COLMORE BUSINESS DISTRICT GUIDE TO

CYBER SECURITY

OCTOBER 2023

COLMORE BUSINESS DISTRICT

SAFER SPACES

DIGITAL GUIDES

TIPS AND ADVICE DURING CYBER SECURITY AWARENESS MONTH

Welcome

October marks the launch of Cyber Security Awareness Month and we're delighted to be partnering with the West Midlands Cyber Resilience Centre to inform and educate businesses within the BID on how important it is to protect yourself and your organisation from cyber-attacks.

Over the following pages, you'll find helpful tips and advice for protecting your business from cyberattacks. Some of the solutions may seem simple and like common sense, but even these quick fixes can help prevent the devastating and long-term effects of loss or even theft of data.

MICHELE WILBY, CEO, COLMORE BID

Cyber scams are hitting more and more businesses across the UK. They attack all sizes of businesses and all sectors. They want your information and data, as well as your money. Getting the basics right with online security can make you up to 80% cyber safer. This means you are less likely to suffer the devastation of a cyber attack, which could ruin your business and its reputation forever. The West Midlands Cyber Resilience Centre is a Police led, part Home Office funded and not for profit business set up to help businesses across the region become cyber safer. A little prevention work now could save your business from costly damage and disruption in the future.

The second theme is Digital Skills, this focuses on sharing educational resources and activities to teach and inform the public on general Internet security. This theme highlights the importance of being able to understand cyber hygiene and good practices online in order to protect ourselves from personal data loss, cyber bullying, and cyber stalking.

Cyber security is a joint responsibility. If national and international awareness months such as this one can help improve cyber security knowledge and understanding across all sectors, then we should all take the time to utilise the information being shared.

VANESSA EYLES, MANAGING DIRECTOR, WEST MIDLANDS CYBER RESILIENCE CENTRE

TOP 10 cyber security tips for working at home

Colmore Bid and the West Midlands Cyber Resilience Centre have teamed up to help you with some Top 10 cyber security tips for your organisation.

This advice will help businesses to carry out a simple security risk assessment of their cyber security and identify any obvious vulnerabilities.

1 STRONG PASSWORD POLICY

Use a strong password for all devices and social media accounts. Create a strong password using three random words – weak passwords can be hacked in seconds. The longer and more unusual your password is, the stronger it becomes and the harder it is to hack. Save your passwords in your browser – use different passwords for different sites.

Online service providers are constantly updating their software to keep sensitive personal data secure, so store your passwords in your browser when prompted; it's quick, convenient and safer than re-using the same password.

Change default passwords on all your devices when initially installed (especially your Wi-Fi router at home) and consider using password managers to store and protect your passwords

It is highly recommended to have separate passwords for each email account. If any are hacked, you will not compromise data in other accounts.

2 MFA

Turn on the multi-factor authentication setting on all your accounts and devices. It's a free security feature that gives you an extra layer of protection online and stops cyber criminals getting into your accounts – even if they have your password.

3 VPN

Use a Virtual Private Network (VPN) to protect and encrypt the data you send or receive. It will also scan devices for malicious software.

4 SOFTWARE UPDATE

Set all your devices and apps to download and install updates automatically to ensure that any crucial fixes are not missed, and the risk of your devices being infected with malware is reduced. Cyber criminals exploit weaknesses in software and apps to access your sensitive personal data. However

providers are continually working to keep you secure by releasing regular updates that fix weaknesses, so criminals can't access your data. Using the latest versions of software, apps and operating system on your phone and other online devices can immediately improve your security.

5 BACK UP

To safeguard your most important personal data and information, back them up to an external hard drive or cloud-based storage system. If your phone, tablet or laptop is hacked, your sensitive personal data could be lost, damaged or stolen.

6 PHISHING EMAILS

Cyber criminals are targeting people and businesses with fake emails. Phishing emails may appear genuine but are embedded with a virus that could compromise your device, as well as manipulate you into sharing personal or financial information. The National Cyber Security Centre (NCSC) launched the Suspicious Email Reporting Service (SERS), where all potential phishing emails or messages can be sent. To date 142k scams have been taken offline due to the reporting mechanism.

The NCSC has the ability to block the phishing email address, preventing it sending further messages, and work with a host of agencies to remove links to malicious websites.

You can report by forwarding the email to report@phishing.gov.uk

Peter Lagson/Unsplash

7 INSTALL ANTI-VIRUS

Install and activate anti-virus software on all your devices, preferably set it to update automatically. This will help you to run a complete scan of your system and check for any malware infections.

8 SAFE ONLINE BROWSING

Only visit trusted websites especially when online shopping. Keep an eye out for websites that have a padlock sign in the address bar, as this shows that the connection and your personal information (e.g. credit card information) is encrypted and secure.

9 SOCIAL MEDIA

It is important to review the privacy, password and security settings for all your social media accounts to ensure they are as secure as possible.

10 COMMUNICATION

Maintain contact with your team, as it is easy to feel isolated or lose focus when working at home.

The National Cyber Security Centre provides government advice for small and medium businesses, to help you take immediate steps to reduce their cyber risk and improve online defences. For more details, sign up for free to the West Midlands Cyber Resilience Centre who can signpost you to the relevant resources for your sector. **Please click here**.

BOYD

Bring your own device

Companies that either encourage or allow staff to BYOD – bring your own device – for work purposes MUST have a BYOD Policy in place that gives directives on…

- Which staff members are permitted to BYOD
- The systems, applications and access levels such personal devices will be granted
- The employer's rights regarding company data held on personal devices (general access and access/recovery/protection of data when an employee leaves the organisation)
- Arrangements regarding available technical support for personal devices used for work purposes
- Data Security arrangements for such devices (security software, operating system updates, use of Virtual Private Networks or personal Wi-Fi, firewalls, anti-virus, password protocols etc)
- How risks connected with BYOD are to be mitigated and controlled.

The National Cyber Security Centre (NCSC) has some very useful guidance on BYOD which **can be accessed here**.

It is important for businesses to understand the legal implications of BYOD. Legal responsibility for protecting personal information is with the data controller, not the device owner.

Any business considering or already using BYOD are strongly advised to familiarise themselves with the BYOD guidance issued by the Information Commissioner's Office, or ICO for short, regarding the legislation concerning business data, particularly:

- The Data Protection Act (DPA), which states employees must take measures against unauthorised or unlawful processing of personal data
- The Employment Practices Code, which states that employees are entitled to a degree of privacy in the work environment

The ICO guidance document **can be accessed here**.

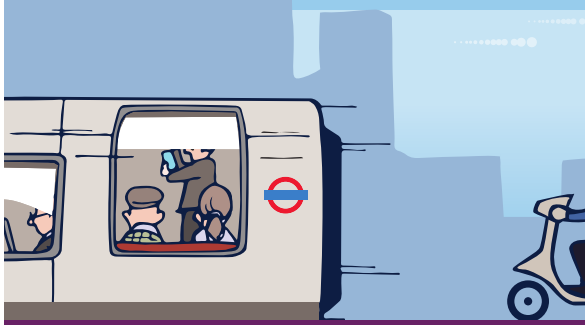
Furthermore, organisations also need to consider how other legal obligations will be met if employees use their own devices for business purposes. For example; organisations will need to consider how any commercial or second party agreements are affected by BYOD, such as their restrictions on using business software on personal devices.

Limit the information shared by devices

Staff are used to sharing their information with other users and in the cloud. The automated backup of device data to cloud based accounts can lead to business data being divulged.

Consider alternative ownership models

Restricted devices may not appeal to some users, so consider giving staff a choice of approved devices which are purchased and controlled by your organisation.



Create effective BYOD policy

Ensure that personally-owned devices are only able to access business data that you are willing to share with authorised staff.

Consider using technical controls

Container applications and technical services such as Mobile Device Management can help you remotely manage personally-owned devices, but they can impact the usability of the device.

Plan for security incidents

When incidents occur, act quickly to limit losses. Could you remotely wipe sensitive data from a personally-owned device if it was lost or stolen?

Encourage staff agreement

Communicate your BYOD policy through staff training so they understand their responsibilities when using personally-owned devices for work purposes.

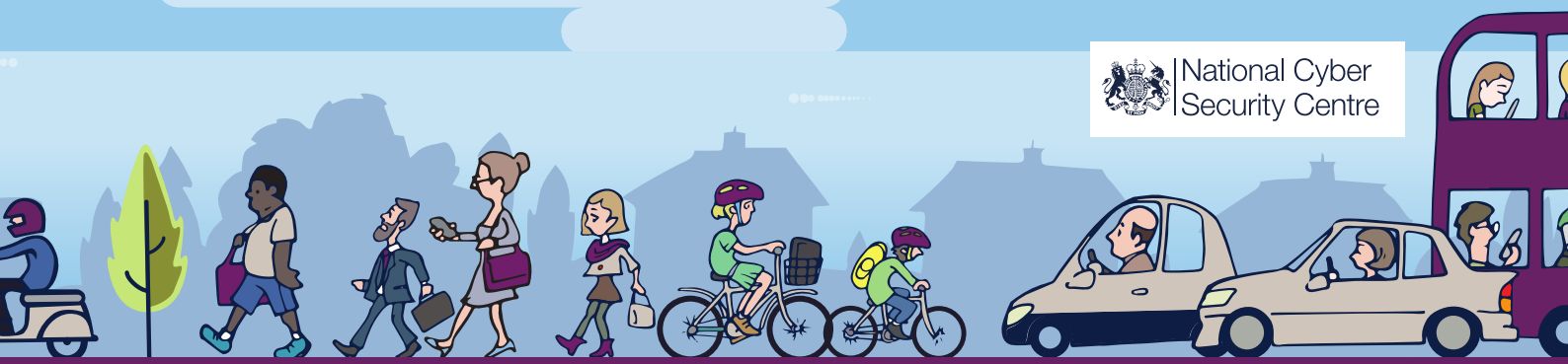
Anticipate increased device support

Your services may need to be accessed by different types of device, so ensure you have the IT support capability and expertise to manage a growing range of devices.

Understand the legal issues

The legal responsibility for protecting other people's personal information is with the data controller, not the device owner.

National Cyber Security Centre



For more information go to www.ncsc.gov.uk @ncsc

Freestocks/Unsplash

CYBER ESSENTIALS CERTIFICATION SCHEME

Cyber Essentials is a UK government scheme supported by the NCSC (National Cyber Security Centre) that helps companies guard against the most common cyber threats and reduce your risk by at least 80%. It also allows you to demonstrate your commitment to cyber security to prospective customers.

Cyber-attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door

to see if it's unlocked. NCSC advice is designed to prevent these attacks.

Cyber Essentials is designed to help organisations of any size demonstrate their commitment to cyber security – while keeping the approach simple, and the costs low.

The scheme's certification process is managed by the IASME Consortium, which licenses certification bodies to carry out Cyber Essentials and Cyber Essentials Plus certifications.

There are two levels of certification: Cyber Essentials and Cyber Essentials Plus.

CYBER ESSENTIALS

A self-assessment option that gives you protection against a wide variety of the most common cyber-attacks. This is important because vulnerability to simple attacks can mark you out as target for more in-depth unwanted attention from cyber criminals and others.

Certification gives you peace of mind that your defences will protect against the vast majority of common cyber-attacks simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place. Cyber Essentials shows you how to address those basics and prevent the most common attacks.

CYBER ESSENTIALS PLUS

Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same, but for Cyber Essentials Plus a hands-on technical verification is carried out. Alternatively you can familiarise yourself with cyber security terminology, gaining enough knowledge to begin securing your IT.

To learn more about Cyber Essentials certification, the IASME accreditation process and the associated costs **please click here**.

CYBER ATTACKS ARE THE DIGITAL EQUIVALENT OF A THIEF TRYING YOUR FRONT DOOR TO SEE IF IT'S UNLOCKED

SO, WHY SHOULD YOU GET CYBER ESSENTIALS?

IN SHORT, CERTIFIED CYBER SECURITY PROVIDES:

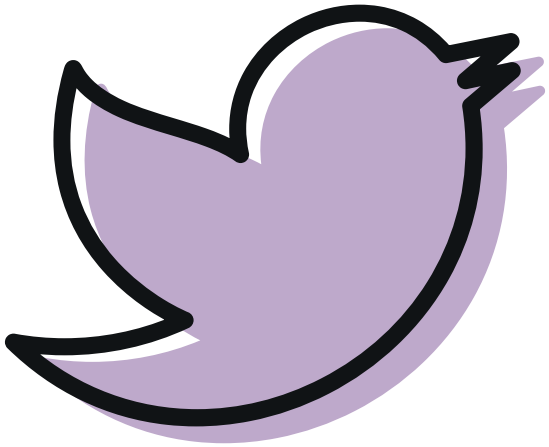
REASSURANCE to customers that you are working to secure your IT against cyber attack

APPEAL to new business with the promise you have cyber security measures in place

You have a **CLEAR PICTURE** of your organisation's cyber security level

ELIGIBILITY to apply for the government contracts that require Cyber Essentials certification

BE SOCIAL BUT BE SAFE with your business



When you are starting or relaunching a business, one of the first things on the 'to do' list is to set up your business social media accounts so you can start telling everyone about your exciting new venture .

Smaller businesses often rely heavily on their social media presence to increase awareness of their brand, sell their services and engage potential customers. It's far cheaper than setting up a website and doesn't require an expert in web design. A few clicks and your business is live for the world to see.

However, social media accounts can also present an opportunity for cyber criminals or even disgruntled ex-employees to damage your business. The National Cyber Security Centre (NCSC) has produced guidance on the potential risks and the steps you can take to try and keep your business social but safe.

MAKE SURE PASSWORDS ARE STORED SECURELY – DO NOT STORE PASSWORDS IN PLAIN TEXT FILES

HOW YOUR BUSINESS SOCIAL MEDIA ACCOUNTS MIGHT BE IMPACTED

- Attempts to spread misinformation or fake news
- Hijacking for malicious purposes, such as redirecting to malicious websites
- Internal staff who have a grudge posting damaging comments
- Draft, incomplete or inaccurate messages being rushed into the public eye

Control access to your business social media accounts

Implementing a sound password process or policy to control access to your business social media accounts can help ensure that only authorised members of staff can publish content.

Even if the other people in your business are friends or family, it's still essential that you protect your passwords to keep your social media accounts as secure as possible.

Most social media products (including social media management tools) contain additional security features such as multi-factor authentication (MFA), so make sure you switch this on. Doing so will protect against attacks on those accounts that are only protected by using passwords.

There may be several people within your business who need access to the social media account, including the ability to publish content.

In such cases the NCSC suggest the following:

- Ensure that account access logging (if available) is switched on. This will provide an audit trail for unauthorised posts, or anomalous access to the account. Use credential protection mechanisms, such as password managers.
- Make sure passwords are stored securely; do not store passwords in plaintext in files, or in shared, unencrypted documents on servers which can be easily accessed by unauthorised persons.
- Avoid sharing passwords, if possible. Where there's a pressing business requirement to share passwords, use additional controls to provide the required oversight. Some password managers allow users to share passwords in a more secure way (for example, they can audit access to the password and automatically sync password changes).
- Using Privileged Access Management (PAM) solutions can further protect the social media accounts, as these can help to secure passwords as well as auditing user access.

MANAGING LEAVERS AND MOVERS

If a member of staff with access to your social media account/s leaves your business (or even changes roles),

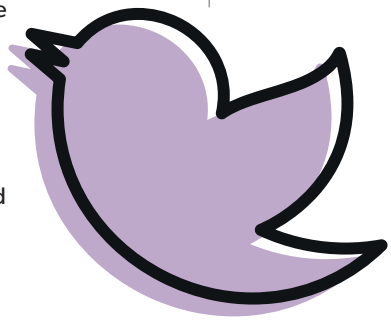
make sure their access to all such accounts is revoked if it's no longer required. This needs to be done promptly – ideally before they move – in case there's any animosity surrounding their departure or move.

Doing this should form part of your organisation's wider process to manage 'joiners, movers and leavers', which should cover managing access to all IT systems (**for more details, tap here**).

If you're using shared passwords, changing these passwords needs to be carefully managed as part of the leavers process.

PUT AN EMERGENCY RECOVERY PLAN IN PLACE

If an employee (or anyone else with authorised access to the account) is publishing damaging content, you'll need to make sure you're able to quickly revoke their access, most likely remotely. This will include managing access to any password vaults or password managers (where used) which contain corporate social media account access credentials.



If your social media channel is hijacked by an attacker, your priority should be regaining control of the account to contain any damage, rather than trying to correct any malicious content that's been posted. Most social media tools provide the means to verify the owner's account(s) using extra identifying information in the case of an account compromise.

Make sure you know how to access this recovery information, and that it's kept up to date. If an attack has also accessed this account recovery information, then the only recourse might be to contact the social media platform owner.

Don't wait until you're in the middle of a real incident before finding what you need to do to regain control. Ensure you know in advance who to contact, and what information you'll need in order to identify yourself to the social media platform owners. For more information about how to recover accounts, refer to the relevant online support pages for your chosen platform or social media management tool.

The full NCSC guidance **can be found here**.

KEEPING UP WITH CYBER THREATS

The Cyber Resilience Centre for the West Midlands is part of the national roll out of Cyber Resilience Centres in the UK which began in 2019. The Cyber Resilience Centre for the West Midlands is designed to support and help protect SMEs and supply chain businesses and third sector organisations in the region against cybercrime.

The WMCRC began its journey in June 2020. Led by **Policing**, and facilitated by **Business Resilience International Management** (BRIM), the centre has followed a structured modular programme based on a highly successful model that had previously been established for over nine years in Scotland.

> WORKING WITH THE POLICE PROVIDES ACCESS TO EMERGING CYBER THREATS

Working with local universities and the police forces in Staffordshire, West Midlands, West Mercia and Warwickshire, provides the centre with access to the latest local as well as national information on emerging cyber threats, criminal trends, best practice for cyber resilience and new technology to provide West Midlands businesses with timely advice to prepare and protect their business, staff and clients from cyber criminals.

The WMCRC also provides affordable testing and training services, with the opportunity to learn how to procure private sector cyber services where needed. Visit **https://www.wmcrc.co.uk/**

Stay up to date with latest advice on cyber threats, news and activity from the West Midlands Cyber Resilience Centre by following us on **LinkedIn** or **Twitter**. Want to receive this directly to your email? **Sign up here for our newsletter**.

THE LATEST SCAMS to be on high alert for

BUSINESS EMAIL COMPROMISE (BEC). WHAT IS IT AND HOW CAN YOU HELP SPOT IT?

In today's digital world, business communication is often done via email. It offers an easy way to quickly communicate and gives you an online trail when it comes to clients/customers, business deals, and more. Unfortunately, email is one of the biggest targets for cybercriminals. One such threat is known as Business Email Compromise (BEC). It's a form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds or revealing sensitive information. Criminals are becoming more sophisticated with how they use BEC so it can be difficult to spot. To help we go over what to look out for and how you can prevent yourself from falling victim to this type of scam.

TAKE A MOMENT TO STOP AND THINK BEFORE PARTING WITH MONEY

HOW ARE BUSINESS EMAIL COMPROMISE ATTACKS CARRIED OUT?

BEC attacks are carried out in several different ways so it's a good idea to familiarise yourself with the different methods so you can spot a potential attack.

EMAIL SPOOFING

This is a pretty common one and one we've all likely seen or experienced in our personal lives. Attackers create fake email addresses that appear to belong to legitimate organisations or executives. They manipulate the "From" field to mimic trusted individuals within the target organisation, making it difficult for recipients to identify the fraudulent nature of the email.

SOCIAL ENGINEERING

BEC attackers often do their research when targeting an individual and then employ a sense of panic, hierarchy, or urgency to get the victim to comply. They'll commonly impersonate executives and employees in order to confuse the victim.

INVOICE FRAUD

Attackers pose as vendors or suppliers and send fraudulent invoices, payment requests, or change of bank details. The invoices look identical to legitimate ones, but the bank account details are altered to divert funds into the attacker's account.

A CAUTIONARY EXAMPLE

To show you these methods in action, we've got a real example of a company falling prey to BEC.

After attackers gained access to an employee's email, they chose a specific customer of the company and set-up redirect rules to send all emails from them to RSS Feeds. They then sent the customer emails requesting a change of bank details, after which they sent invoices, followed by urgent reminders.

The customer they had targeted was a large household name industry supplier. It's likely they targeted them in the hope that the company was so big no one would follow up on this change and instead would just action the invoices.

When carrying out this attack, they were very careful to keep fake details as close to the real company's details as possible. They opened bank accounts in almost the same name, the new details were Company Name Limited whereas the actual company is Company Name, Ltd. The bank even approved the creation of these accounts and wouldn't take action when contacted by the victim.

The only reason the attack was caught is due to the customer ringing the company to confirm that the bank details were changing. Fortunately, this call alerted the company to the attack, but if the customer had actioned the invoices, no one at the company would have been any the wiser.

SO HOW CAN YOU PREVENT THESE ATTACKS?

The above example demonstrates just how easy it is to fall victim to one of these attacks and how you can have no knowledge that it's taking place. Luckily there are steps you can take to ensure this doesn't happen to your own business.

EDUCATE YOUR EMPLOYEES

This is a simple yet vital step in helping to prevent cybercrime from affecting your business. Employees should be trained to identify suspicious emails, verify the authenticity of requests, and report any suspicious activity promptly. Encourage a culture of enquiry and make sure they understand you'd rather anything that doesn't look quite right was double checked.

MAKE SURE YOUR EMAILS ARE SECURE

This is an obvious one but make sure your email security measures are robust. Use measures such as multi-factor authentication, email encryption, and advanced spam filters to prevent attacks.

PUT SECURE PAYMENT PROCESSES IN PLACE

Establish and follow strict payment verification procedures. Employees responsible for processing payments should be required to verify payment requests through a separate channel, such as a phone call using a number held on file, to confirm that anything to do with payments or bank details is legitimate.

LOOK AT THE LANGUAGE USED

Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours'. Attackers will try and encourage you to act in a panic, so you don't have time to look logically at the request, so it's important you pay attention to anything that encourages this.

VERIFY AUTHENTICITY

Verifying the authenticity of customers, suppliers, etc is essential. Take the time to double check email addresses, attackers will often create email addresses that look very similar but will have minor differences. You can also look at the graphics used in emails. Again, attackers will try to make any logos as similar as possible, but they will often lack the same quality, which can be another indicator of a cyber attack. Consider contacting the customers using information already held within your systems you know to be genuine and speaking to the direct.

Joesph Frank/Unsplash

INCIDENT REPORT PLAN

If the worse should happen and you do become a victim of a BEC attack, it's important you have a response plan in place to minimise its impact. This plan should outline the steps to be taken in case of a suspected or confirmed attack, including notifying relevant stakeholders, isolating affected systems, and engaging law enforcement agencies.

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to **www.ncsc.gov.uk** **@ncsc**

FURTHER GUIDANCE:

NATIONAL CYBER SECURITY CENTRE

https://www.ncsc.gov.uk/

COLMORE BUSINESS DISTRICT

2nd Floor, 37a Waterloo Street, Birmingham B2 5TJ
Email: info@colmorebid.co.uk
Tel: 0121 212 1410

Produced for Colmore BID by **Edwin Ellis Creative Media**