. If your business is registered at your home address this address will be shown online.



Separate business information from personal information

Do not have personal contact details on business websites and vice versa. Keep work and personal life separate.

Have privacy settings on social media sites

Do not let everyone see everything. Make sure that personal information and details you only want friends or colleagues to see are kept private. To do this have privacy settings on social media sites that restrict who can view your information. Also, be wary of people that want to follow or friend you. Do you know who they really are? Think what interest they may have in you and whether it is appropriate that they see personal information about you.

CYBER SCAMS

WI-FI HOTSPOTS

Publicly available Wi-Fi connections or 'hot spots' can be useful for accessing the internet when you are not at home or your workplace. Not all Wi-Fi connections are secure though, and there are ways in which they can be used by cyber criminals to intercept your data.

Sniffing

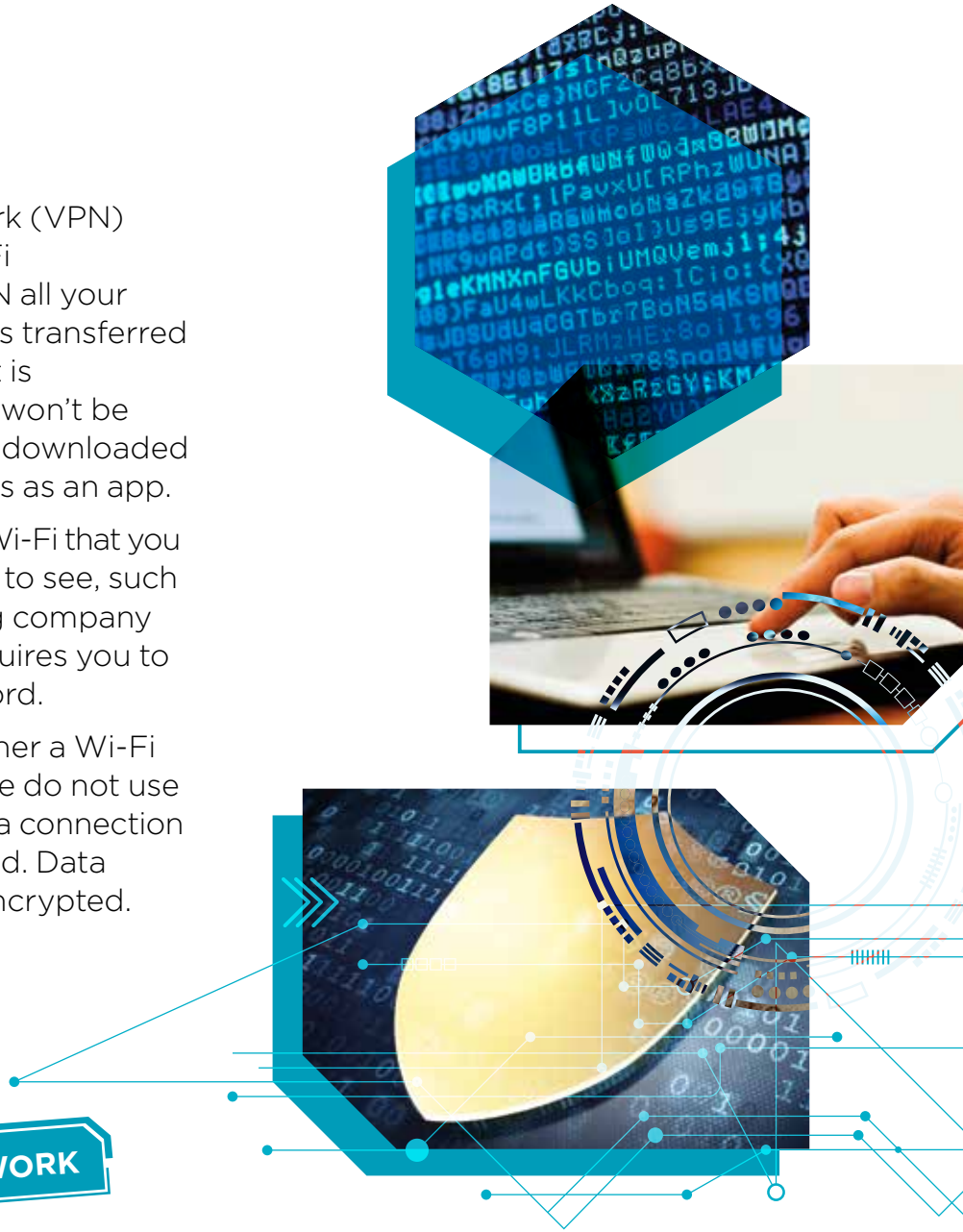
Sniffing is a technique whereby the cyber criminal captures your data as you send it over the Wi-Fi network. By doing this they can steal passwords, login details and sensitive information and then either use it to commit offences against you or sell it on to another party. Even if you are not typing login credentials into your device every time you open an app on a phone, such as an email or social media application, login details are sent across the network and can be intercepted.

Evil Access Points

Cyber criminals can set up their own public hot spots in an attempt to get you to connect to them. First they connect their computer to the internet. They then broadcast their signal as a Wi-Fi connection frequently calling it something like 'free_wifi' or 'coffee_shop_wifi'. Once you connect to the hot spot you are effectively connecting to the criminal's computer and they can capture any data you are sending.

Protect Yourself

- Use a Virtual Private Network (VPN) when accessing public Wi-Fi connections. By using a VPN all your data will be encrypted as it is transferred over the network so that if it is intercepted by anyone they won't be able to read it. VPNs can be downloaded on to phones and computers as an app.
- Don't do anything on public Wi-Fi that you wouldn't want other people to see, such as online banking, accessing company e-mails or anything that requires you to enter a username or password.
- If you are unsure as to whether a Wi-Fi hotspot connection is secure do not use it and use your 3G or 4G data connection to access the internet instead. Data passed over 3G and 4G is encrypted.



VIRTUAL PRIVATE NETWORK

THE FUTURE

The internet has opened up a world of opportunity for business and consumers. It has sped up transactions, simplified processes and created a more convenient interface between business and customers. Many small businesses can now be run using only a laptop from a kitchen table. Technology will continue to improve, but what effect will this have on security?

The internet of things – IOT

With the increase in the number of internet connected devices, such as cars, TVs and fridges, it hasn't taken long for cyber criminals to identify how they can exploit them to commit cybercrime. It has already been identified that groups of cyber criminals have utilised internet bandwidth linked to IOT devices to conduct large scale DDoS attacks. It has also been reported that vehicle software has been hacked with attackers taking over vital functions such as braking and steering.

Escalation of cyber extortion

We expect to see more ransomware and larger ransom demands made against victims, especially when a large business is threatened. As well as using more complex malware to encrypt files we also expect to see an increase in the number of cyber extortion groups and methods of attack. Cyber criminals are already demanding ransoms to halt DDoS attacks, or are approaching businesses with demands for cash after stealing critical data from company networks.

Legislation

The European General Data Protection Regulation (GDPR) comes in to force on May 25th 2018 and will bring into effect a set of rules that anyone processing customer's personal data must abide by. Customers will have more say over what you can do with their data and how it can be used and reporting a data breach will be mandatory. It will also give greater power to regulators to impose significant fines if your business is responsible for losing data, up to 5% of global turnover or €20m. In the event the UK leaves the EU it is likely businesses holding the data of EU citizens will still be expected to comply with this directive if they wish to do business in Europe.

CYBER SCAMS

HOW TO REPORT

Reporting crime, including cybercrime, is important. If you do not tell the authorities, how do they know it has happened and how can they do anything about it? Remember that if you are a victim, however minor, there may be other businesses in a similar position. Your information may form part of one big jigsaw and may be vital to completing the picture and catching the criminals.

Where to report

Report all fraud and cybercrime allegations to Action Fraud either online at www.actionfraud.police.uk

Or by telephone on 0300 123 2040

Unless:

- A crime is in progress or about to be committed.
- There is a locally known suspect or the suspect can be easily identified.
- The crime involves a vulnerable victim.

If this is the case contact police directly on 999, or 101 if not an emergency. You can also report at your local police station.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Help disrupt fraudsters by reporting scam emails that you receive

The Action Fraud website allows you to make reports regarding phishing emails you have received or malware that has affected your computers, systems or devices. Reports of this type are forwarded to the National Fraud Intelligence Bureau run by the City of London Police for collation and analysis. This enables crucial intelligence to be gathered and preventative action to be taken. This activity will seek to disrupt the fraudsters and close down the links between them and victims.

FURTHER ADVICE

Below is a list of websites that you may find useful:

www.actionfraud.police.uk
Action Fraud is the UK's national reporting centre for fraud and cybercrime. If you have been the victim of a cybercrime you should report the incident directly to Action Fraud by telephone or via their website, (*see page 28 for contact details*). The Action Fraud website also has up to date information on numerous types of fraud and cybercrime and details of how to protect yourself when online.

www.cyberaware.gov.uk
Cyber Aware (formerly Cyber Streetwise) provides cyber security advice for small businesses and individuals, such as using strong passwords made up of 'three random words' and always downloading the latest software and app updates, that can help you protect your devices from cyber criminals. Its guidance is based on expert advice from the National Cyber Security Centre, a part of GCHQ.

For more information, visit www.cyberaware.gov.uk

www.ersourocu.org.uk
The Eastern Region Special Operations Unit (ERSOU) website has a 'cyber protect tab'. This provides advice and links to other relevant organisations that can provide guidance and support in protecting yourself online. It also provides the details of your local 'Cyber Protect Officers' who are specialists in cybercrime prevention. To report a cybercrime call 101 for your local Force or call Action Fraud (*details on page 28*).

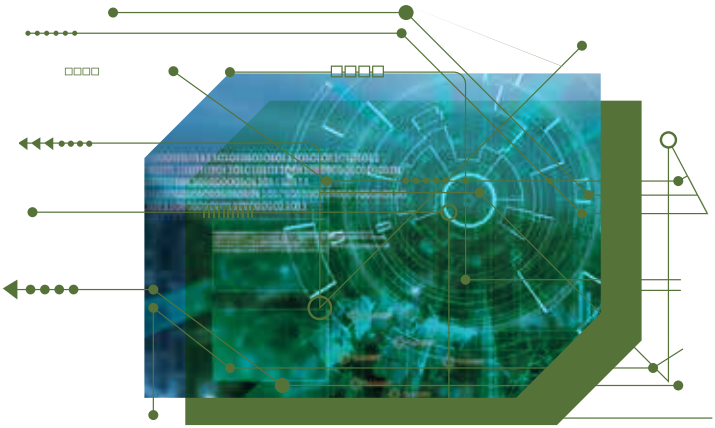
www.financialfraudaction.org.uk
Financial Fraud Action UK Ltd (FFA UK) is responsible for leading the collective fight against fraud in the UK payments industry. Working with its members – who include the major banks, credit, debit and charge card issuers, and card payment acquirers – FFA UK aims to lead the industry's fight against financial fraud to reduce the impact it has both on individuals and companies, and on the industry as a whole. The FFA UK website contains a wealth of information on how you can protect yourself and your business from fraud and cybercrime.

PROTECT YOURSELF

FFA UK have launched Take Five to Stop Fraud which urges people to stop and consider whether the situation is genuine – to stop and think if what they're being told really makes sense.

www.takefive-stopfraud.org.uk

www.fsb.org.uk
The Federation of Small Businesses offers its members a wide range of vital business services including advice, financial expertise, support and a powerful voice in lobbying government. Their mission is to help smaller businesses achieve their ambitions.



www.getsafeonline.org
Get Safe Online is the UK's most popular source of easy-to-understand information about online safety. Their website is a unique resource providing practical advice on how to protect yourself, your business and your family against common types of cybercrime. The website contains guidance on many other related subjects too – including performing backups and data protection.

www.gov.uk/government/policies/cyber-security
This website is an online resource detailing the government's policies with regards to cyber security. It contains a number of reports and policy papers detailing the government's efforts to combat cybercrime along with copies of press releases and cyber security guidance for businesses

www.ico.org.uk
The role of the Information Commissioner's Office is to uphold information rights in the public interest. Their website contains information on how to comply with relevant legislation regarding the management of personal data including protecting personal information and providing access to official information.

CYBER SECURITY

www.nationalcrimeagency.gov.uk
The National Crime Agency (NCA) leads UK law enforcement's fight to cut serious and organised crime. Their website contains information regarding current crime threats and online safety guidance for businesses.

www.ncsc.gov.uk
The National Cyber Security Centre (NCSC) is a part of GCHQ and is the UK's lead authority on cyber security.

The NCSC's main purpose is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. It works with UK organisations, businesses, and individuals to provide authoritative and coherent cyber security advice and cyber incident management, underpinned by world-class research and innovation.

NCSC also provides incident response to minimise harm to the UK, help with recovery and learn lessons for the future.

For more information, visit: www.ncsc.gov.uk

www.nomoreransom.org
The "No More Ransom" website is an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre and private cyber security companies with the goal of helping victims of ransomware retrieve their encrypted data without having to pay the criminals. Since it is much easier to avoid the threat than to fight against it once the system is affected, the project also aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection.

ADDITIONAL SUPPORT

CiSP

The Cyber-security Intelligence Sharing Platform (CiSP) is operated by the NCSC and allows members from across different sectors and organisations to exchange cyber threat information in real time, in a secure and dynamic environment, while operating within a framework that protects the confidentiality of shared information.

The platform contains a number of open and closed forums allowing users with from specific business areas or with particular interests to share information with other like minded users.

For more information, and to join CiSP see:
www.ncsc.gov.uk/cisp

National Cyber Security Centre
a part of GCHQ

CiSP

Cyber Essentials

The Cyber Essentials scheme provides businesses, both small and large, with an accreditation that allows your company to advertise the fact it has met a government endorsed standard of cyber security. By focusing on basic cyber hygiene, companies will be better protected from the most common cyber threats.

Cyber Essentials is for all organisations, of all sizes, and in all sectors. This is not limited to companies in the private sector, but is also applicable to universities, charities, and public sector organisations.

Cyber Essentials is mandatory for central government contracts advertised after 1 October 2014 which involve handling personal information and providing certain ICT products and services.

The Cyber Essentials scheme has been developed in close consultation with industry as part of the UK's National Cyber Security Program.

For more information visit:
www.cyberaware.gov.uk/cyberessentials/

CYBER SCAMS

GLOSSARY

Botnet

A collection of infected computers which can be remotely controlled by a cyber criminal.

Brute force attack

The use of computer programmes to try and identify the password allowing unauthorised access to a system.

Cookies

Files held on your computer containing information about your website usage.

Data loss

The accidental loss of data, not its theft.

Data theft

The deliberate theft of data.

Data leakage

When information about a person or business is published online. This information may be used to construct spearphishing emails.

Distributed Denial of Service attack (DDoS)

An attack launched on a system by a network of computers, called a Botnet, which causes disruption to a computer or website.

Email malware distribution

Malware which is delivered via an attachment in an email.

Exploits

These are designed to take advantage of a flaw or vulnerability in a computer system, typically for malicious purposes such as installing malware.

Hacktivism

This is hacking that takes place for political or social purposes.

MALICIOUS SOFTWARE

Keylogging

This involves the logging of keystrokes on a compromised computer or device.

Malware

This is malicious software which includes spyware, trojans, viruses and worms.

Patches

These are fixes for vulnerabilities found in software, operating systems or applications.

Phishing emails

This is the process of tricking recipients into revealing sensitive information via the sending of fraudulent emails.

Ransomware

This is a type of malware that denies you access to your files or computer until a ransom is paid.

Social engineering

This refers to the manipulating of victims in to disclosing information or completing a task they would not usually do.

Spearphishing

This is targeted phishing often using spoofed email addresses and containing information found from 'data leakage' to add legitimacy to its content.

Spoofing

Email spoofing is when the sender email address is falsified to assist in social engineering. Software available online is used to hide the true sender of an email.

Spyware

This is malicious software that allows cyber criminals to obtain private information without a user's knowledge. It may record keystrokes or what websites have been visited and pass this information to the cyber criminal.

Trojan

Trojans are malicious programmes that appear to be something they are not. This could be a download that states it is a video player when in fact it is malware.

Virus

Viruses are pieces of malicious software that embed into a file and can be spread from one computer to another. They can be particularly harmful and may be used to steal data or take control of a computer – see Botnet.

Vulnerability

These are faults within programmes that can be exploited by cyber criminals to attack computers, systems and mobile devices.

Worm

A worm is a type of virus that exploits a particular vulnerability within a system and uses this to spread itself to other systems.

Zombie

A zombie is a computer that can be remotely controlled by a cyber criminal. It will have been infected with malware and may be used as part of a Botnet.

This booklet has been written and produced by the Metropolitan Police FALCON Cyber Protect team.

To contact your local cyber protect officer please visit the a ‘cyber protect tab’ at **www.ersourocu.org.uk**

FALCON
FRAUD AND LINKED CRIME ONLINE

Eastern Regional Special Operations Unit – Eastern ROCU would like to thank the Metropolitan Police Service's FALCON Protect Team for their time and effort in producing this booklet.