aztech
IT Solutions

Cyber Security for SMEs in 2019

THE ULTIMATE GUIDE

The Ultimate Guide to:
Cyber Security for SMEs in 2019

The ability to harness enterprise data and use AI to support decision-making processes is a necessity for modern businesses. Organisations must function productively, safely, and efficiently in the age of connectivity – it is essential for their survival in the market.

However, with the rapid rate of development in software and technology, 2019 is proving to be a busy one for the IT industry; the rising tide of cybersecurity threats is placing considerable pressure on businesses to protect their data and access points with greater vigilance than ever before.

It is vital for all businesses, especially small-to-medium enterprises, to recognise the potential danger and take the necessary measures to safeguard their digital activities. It's often precisely these types of organisations that are unable to recover after a security breach.

Top cybersecurity threats affecting SMEs

Phishing

These emails are often riddled with grammatical errors and are clearly elaborate, but the perpetrators of phishing emails are becoming more and more sophisticated.

This makes is harder for victims to tell the difference between genuine emails from trusted service providers (banks, insurance, legal companies) and copycat phishing mail.

Phishing can occur via emails, text messages or over the phone. Someone posing as a representative of an official institution will contact individuals and request sensitive data under the guise of needing to confirm their identity.

In this scenario, the individual may reveal banking details, personally identifiable information and other data that could leave them vulnerable to exploitation.

Tell-tale signs you're being phished

An incredible offer

Hackers understand the art of using eye-catching offers to capture the attention of vulnerable hopefuls who may be lured into believing that they've won a coveted prize such as an iPad or a holiday abroad.

If it looks suspicious and you have no recollection or way of tracing your entry into the supposed competition, it's very likely that you are facing a scam.

Attachments

If you receive an unexpected email from someone you don't know, or it doesn't make sense for the contact to send you an attachment, don't open it.

Symantec state that '48 % of malicious email attachments in 2018 were office files', which is why you should double check the sender's email address or call your colleague who sent you the email to make sure it was them.

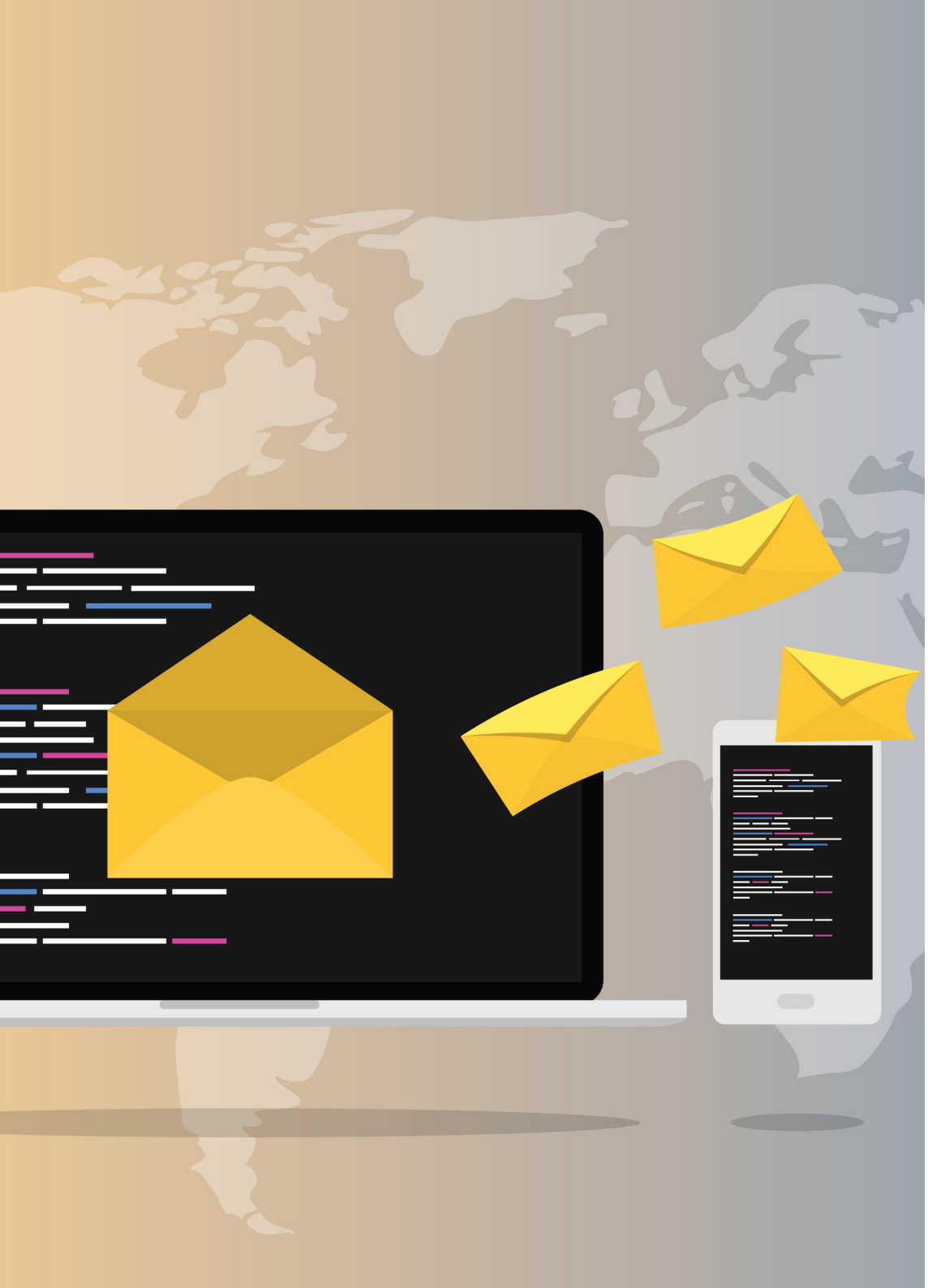
If you download an unexpected attachment, you could easily download malware without realising.

Pressure to act fast

Phishing often preys on the individual's anxiety about missing out.

The incredible offer will usually have an "Act Now!" feel about it. Or, the content could imply that you will lose access or privileges to an account that you have, therefore you must follow a specific set of instructions to safeguard your assets.

If something feels off, it's best to directly call your service provider or check your account by accessing the official website independently. If you suspect that the email is fraudulent, do not click on the link – ever.



Pressure to act fast

Phishing often preys on the individual's anxiety about missing out.

The incredible offer will usually have an "Act Now!" feel about it. Or, the content could imply that you will lose access or privileges to an account that you have, therefore you must follow a specific set of instructions to safeguard your assets.

If something feels off, it's best to directly call your service provider or check your account by accessing the official website independently. If you suspect that the email is fraudulent, do not click on the link – ever.

Strange links

Be vigilant with the links you click on.

Are you expecting to be sent a link? Do you know the source? Check the spelling and make sure it's not a near miss for the official URL you were intending to visit.

Never click on a link from a suspicious email -
Alternatively, if you hover over the link, the real hyperlink will appear in the bottom left of your screen, or as an info pop up as you hover over.

Email Address

If you've received an 'unexpected' email, such as those mentioned above, but you're still unsure if it's phishing or not, hover over the email address – this is one of the safest ways for you to check if it's phishing as you won't need to open the email.

Phishing emails often name the contact as a specific email address or user (Your Bank 'example@yourbank.com'), but the actual email address is full of special characters, numbers and letters, and is typically longer than a standard email address.

Ransomware

Ransomware is a type of malicious software that infiltrates your computer, often using a Trojan file.

In appearance, the file may seem legitimate enough for you to download but, once opened, it unlocks viruses that could block access to your computer and / or files until a ransom has been paid – its sole purpose is to extort.

Let's take a look at a few common culprits:

Lockers

Infects your PC and locks you out, rendering the device useless and your files inaccessible.

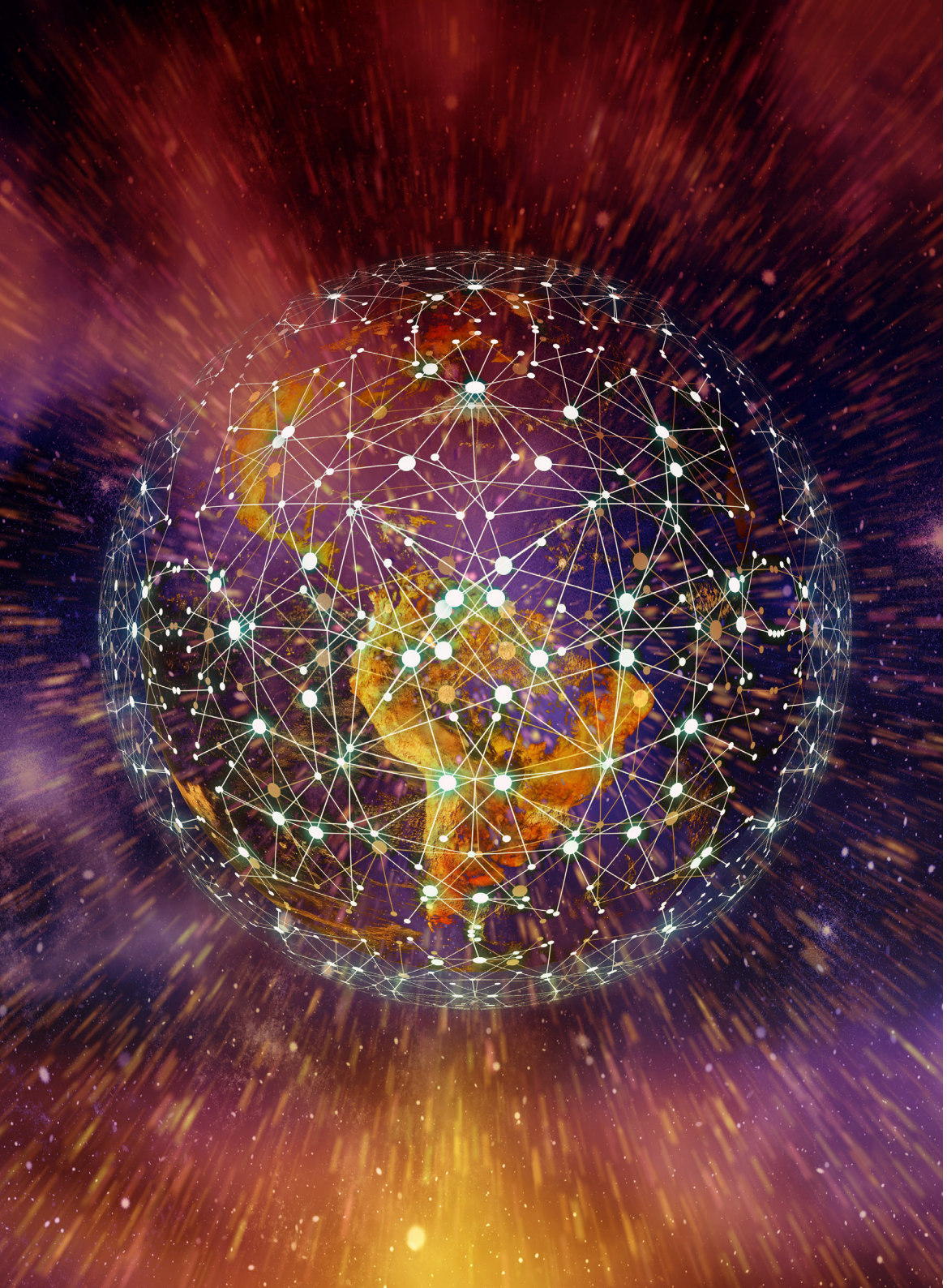
Crypto-malware

An insidious piece of malware that will conceal itself on your device and mine data for as long as possible.

Scareware

Warns you that your computer is under threat from a virus and that you need to pay a fee to resolve the issue.

Scareware can initiate pop-ups and bombard you with alerts until you take the required action.



Malware

Malware, short for malicious software, is similar to ransomware. It can sneak onto your computer undetected or well disguised, simply by you clicking or downloading malicious content.

Its main priority is destroying, stealing and encrypting your sensitive data, so hackers can gain access to your computer and your activity.

Here are some of the types of malware you may encounter:

Spyware

Wants to spy on you and will hide in the background waiting for you to do something noteworthy online such as, input your password or credit card details.

Worms

Will infect as much as it possibly can. This malware will creep into your network and go from one machine to the next until your devices become dysfunctional.

Adware

A software application that facilitates advertising banners being displayed while you use a particular program. Although it may not be as malicious as other types of malware, it can be irritating, preventing you from working as you'll constantly be closing pop-ups.

Viruses

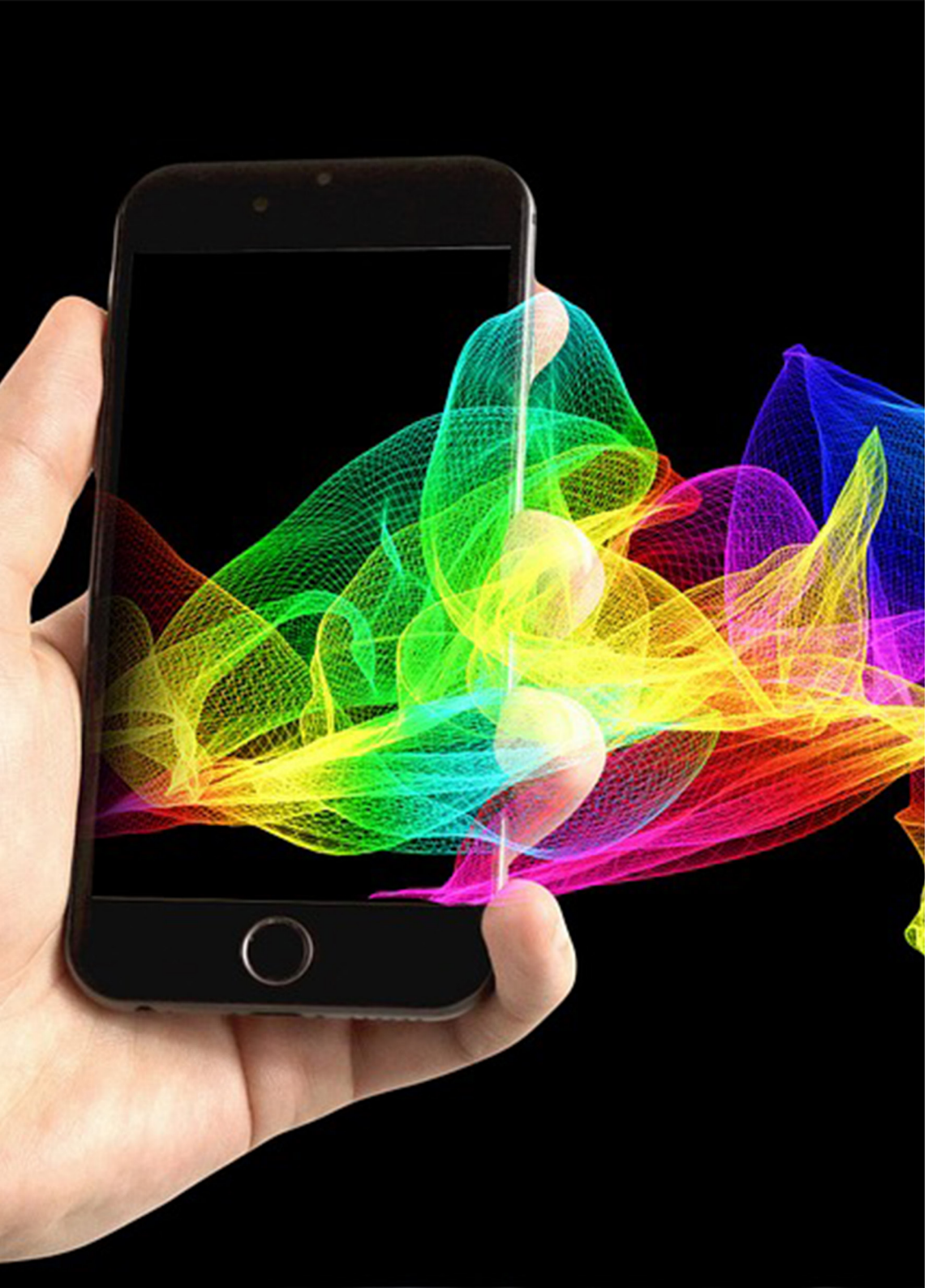
Will find an uncorrupted file and infect it, damaging your system and its ability to work correctly.

Mobile cyber attacks

Mobile devices have become a fundamental tool for most businesses as connectivity is essential, and mobile devices help us perform our jobs with more freedom and flexibility.

Organisations have begun allowing staff to bring their own devices to work as it reduces costs and lets employees work with what feels most comfortable to them.

However, it can become difficult to monitor legitimate users and detect unauthorised sessions on your network.



What are the big mobile threats to watch out for?

Cryptojacking

This is the unauthorised use of someone else's computer to mine cryptocurrency.

With cryptocurrency becoming a highly influential commodity, it makes sense that hackers would view mobile devices as an excellent resource to mine.

Major international app stores have now banned cryptomining applications, however, cybercriminals have a way of finding loopholes, and some devices are more vulnerable than others.

Cryptomining can affect your phone quite severely, causing the battery to overheat and the device to become permanently damaged.

Password exploitation

Employees don't always have the most effective passwords, despite the obvious risks. This is partly due to organisations having a high number of staff, making it difficult to manage and monitor password hygiene.

According to NCSC's Cyber Survey, 'breach analysis finds 23.2 million victim accounts worldwide used 123456 as password [sic]'. Contrary to popular belief, the longer your password is, the harder it is to be hacked.

You don't have to use special characters combined with capitalisation and numbers - SOMETHINGLIKETHISCANBEHARDERTOHACK than S0mEth1N6L!kEtHIS.

You should opt for passwords that are 12 characters or more, anything less than 8 characters is too short. String a set of words together that you'll easily remember, but don't write it down where it will be easily found.

Advanced persistent threats (APTs)

Company secrets can be valuable to competitors or hackers who are looking for a way in to exploit your vulnerabilities.

An APT is a silent cyberattack where the intruder will hack your network and remain undetected for an extended period of time, monitoring your activity and stealing any data that could be detrimental to your business.

To avoid detection the attackers use sophisticated, persistent techniques, rewriting malicious code, often dedicating many resources to their cause.

One of the main aims of ATP attacks is to enable the cybercriminal to instigate social engineering manipulations.

The attacker will research the target or enterprise and gather as much intelligence as possible - once they have a grasp of your internal process and other important corporate values, they can engage in a variety of sinister acts, such as extorting money or compromising your company's assets.

4 steps you need to take to protect your organisation

1. Assess your current cybersecurity status

If you're not sure where you stand, you won't know where to go - if you don't have an on-site IT specialist, it is advisable to bring in a third-party cybersecurity expert.

They can analyse your current systems and assess whether there are any areas of concern, or places where your network is open to vulnerabilities.

- Our security specialists can review your IT security policy, provide guidance and advise on any areas for improvement
- We can also help to induct the latest best practices into your organisation and ensure that it is implemented correctly

2. Train your staff

Untrained employees are ideal targets for cybercriminals as they may unwillingly click or download malicious content. This is why it's crucial to prepare and train your staff on the potential dangers of cybercrime and what they should keep an eye out for.

Creating awareness and educating your team members is crucial when establishing security policies within your business.

We offer user awareness training to help educate your staff on the warning signs of a potential attack and help them remain vigilant to the latest cyberthreats.

3. Ensure that you can remotely protect your data

Mobile devices are here to stay, and your business probably makes frequent use of them. With employees bringing their own devices for work, it can become difficult to know who's on your network and what they are accessing.

If a device is stolen or lost, it puts your confidential data at risk. That's why your organisation needs to have the necessary infrastructure to monitor how your data is being used.

- We can assist with asset management and device encryption to protect your data, especially with roaming users.

4. Update your software

Your devices and programs should always be updated to the latest versions.

Old applications are vulnerable to 'zero-day' exploits (an attack that occurs on the same day a weakness is discovered within software), and if your business isn't prepared, a cybercriminal could take advantage and penetrate your network.

Just like your other software, anti-virus applications must be routinely updated and managed to ensure that nothing unwanted can slip through the cracks.

Be sure to run them frequently and check for updates.

Are you protected?

Have you thought about your disaster recovery plan? When was the last time you updated your security policies?

Cyberattacks can be crippling to any organisation, whether they're small, medium or large.

Spotting the loopholes and vulnerabilities requires a professional approach - the best place to start is by seeking the advice of a security expert.

We offer a no-obligation consultation, and whether you're at the initial set up stages of your business or are looking to bolster your current efforts, we'd be happy to discuss the best options for your company.

If you have any questions, please don't hesitate to get in touch.

01908 571 510

General Enquiries:
info@aztechit.co.uk

Sales:
sales@aztechit.co.uk

aztech
IT Solutions