



Common online frauds and how to avoid them

KAREN J

NCSC

14 OCTOBER 2020

**CHARITY
FRAUD
AWARENESS
WEEK**

19-23 OCTOBER 2020

Now

MORE THAN EVER...

#CHARITYFRAUDOUT

Common online frauds and how to avoid them

Karen J, NCSC



**46% of all UK businesses
identified at least one breach
or attack in the last year**



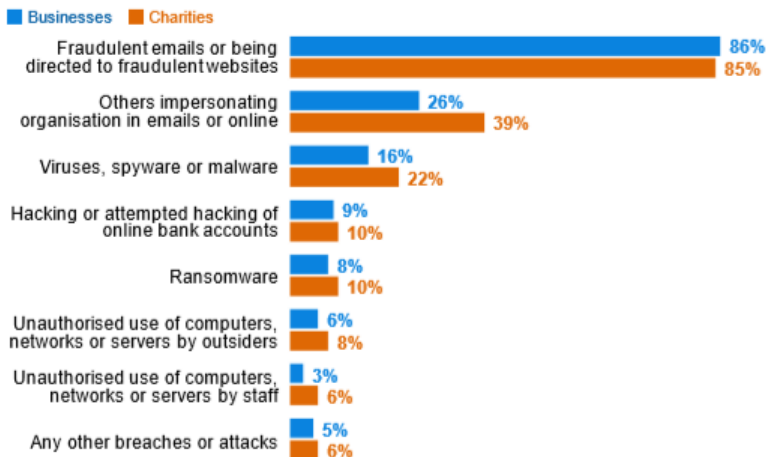
** The Department for Digital, Culture, Media and Sport's 'Cyber Security Breaches Survey 2020' reported that almost half (46%) of all businesses have identified at least one cyber security breach or attack in the last 12 months (and 43% have among micro and small firms)*

Threat Overview

Percentage of organisations that have identified breaches or attacks in the last 12 months



Percentage that have identified the following types of breaches or attacks in the last 12 months, among the organisations that have identified any breaches or attacks



Findings from 2018 report:

The most significant cyber threats that law firms should be aware of are:

1. Phishing
2. Data breaches
3. Ransomware
4. Supply chain compromise



<https://www.ncsc.gov.uk/report/-the-cyber-threat-to-uk-legal-sector--2018-report>

2019 Incident trends

1. Cloud Services
2. Ransomware ✓
3. Phishing ✓
4. Vulnerability scanning
5. Supply chain attacks ✓



<https://www.ncsc.gov.uk/report/incident-trends-report>

Cloud Services



Cloud services, and Office 365 in particular, are an increasingly common target for a range of threat actors.

In some cases, these services are only protected by a username and password.

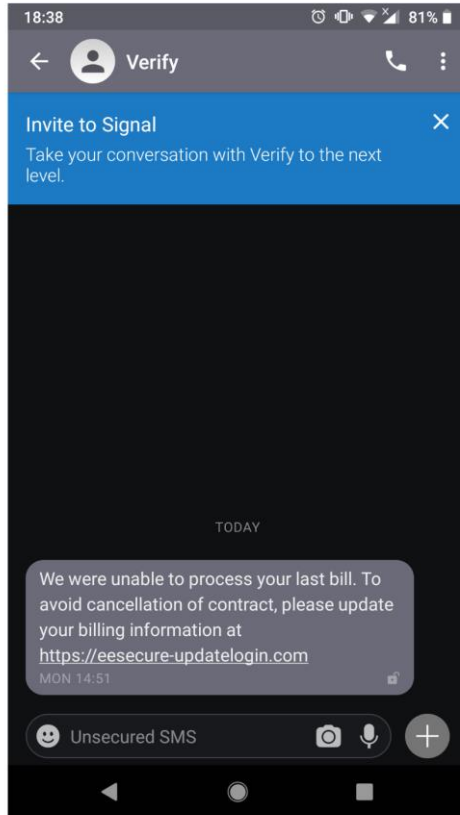
There has been significant use of tools and scripts to try and guess users' passwords. Password spraying and credential stuffing



Newcastle University cyber attack 'to take weeks to fix'

🕒 6 September

Phishing and Vulnerability scanning



Phishing has been the most prevalent attack delivery method seen over the last few years. Common tactics include:

- *targeting Office 365 credentials*
- *sending emails from real, but compromised, email accounts*
- *fake login pages*

- **Vulnerability scanning** remains a common reconnaissance method to identify unpatched, legacy or vulnerable software.



ALERT / 31-01-2020

Fake PayPal emails lead to over £1 million in losses

Action Fraud is warning people selling items online to be on the lookout for fraudsters sending fake PayPal emails.

0
SHARES





NEWS / 24-01-2020

The Amazon Prime scam that has cost victims over £1M

Criminals are continuing to target unsuspecting members of the public using Amazon Prime scam calls.

0
SHARES



COVID 2020

- MORE PEOPLE ARE NOW WORKING FROM HOME
- USING PERSONAL DEVICES
- PROCESSES WERE SET UP QUICKLY IN A HURRY SO THAT DAY TO DAY BUSINESS COULD CONTINUE
- 6 MONTHS LATER...
- CHANGED WORKING PATTERNS FOREVER
- HUGE OPPORTUNITY FOR CYBER CRIME – FURLOUGH OVERPAYMENTS, FURLOUGH ABUSE, TEST AND TRACE SCAMS...



1. Click here for a cure


Message Confidential Cure Solution on Corona virus - Temporary Items

Confidential Cure Solution on Corona virus

CG Tuesday, February 4, 2020 at 10:10 AM
Show Details

Corona virus prevention vaccine and cure medication has been secretly developed by our medical scientist who's names are meant to remain silent for security reasons. We know that the world has been struggling to contain this deadly virus developed and sprayed by wicked scientists to reduce the population of the world so the government will have control over you. The government of China knows the exact cause of this deadly virus, the government of America and other world government also knew about it but they end up blaming animal rodents for the outbreaks.

This corona virus is a weapon created to discredit rivals government health systems or the other way to control the citizens of the world but due to some people like us and our medical teams hate the injustice going in this world. Our secret medical scientist team has developed the cure and prevention to counter this evil act of the world to save lives of innocent people around the world. For those interested to secure their lives kindly reply and get more information about shipping or delivery to you and private distribution.



Dr. Carlos Gemab sent you a free health guideline

[Click for Corona-Virus Cure Review](#)

2. Covid-19 tax refund

New programme against COVID-19



<GOV UK Notify>

 GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a tax refund (rebate) of 128.34 GBP.

[Access your funds now](#)


The funds can be used to protect yourself against COVID-19(<https://www.nhs.uk/conditions/coronavirus-covid-19/> precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

3. Little measure that saves


Message Coronavirus (2019 -nCoV) Safety Measures - Temporary Items

Coronavirus (2019 -nCoV) Safety Measures

 @who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

Show Details

 CoronaVirus_Safety...
1.6 MB

[Download All](#) [Preview All](#)


Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

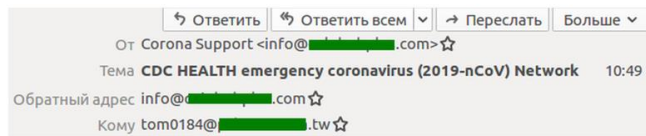
This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

General Internist
Intensive Care Physician
WHO Plague Prevention & Control

Donate here to help the fight...



Dear Sir/Madam

The center for disease control and Prevention (CDC) continues to work to go all out to control an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China, that began in December 2019. Updated list of new case around your city are available at www.cdc.gov/coronavirus/2019.

CDC has established an incident management system to co-ordinate a domestic and international public health response to check mate this virus. Funding of the above project is quite a huge costs and we plead for your good will donation, nothing is too small. From \$10 to any amount

This e-plate form is for timely intervention due to holiday extension of our public Institute/ banks not working, it is really affecting us but together, we must stop the virus! All our research groups have been working round the clock to find a vaccine

Please kindly find our Bitcoin account detail below for your donation and support.

17iiciHtCDFQmEpdmhJ43DtnkGvWgjiXVm

Thanks you for your goodwill contribution in standing against this virus, you are a hero. Please help us share this message to reach as many as possible.

Sincerely

KASPERSKY

The CDC is not asking for donations in Bitcoin




Cyber criminals are preying on fears of COVID-19 and sending scam emails. These may claim to have a cure for the virus, offer a financial reward, or might encourage you to donate. If clicked, you're sent to a dodgy website which could download viruses onto your device, or steal your passwords.

Don't click on any such links. For genuine information about the virus, please use trusted resources such as the **Public Health England** or **NHS** websites.

If you've already clicked, don't panic:

- open your antivirus software and run a full scan, following any instructions
- if you've been tricked into providing your password, you should change your passwords on all your other accounts
- if you're using a work device, contact your IT department and let them know
- if you have lost money, you need to report it as a crime to Action Fraud (you can do this by visiting www.actionfraud.police.uk)

1. Setting up user accounts & accesses



Set strong passwords for user accounts; use NCSC guidance on passwords and review your password policy. Implement two-factor authentication (2FA) where available.


2. Preparing for home working



Think about whether you need new services, or to just **extend** existing services so teams can still collaborate. [NCSC guidance on implementing Software as a Service \(SaaS\)](#) can help you choose and roll out a range of popular services. In addition:

- Consider producing 'How do I?' guides for new services so that your help desk staff aren't overwhelmed with requests for help.
- Devices are more likely to be stolen (or lost) when home working. Ensure devices encrypt data whilst at rest. Most modern devices have encryption built in, but may need to be turned on and configured.
- Use mobile device management (MDM) software to set up devices with a standard configuration in case the device needs to be remotely locked, or have data erased from it.
- Make sure staff know how to report any problems, or raise support calls. This is especially important for security issues.
- Staff feeling more exposed to cyber threats when home working should work through the [NCSC's Top Tips for Staff e-learning package](#).

3. Controlling access to corporate systems



Virtual Private Networks (VPNs) allow home workers to securely access your organisation's IT resources (such as email). If you've not used one before, refer to the [NCSC's VPN Guidance](#), which covers everything from choosing a VPN to the advice you give to staff.

If you already use a VPN, make sure it's fully patched. You may need extra licenses, capacity or bandwidth if you're supporting more home workers.

4. Helping staff to look after devices



Whether using their own device or the organisation's, ensure staff understand the risks of using them outside the office. When not in use, staff should keep devices somewhere safe.

Make sure they know what to do (and who to call) if devices are lost or stolen. Encourage users to report any losses as soon as they can.

Ensure staff understand how to keep software and devices up-to-date, and that they apply updates promptly.

5. Using removable media safely



USB drives may contain sensitive data, are easily lost, and can introduce malware into your systems. To reduce the likelihood of infection you can:

- disable removable media using MDM settings
- use antivirus tools where appropriate
- only permit the use of sanctioned products
- protect data at rest (encrypt) on removable media
- encourage alternative means of file transfer (such as online tools).



Moving online

Questions to ask your IT providers

COVID-19 has seen many organisations shutter their physical premises and move their business online. Establishing the IT services to support this transition can seem like quite a challenge. This guidance will help you determine how ready your business is, and point the way to any new cyber security measures you should put in place.



Dealing with new ways of working

Moving your business online will present some new risks, placing more reliance on digital technologies such as web hosting, credit card processing, and productivity tools like email, video and chat.

You shouldn't need a degree in computer science to run your small business securely. But, cyber security is complicated. If you don't have all the IT skills yourself, it can be hard to know what to do - and when you've done enough.

Having good relationship with your IT service provider(s) will help massively with this. So we've identified and explained the key cyber security topics we think you should care about, so you can be sure you're covering all the right bases.

1. Assess the cyber security of your business



Consider if the measures you take to deal with the lockdown will become more permanent ways of working. For example, will you look to expand your online business? If so, you'll need systems which are sustainable and can scale as your business adapts and grows.

2. Establish a baseline



Answering the questions below will give you a good idea of your security status, and identify what areas need attention. The NCSC's **Cyber Essentials** scheme provides a way to demonstrate to others that you have good security in place.



What IT products and services do you use? Is it your job to look after these, or a service provider's?



Some insurance policies now include a basic level of **cover for cyber risks**. This can be useful if you suffer an incident. Review your policies to understand the level and type of cover (if any) that is provided.



Are you using cloud services? The **NCSC's cloud guidance** can help you choose secure products, and use them safely.



Do you have access to IT support? As you become more reliant on digital services, think about how you'd cope if these were unavailable.



Are there any regulations you need to follow? If your business is now processing **Personally Identifiable Information (PII)** online, you will need to read up on GDPR. If you are processing card payment information, the Payment Card Industry Data Security Standard will apply.

3. Talking to your IT service providers



If you are talking directly with your supplier, the following questions will help you ensure that security is at the forefront of any new service you decide to take on.



Patching & Updates: Ask your suppliers how often they patch the services you use, and check any contracts or SLAs to ensure that patching is included.



Backups: What sort of backup arrangements are in place and how often are these tested? You should know how often your data is backed up, where it is stored, and who has access to it.



Access: Is your data (and the data of others which you have responsibility for) being properly protected? Are you able to put 2FA in place to limit access to your data and services?



Logs: Are logs being kept for security purposes? Logging can play a vital role in diagnosing any problems. Logs will also prove invaluable when responding to and recovering from security incidents.



Incident Response: What will happen if things go wrong? Service providers should operate on the presumption that they will be attacked. It should be clear how and when they will engage with you during a security incident.

Find out more

For more information about how to improve cyber security within your organisation, please read the NCSC web pages especially for small businesses at www.ncsc.gov.uk/smallbusiness.

Video conferencing services: security guidance for organisations



Cyber Security Small Business Guide

Backing up your data

Take regular backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.
- **Ensure the device containing your backup is not permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at www.ncsc.gov.uk/smallbusiness

- Configure devices so that when lost or stolen they can be **tracked, remotely wiped or remotely locked**.
- Keep your **devices** (and all **installed apps**) **up to date**, using the **'automatically update'** option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots – **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.

- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords – when implemented correctly – are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- **If you forget your password** (or you think someone else knows it), tell your IT department as soon as you can.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with their device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager**, but only for your less important websites and accounts where there would be no real permanent damage if the password was stolen.

Create a separate password for your email

Your personal email account contains lots of important information about you and is the gateway to all your other online accounts.

If your email account is hacked all your other passwords can be reset, so use a strong password that is different to all the other ones you use.

Visit [cyberware.gov.uk](https://www.cyberware.gov.uk) for advice on how to reset your email password.

Create a strong password using three random words

Weak passwords can be hacked in seconds. The longer it is, the stronger it becomes and the harder it to hack. Make yours strong by using a sequence of three words.

You can make it even stronger with special characters, so 'FlamingoHeadMan' could be '42@FlamingoHeadMan'.

Starting with your most important accounts (such as banking, email and social media), replace your old passwords with new ones, by stringing three random words together.

Visit [cyberware.gov.uk](https://www.cyberware.gov.uk) for more advice on how to create a strong password

Save your passwords in your browser

Using the same password all over the internet makes you vulnerable – if that one password is stolen all your accounts can be accessed.

It's good practice to use different passwords for the accounts you most care about. Remembering lots of passwords can be difficult, but if you save them in your browser you don't have to.

Online service providers are constantly updating their software to keep your 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 for all your accounts.

Visit [cyberaware.gov.uk](https://www.cyberaware.gov.uk) for advice on how to save passwords in your browser.

Turn on two-factor authentication

Two-factor authentication (2FA) is 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.

It reduces the risk by asking you to provide a second factor, such as getting a text or code when you log in, to check you are who you say you are.

Check if the online services and apps you use offer 2FA. If they do, turn it on. Start with accounts you care most about such as banking, email and social media.

Visit [cyberaware.gov.uk](https://www.cyberaware.gov.uk) for advice on how to turn on 2FA.

Update your devices

Cyber criminals exploit weaknesses in software and apps to access your sensitive personal data, but manufacturers are continually working to keep you secure by releasing regular updates.

Using the latest software, apps and operating system on your phone or tablet can fix bugs and immediately improve your security.

Update regularly or set your phone, or tablet, to automatically update so you don't have to think about it.

Visit [cyberaware.gov.uk](https://www.cyberaware.gov.uk) for advice on how to turn on automatic updates.

Turn on back up

If your device is compromised by a cyber criminal your sensitive personal data can be lost, damaged or stolen.

Keep a copy of all your important information by backing it up.

You can choose to back up all your data or only information that is important to you.

Visit [cyberaware.gov.uk](https://www.cyberaware.gov.uk) for advice on how to turn on automatic back up on your device.

Products & Services



NCSC Website



Small Business Guide



10 Steps



Cyber Essentials (Plus)



Trust Groups



Top Tips for Staff



Board Toolkit



Sector Specific Toolkit



Response & Recovery Small Business Guide



Sector Specific Assessment

Exercise in a Box



Themes:

- Preventing malware damage
- Backing up your data
- Avoiding phishing attacks
- Using passwords to protect your data
- Keeping your smartphones and tablets safe.

Scenarios:

- Phishing leading to ransomware
- Mobile phone theft and response
- Insider threat Leading to a Data Breach
- Third party software compromise
- BYOD
- Threatened leak of sensitive data
- Unknown Wi-Fi attack
- Supply Chain Risks
- Home & Remote Working
- Technical Scenario



Choose exercises

Think about what aspects of cyber threat management you'd like to explore. Each exercise gives an indication of the level of detail covered from the five management steps listed in the [cyber security small business guide](#).

As a minimum, your organisation should feel confident it adequately covers those five steps. They can be achieved at relatively low cost and provide the foundation to good cyber security management.

Discussion based exercises

Select

A phishing attack that leads to a ransomware infection

Understand how well you are protected against phishing emails, and how you could recover from a ransomware infection.

- Preventing malware damage
- Avoiding phishing attacks
- Backing up your data

Time needed with participants

60 - 90 mins

▶ [Resources needed to run the exercise](#)

Mobile phone theft and response

Explore how you would be protected from a thief who steals a mobile phone and tries to use it to extract confidential

Rockies Telecoms Company

[Edit profile](#)

Useful Resources

[Getting started with Exercise in a Box](#)

[Beginner's guide to exercises](#)

[Glossary](#)

[Be a part of Research](#)

[Contact Us](#)

NCSC guides

[Small Business Guide](#)

A cyber security guide for small businesses

[Small Business Guide: Response and Recovery](#)

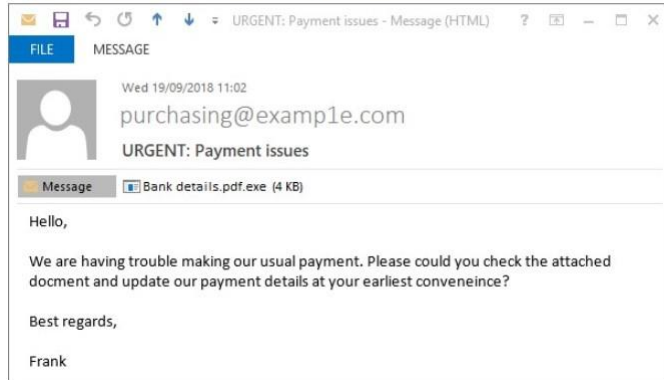
Guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident

[Cyber Essentials](#)

A certification scheme that



Inject 1 – Email received by Finance



A phishing attack that leads to a ransomware infection

Inject 1

Your finance team have received an email from a customer stating they've attempted to make a payment but are having trouble. The email comes from a different address than the customer typically uses, containing only a slight misspelling of the customer's name. A file is attached, and the message requests that the finance team open it to help the customer in making their payment.

- Discussion point 1
 - What mechanisms does your organisation have in place to make it difficult for attackers to reach your users?
- Discussion point 2
- Discussion point 3
- Discussion point 4

Previous Step Inject 1 Step 2 of 13 Next Step

This information is exempt under the freedom of Information Act 2000(FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown copyright ©.



A phishing attack that leads to a ransomware infection

Executive summary

Rockies Telecoms Company ran a cyber exercise session on 27th August 2020 using the NCSC's Exercise in a Box tool. This report summarises the results of this exercise, and includes recommendations for your organisation to consider.

The exercise was run in order to ascertain your organisational understanding of dealing with a potential cyber threat.

Team statements

We make it difficult for attackers to reach our users with phishing emails. - **Somewhat confident**

We provide clear training to allow our users to identify and report suspected phishing attacks. - **Slightly confident**

We effectively detect and prevent viruses and malware running on our organisations IT. - **Not at all confident**

We have a clear policy for keeping our organisation's software current and always apply the latest security updates. - **Somewhat confident**

We place appropriate limits on the software that can be installed or run on our organisations IT. - **Slightly confident**

If we lost access to our business-critical data, we could recover from our backups without significant disruption. - **Fairly confident**

We have a clear and consistent approach for communication with staff, media and stakeholders during an incident. - **Fairly confident**

Awareness and opportunities

Knowledge

* Understanding roles and responsibilities. * Need for good communications internally and externally. * We've learned we need procedures in place for business continuity

New understanding

* That we need better and regular user training to identify threats

Opportunities

* Standard system builds where possible with lowest level of privilege. * Consistent and clear communications plan for future inc

Related guidance

[Small Business Guide](#) – How to improve cyber security within your organisation - quickly, easily and at low cost.

[Small Business Guide: Response and Recovery](#) Guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident

[Mitigating Malware](#) – This guidance describes how organisations of all sizes - and home users - can reduce the likelihood of being infected by malware.

[Review Phishing](#) guidance information on how to defend your organisation from email phishing attacks.

[Review the NCSC protecting your organisation from ransomware](#) guidance to understand how to prevent a ransomware attack, and what to do if your organisation is infected by ransomware.

The concept of 'least privilege' is covered in [NCSC's Managing user privileges](#) which forms part of the NCSC's '10 Steps To Cyber Security' concerns.

This information is exempt under the freedom of Information Act 2000(FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown copyright ©.



Is Cyber insurance right for you?





National Cyber
Security Centre

a part of GCHQ

**Thanks for
listening**



Webinars and events

fraudadvisorypanel.org/event/upcomingevent

Webinars

*Beyond COVID-19:
Keeping your charity safe from fraud*
20 October (free)

*Future Fraud Professionals Career Talks:
National Crime Agency*
27 November (free)

Fraud Conference (online)

*The counter-fraud practitioner's toolkit:
preparing for the new world*
02 & 03 February 2021

Training

Managing fraud in small charities
23 October

Auditing fraud
11 November

Upcoming Business and Management Faculty webinars

60 minute webinars – 10.00am

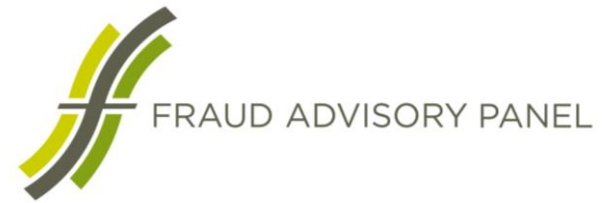
Supply chain assurance in the retail sector
20 October

Navigating 'office politics' positively
5 November

Practical Excel tips
7 December

[Icaew.com/bamevents](https://www.icaew.com/bamevents)

Business and Management Faculty



THANK YOU FOR ATTENDING

Contact the Business and Management Faculty

icaew.com/bam

✉ bam@icaew.com ☎ +44 (0)20 7920 8508

@ICAEW_BAM

Contact the Fraud Advisory Panel

fraudadvisorypanel.org

✉ info@fraudadvisorypanel.org ☎ +44 (0)20 7920 8637

@Fraud_Panel

Upcoming webinars and events

icaew.com/bamevents

fraudadvisorypanel.org/event/upcomingevent

