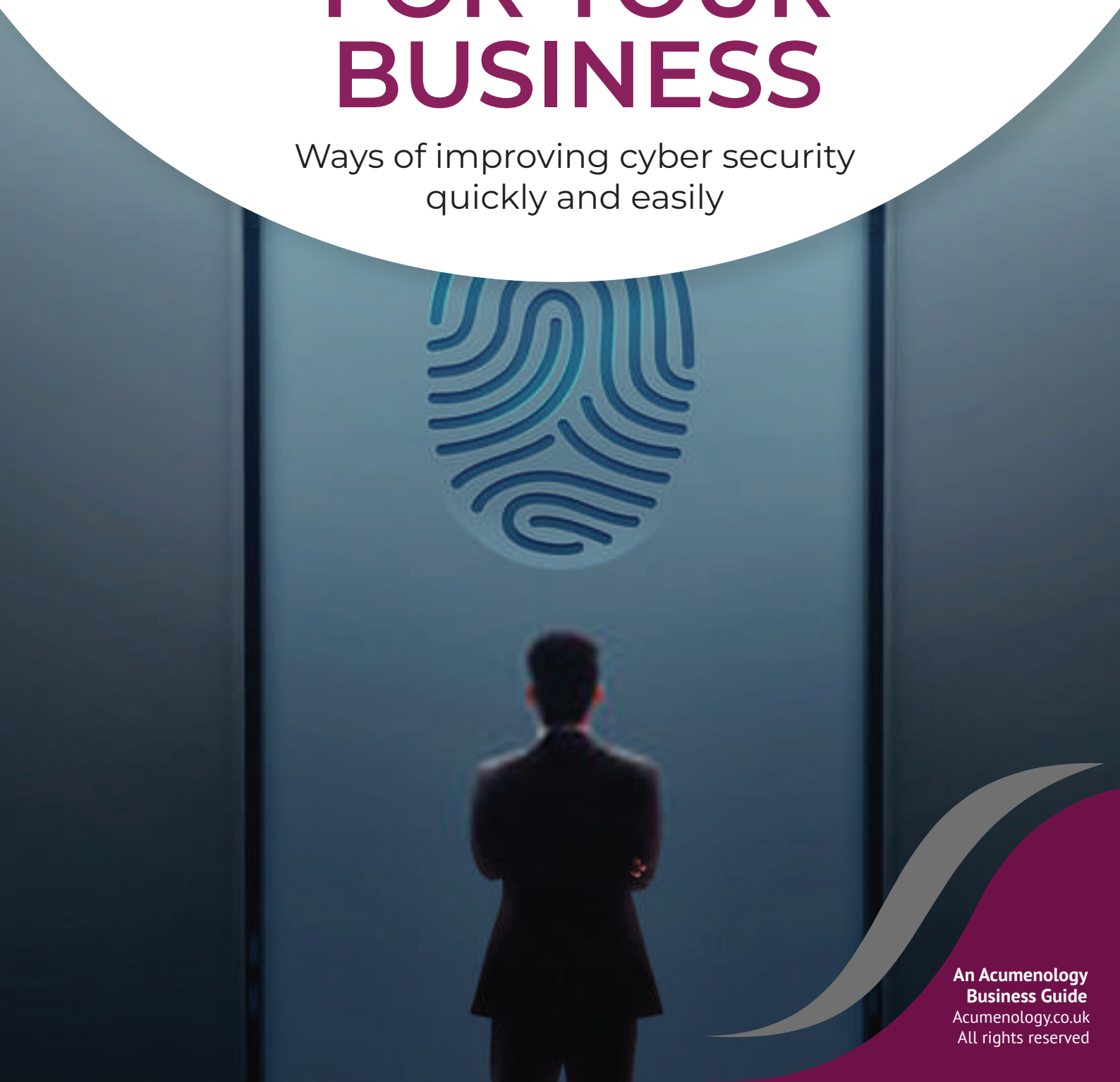
Acumenology

business support

HOW TO IMPROVE CYBER SECURITY FOR YOUR BUSINESS

Ways of improving cyber security quickly and easily



An Acumenology Business Guide

Acumenology.co.uk

Contents

01

Introduction

If you are a small or micro business, there is an increasing chance that you will experience a cyber security breach. The National Cyber Security Centre (NCSC) estimates a 1 in 2 chance of experiencing a cyber-attack resulting in potential losses of over £1500.

This guide will provide you with information that is easy to understand and costs little to implement and doing so will significantly your protection from the most common types of cyber-crime.

It is based on the NSCS Cyber Security Small Business Guide and covers 5 topics that will show you how easy it can be to protect your organisation's data, assets, and reputation.

To further help you, Acumenology has produced a series of Business Guides on a range of relevant topics.
You can find these at: www.acumenology.co.uk/business-guides

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

02

Backing up your data

Data is critical for the operation of any business and thus it is essential that all businesses irrespective of size regular backup their data and that it can easily be restored.

Doing so has the additional advantage that you can't be blackmailed by ransomware attacks.

4 things to consider when backing up your data.

1. Identify the data you wish to back up

Identify the essential data your business couldn't function without.

2. Ensure your back up is separate from your computer

Your data should be backed up on an external drive and/or a third-partycloud-based system.

At Acumenology we back up our data daily on an external drive as well as a separately on a 3rd party cloud backup system
Ensure access to backups is restricted so that it is not accessible by staff and is not permanently connected (either physically or over a local network) to the device holding the original copy.

Ransomware (and other malware) can often move to the attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover from.

For more resilience, consider storing your backups in a different location, so fire or theft won't result in you losing both copies.

Cloud backup solutions are a cost-effective way of achieving this.

3. Consider cloud backup

Using cloud backup means your data is physically separate from your location.

Service providers provide data storage and web services without you needing to invest in expensive hardware.
Most providers offer a limited amount of storage space for free, and larger storage capacity for minimal costs to small businesses.

Most service providers have good security practices. However, before contacting them we recommend you get some prior knowledge to help you decide what to look for when evaluating their services, and what they can offer.

We recommend you read the NCSC's Cloud Security Guidance

4. Back up daily

Ensure your backups run daily. This applies to both the data you backup on an external drive and, the backup carried out via your cloud service provider.

Most solutions allow you to do this automatically and using automated backups not only saves time, but also ensures that you have the latest version of your files should you need them.

You can also find out more on the ICO website Cloud computing.

03

Protection against malware

Malicious software ('malware') is software or web content that can harm your organisation's IT services.
The most well-known form of malware is viruses, which are self-copying programs that infect software.

Consider these 5 tips that can help protect you from malware attacks.

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

1. Install and turn on antivirus software

Most popular operating systems come pre-loaded with FREE Antivirus software and should be used on all computers and laptops.
All that is required is to click 'enable'.

2. Only download apps that can be trusted

You should only download apps for your portable devices from manufacturer-approved stores (like Google Play or Apple App Store).

These apps are checked to provide a certain level of protection from malware.
You should prevent staff from downloading third party apps from unknown vendors/sources, as these will not have been checked.

3. Keep all your equipment up to date

Ensure all your IT equipment including mobile devices are always kept up to date with the latest version of the software and firmware.

Operating systems should be set to 'automatically update' whenever this option is available.

4. Control how external drives are used

Using USB drives or memory cards to transfer files is commonplace, and it is hard to keep track on who and how people use them.
Inadvertently using a device containing malware can have devastating consequences.

You are reduce your risk by:

- Blocking access to physical ports for most users
- Using antivirus tools
- Only allowing approved devices to be used
- Ensuring files are transferred by email or cloud transfer such as MultCloud, Google Drive, One Drive or WeTransfer

5. Switch on your firewall

Firewalls create a 'buffer zone' between your own network and external networks (such as the Internet).
Most popular operating systems now include a firewall, so it may simplybe a case of switching this on.

04

Keeping mobiles and tablets safe

Businesses now commonly use mobile technology as part of their everyday business and with these devices being as powerful as computers it is important to ensure they are protected.

Here are 5 tips to keep your mobile devices secure.

1. Switch on password protection

Choose a complex PIN or password. Many devices now include fingerprint and/or facial recognition. Make sure you use these features if available.

2. Keep devices tracked

Having devices lost or stolen have to be allowed for. You can use various freely available tools to minimise your risk by:

- Tracking the location of your device
- Remotely lock access to the device
- Remotely erase the data on the device
- Retrieve a backup of data stored on the device

You can set up these tools on all your organisation's devices with a single click by using the appropriate mobile device management software.
To find out more CLICK HERE

3. Keep your device up to date

Ensure your devices are kept up to date at all times. Set your devices to automatically update where possible.

4. Keep your apps up to date

All applications installed should also be updated regularly. These updates will add new features as well as patching any security vulnerabilities.

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

5. **Do not connect to unknown Wi-Fi Hotspots**

Public Wi-Fi hotspots can be accessed by third parties to:

- Access your work whilst connected
- Access your login details to apps and web services whilst you are logged on

The safest method is to use your mobile 4G network, which has built-in security. You can also use 'tethering' (where your other devices such as laptops share your 4G connection).

You can also use Virtual Private Networks (VPNs), which encrypts your data but make sure you only use VPNs provided by reputable service providers.

For more information CLICK HERE

05

Using passwords to protect data

Your devices contain a lot of business-critical data, as well personal information and details of online accounts.

Using passwords correctly is a easy and effective way to prevent unauthorised access to your devices.

4 things to keep in mind when using passwords.

1. **Switch on password protection**

For mobile devices set a screen-lock password, PIN, or other authentication method.

Make sure that your office equipment also all use an encryption product. Most devices will have encryption built in.

2. **Use two factor authentication**

Where possible use two factor 2FA. This adds another layer of security for little effort.

2FA requires two different methods of authentication before you can use the service.
Generally, a password plus one other method.
This could be a code that's sent to your smartphone (or a code that's generated from a bank's card reader).

3. **Avoid predictable passwords**

Set passwords that are easy for you to remember, but hard for somebody else to guess.
A good rule is 'make sure that somebody who knows you well, couldn't guess your password in 20 attempts'.

4. **Manage password overload'**

Do not be overzealous with passwords.
Only enforce password access to a service if you really need to.

Where you do use passwords do not enforce regular password changes.
Passwords really only need to be changed when you suspect a compromise of the login credentials.

Use password managers. These are tools that can create and store passwords and which can be accessed via a 'master password'.

For more information on setting up passwords read the NCSC's password policy guidance.

06

Avoiding phishing attacks

A phishing attack involves scammers sending fake emails to thousands of people, asking for sensitive information (such as bank details), or containing links to bad websites.

Phishing emails are getting increasingly sophisticated and harder to spot.
Whatever your business, it is likely you will receive phishing attacks at some point.

Here are some tips to help you identify the most common phishing attacks.

1. **Configure your accounts to reduce the impact of successful attacks**

Configure employee access using the principle of 'least privilege'.
This means giving staff the lowest level of user rights required to perform their jobs.

If they become a victim of a phishing attack, the potential damage is reduced.

Minimise employee access to browse the web and or check personal emails using business devices. They can do so on their own device.

This can be done using an Administrator account which allows you to change security settings, install software and access all files on a computer.

Use two factor authentication on important accounts which means that even if a password is compromised they will still not be able to gain access.

2. Train your employees to recognise phishing attacks

Make your employees aware of your organisations normal way of working so that they are in a better position to identify requests that are 'out of the ordinary'.

Most importantly, train them to understand and spot potential phishing attacks.

Here are some examples of the different types of phishing attacks.

- **Fraud CEO email**
  A low-level employee working in the finance dept. receives a fraud email purporting to be from the CEOrequesting transfer of funds.

- **Clone phishing**
  The attack creates a virtual replica of a legitimate message and sends the message from an email address that looks legitimate. Any links or attachments in the original email are swapped out for malicious ones.

  The cybercriminal uses the excuse that they're re-sending the original message because of an issue with the previous email's link or attachment to lure end-users Into clicking on them.

- **Domain spoofing**
  This occurs when a cybercriminal "spoofs" an organization or company's domain to:

  - Make their emails look like they're coming from the official domain.
    A cybercriminal forges a new email header that makes it appear like the email is originating from a company'slegitimate email address.

  - Make a fake website look like the real deal by adopting the real site's design and using a similar URL.
    The cybercriminal creates a fraudulent website and with a domain that looks legitimate or is close to the original (apple.com vs apple.co,)

- **Evil twin**
  This is where "a rogue wireless access point that masquerades as a legitimate Wi-Fi access point so the attacker can gather personal or corporate information without the end-user's knowledge."

  This type of attack has also been referred to as the Starbucks scam because it often takes place in coffee shops.

- **HTTPS phishing**
  The cybercriminal sends an email with only a legitimate-looking link in the email body.

  There's often no other content except for the link itself (which may be clickable or a non-active link that requires the recipient to copy-and-paste the URL into their web address bar.

  This this type of phishing email difficult for filters to detect.

- **Smishing**
  Smishing is phishing by SMS. It lures users into downloading malicious payloads by sending text messages that appear to come from legitimate sources and contain malicious URLs for them to click on.
  It could be something disguised as a coupon code — 20% off your next purchase or it could be an offer to win free tickets.

- **Spear phishing**
  Unlike general phishing emails, spear phishing emails target specific individuals within an organisation.

  They personalize the emails to their intended victims by using email subject lines that would be topics of interest to the recipients to trick them into opening the message and clicking on links or attachments.

  91% of cyberattacks start with a spear phishing email

- **Vishing**
  This is 'voice phishing' or phishing over the phone.
  A vishing attack occurs when a criminal calls your phone to try to get you to provide personal or financial information.

They pretend to be someone else — the Inland Revenue, your bank, or credit card company. They'll claim that you owe taxes, or that your credit card has suspicious activity and needs to be shut down right away… they'll first just need to "verify" your personal information before they can close the card and reissue a new one.

- **Watering hole phishing**
  This attack targets businesses by:
  - Identifying specific websites that your company or employees visit most often and infecting one of the sites with malware.

    The sites that are selected for infection might be a supplier whose services your company uses. The goal is to infect the websites so that when you or your employees visit, your computers will automatically be loaded with malware.

- **Whaling**
  Whaling unlike spear phishing targets high level executives by sending highly targeted emails

3. Report all attacks

Encourage your staff to ask for help if they suspect a phishing attack or think that they have been a victim.

It is important to take steps to scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred.

If you believe that your organisation has been the victim of online fraud, scams or extortion, you should report this through the Action Fraud website.
Action Fraud is the UK's national fraud and cyber-crime reporting centre.

07
Conclusion

In this day and age with cybercrime on the increase, it is highly likely that your organisation and/or its employees will at some time be subjected to a cyber-attack.

Thus, it is only prudent that you take this threat seriously and familiarise both your employees and yourself on not only on recognising possible cybercrime attacks but that you take proactive steps in preventing them from occurring in the first place.

The NCSC is an excellent resource and has provided a series of videos on how to improve cyber security within your organisation. Click here to find out more.

Acumenology has produced a series of Business Guides on a variety of topics relevant to starting and running a business.

These can be found at:
www.acumenology.co.uk/business-guides