Netitude

5 BEST PRACTICES FOR SME CYBER SECURITY

Affordable & practical advice for businesses

TABLE OF CONTENTS

INTRODUCTION

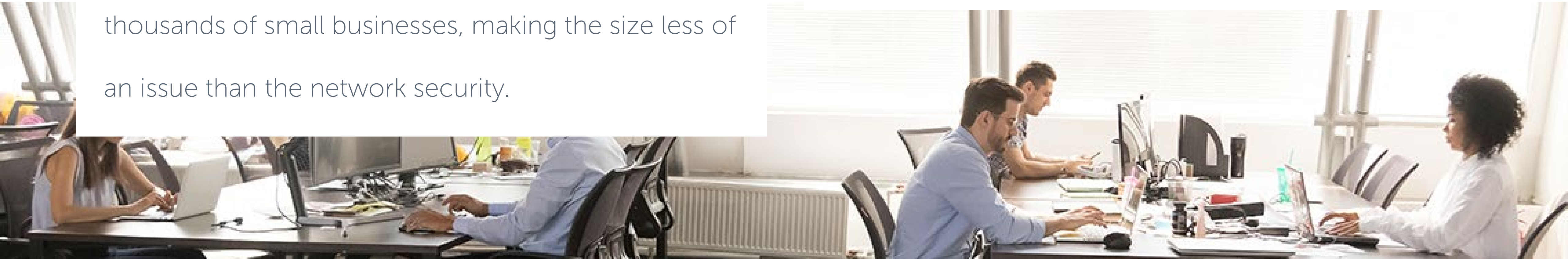
Cyber security doesn't have to be a daunting for small business owners. In this guide, we'll outline five easy steps to follow that could save time, money and even your business' reputation.

While this guide can't guarantee protection from all types of cyber-attack, our suggestions can significantly reduce the chances of your business falling victim of cybercrime.

WHAT MAKES SMEs THE PERFECT TARGET FOR CYBER ATTACKS?

The motivation for almost all cyber-attacks is to get personal data to use in credit card or identify theft. While larger enterprises typically have more data to steal, small businesses have weaker network security, making it easier to breach the network. By using automated attacks, cybercriminals can breach thousands of small businesses, making the size less of an issue than the network security.

The lack of time, budget and knowledge on proper security is a top reason for the high rate of SMB (small to medium businesses) attacks. Other reasons include not having an IT security specialist, not being aware of the risk, lack of employee training, not updating security programs and failure to secure endpoints.



UNDERSTANDING THE THREAT AND BELIEVING YOU’RE AT RISK

65%

of SMEs suffered a cyber attack from 2019-2020 compared to 46% of all businesses on average

24%

of senior managers are updated on cyber security less than once a year

18%

of SME decision makers list cyber security as their least concern

81%

do not receive any training on cyber security

68%

have no formal policies for ensuring cyber security

26%

have no cyber security measures at all

STEP #1 – SAFEGUARD YOUR DEVICES

Let’s start with something simple.

Mobile technology is now an essential part of modern business, with more of our data being stored on tablets and smartphones than ever. What's more, these devices are now as powerful as traditional computers, and because they often leave the safety of the office (and home), they need even more protection than 'desktop' equipment.

5 TIPS FOR KEEPING YOUR DEVICES SAFE

Netitude

1. Switch on password protection

A appropriately complex PIN or password (rather than a simple one that can be easily guessed or picked up from your social media profiles) will prevent the average person from accessing your phone. Many devices now include fingerprint or facial recognition to unlock your device, without the need for a password. However, these features are not always enabled 'out of the box', so check they've been switched on.

2. Make sure devices can be tracked, locked, or wiped

Staff are more likely to lose or have their tablets or phones stolen when they are away from the office or home. Fortunately, most devices include free web-based tools that are invaluable should you lose your device.

You can use them to:

- ✓ Track the location of a device.
- ✓ Remotely lock access to the device (to prevent anyone else using it).
- ✓ Remotely erase the data stored on the device.
- ✓ Retrieve a backup of data stored on the device.

5 TIPS FOR KEEPING YOUR DEVICES SAFE

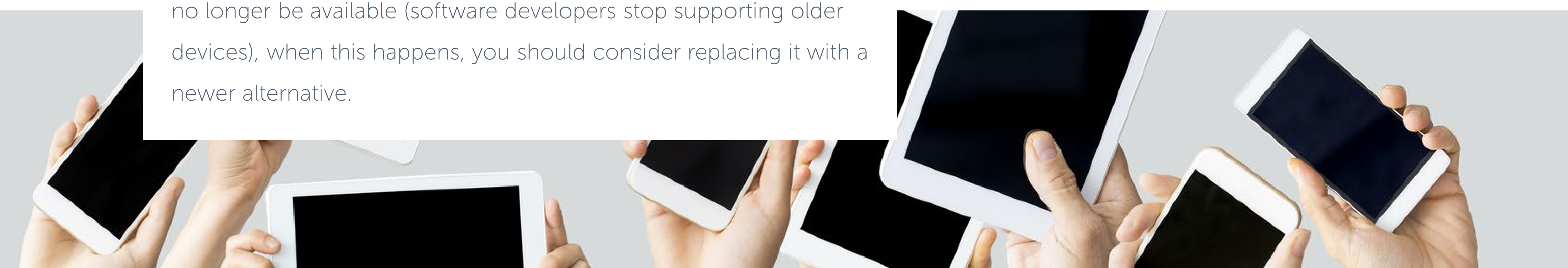
3. Keep your device up to date

Regardless of which phones or tablets your business uses, it’s important that they are always kept up to date. All manufacturers (like Windows, Android, iOS) release regular updates that contain critical security updates to keep the device protected. This process is quick, easy, and free; devices should be set to automatically update, where possible.

Make sure your staff know how important these updates are, and if necessary, explain how to do it. At some point, these updates will no longer be available (software developers stop supporting older devices), when this happens, you should consider replacing it with a newer alternative.

4. Update your apps

Just like the operating systems on your devices, all the applications that you have installed should also be updated. Updates don’t just add new features, but they will also patch any security holes that have been discovered. Make sure staff know when updates are ready, how to install them, and that it's important to do so straight away.



5 TIPS FOR KEEPING YOUR DEVICES SAFE

5. Don’t use to public Wi-Fi

When you use public Wi-Fi hotspots (in hotels, coffee shops etc.), there is no way to easily find out who controls the hotspot, or to prove that it belongs to who you think it does. If you connect to these hotspots, somebody else could access:

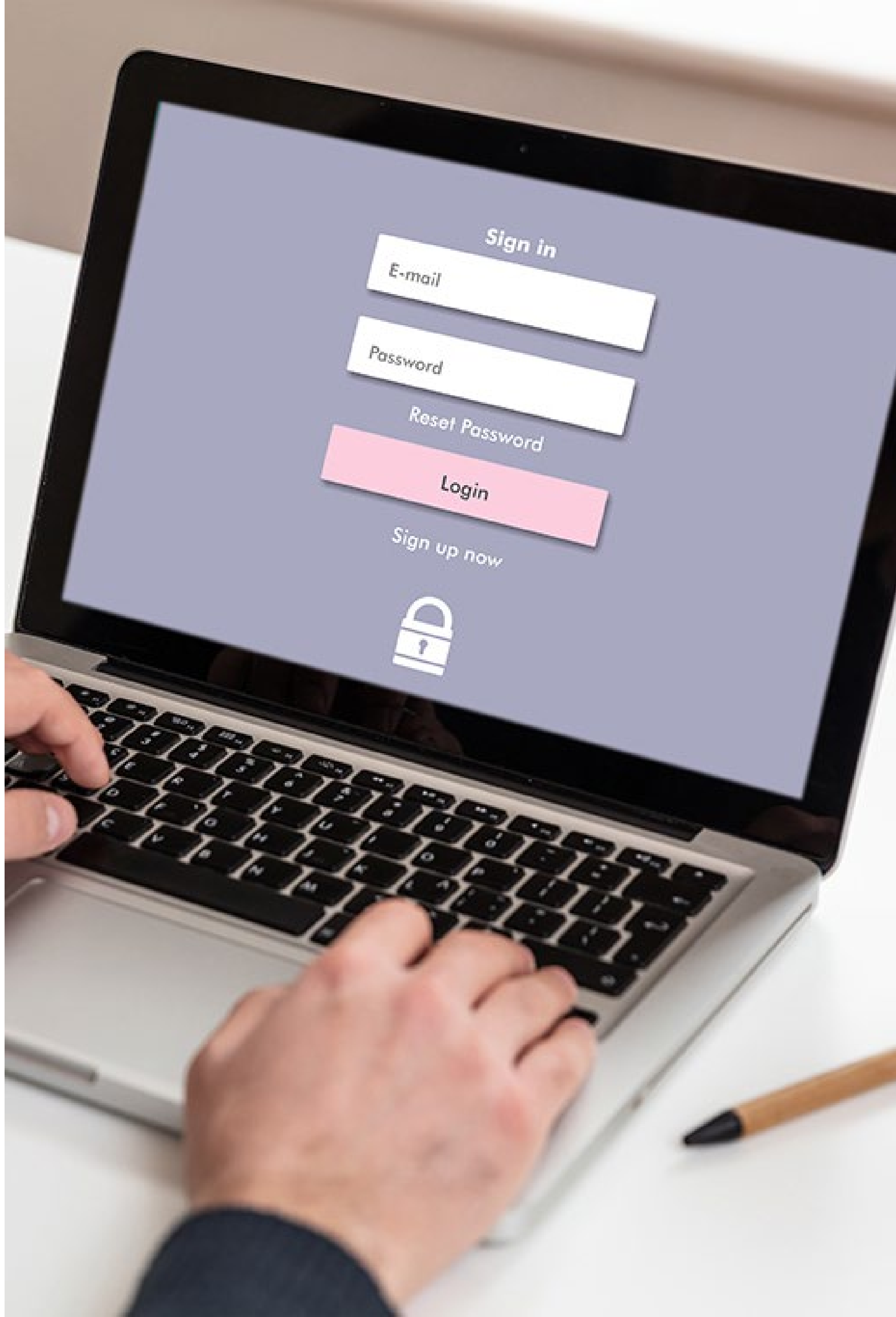
- ✓ What you're working on.
- ✓ Your private login details that many apps and web services maintain whilst you're logged on.

The simplest precaution is not to connect to free or public wifi, and instead use your mobile phone’s 3G or 4G network, which will have built-in security. If you want to use your laptop or tablet, you can share your 3G/4G signal from your phone using a “personal hotspot”, or a wireless 'dongle' provided by your mobile network. You can also use Virtual Private Networks (VPNs), to encrypt your data before it is sent across the Internet. If you're using third party VPNs, you'll need the technical ability to configure it yourself, and should only use VPNs provided by reputable service providers.

STEP #2 - PROTECT YOUR DATA WITH STRONG PASSWORDS

Your laptops, computers, tablets and smartphones hold lots of business-critical data, including your own, the personal information of your customers, and also details of the online accounts that you access. It is essential that this data is available to you, but not available to unauthorised users.

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised users accessing your devices.



5 PASSWORD CONSIDERATIONS

Netitude

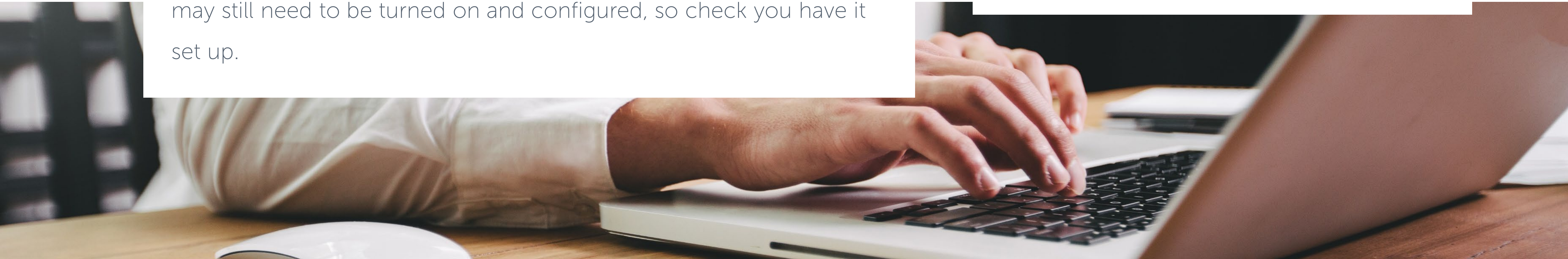
1. Switch on password protection for all devices

Set a lockscreen password, PIN, or other authentication method (such as fingerprint or face unlock). For more advice of password security download out guide.

Password protection is not just for smartphones and tablets. Make sure that your office equipment (laptops. PCs etc.) all use an encryption product (such as BitLocker for Windows) using a Trusted Platform Module (TPM) with a PIN, or FileVault (on macOS) to start up. Most modern devices have encryption built in, but encryption may still need to be turned on and configured, so check you have it set up.

2. Change default passwords

One of the most common mistakes is not changing the manufacturers' default passwords that smartphones, laptops, and other types of equipment are issued with. Change all default passwords before devices are given to staff. You should also regularly check devices (and software) specifically to detect unchanged default passwords.



5 PASSWORD CONSIDERATIONS

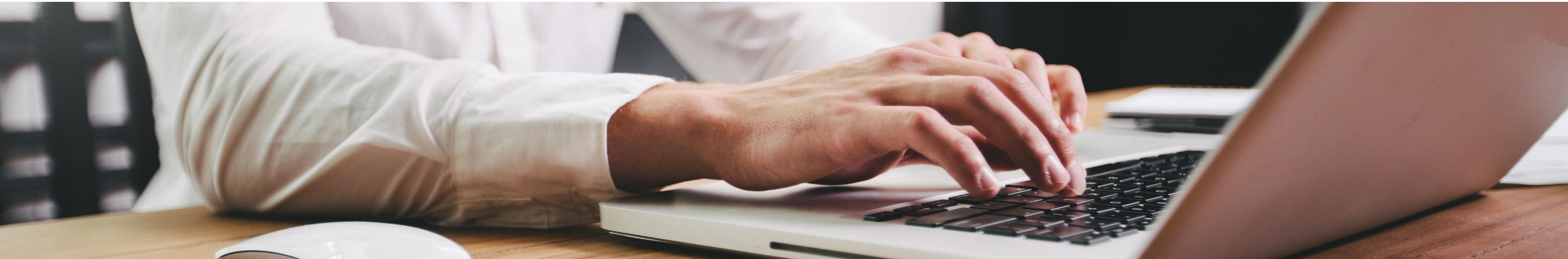
Netitude

3. Don’t use predictable passwords

If you oversee IT policies within your organisation, make sure staff are given actionable information on setting passwords that is easy for them to understand.

Passwords should be easy to remember, but hard for somebody else to guess. Staff should also avoid using the most common passwords, which criminals can easily guess.

Your IT systems should not require staff to share accounts or passwords to get their job done. Make sure that every user has personal access to the right systems, and that the level of access given is always the lowest needed to do their job, whilst minimising unnecessary exposure to systems they don't need access to.



5 PASSWORD CONSIDERATIONS

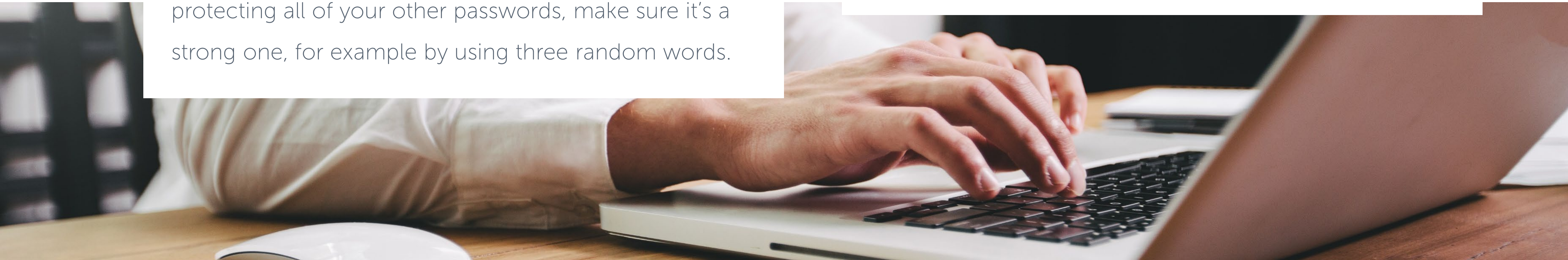
4. Use a password manager

You should also provide secure storage so staff can write down passwords for important accounts (such as email and banking), and keep them safe (but not with the device itself). Staff will forget passwords, so make sure they can reset their own passwords easily.

Consider using password managers, which are tools that can create and store passwords for you that you access via a 'master' password. Since the master password is protecting all of your other passwords, make sure it's a strong one, for example by using three random words.

5. Enable two-factor authentication

If you're given the option to use two-factor authentication (2FA) for any of your accounts, you should do; it adds a large amount of security for a little extra effort. 2FA requires two different methods to 'prove' your identity before you can use a 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) that you must enter in addition to your password.

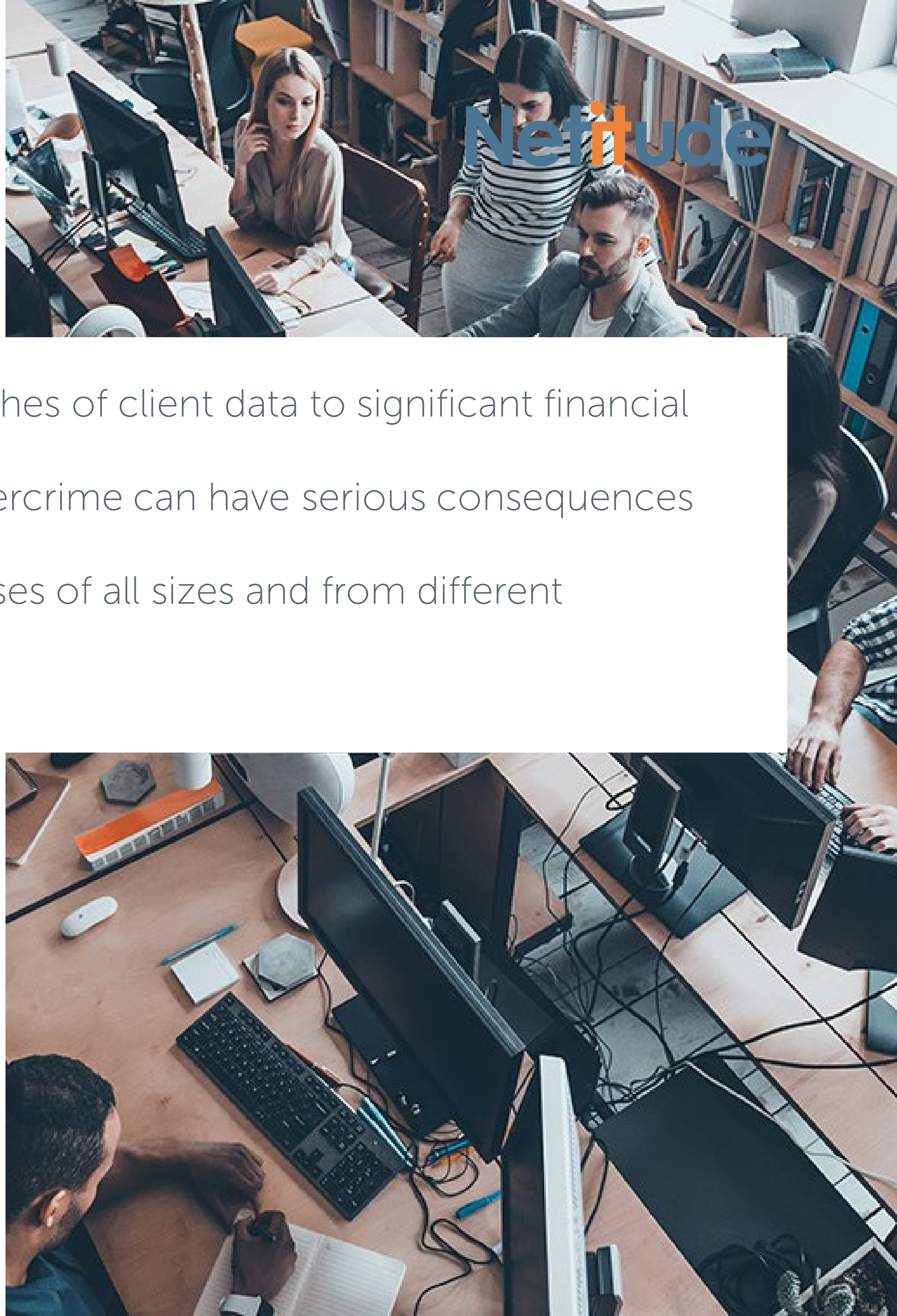


STEP #3 – DEFEND YOUR BUSINESS FROM MALWARE

Malware (malicious software) is software or web content that can harm your organisation, like the WannaCry outbreak that crippled the NHS. The most well-known form of malware is viruses, which are self-copying programs that infect legitimate software.

With the rise of technology, malware attacks are becoming increasingly common for both individuals and businesses and have increased by an incredible 67% since 2014.

From breaches of client data to significant financial losses, cybercrime can have serious consequences for businesses of all sizes and from different industries.



5 GUIDELINES TO HELP PREVENT MALWARE DAMAGING YOUR BUSINESS

1. Install antivirus software

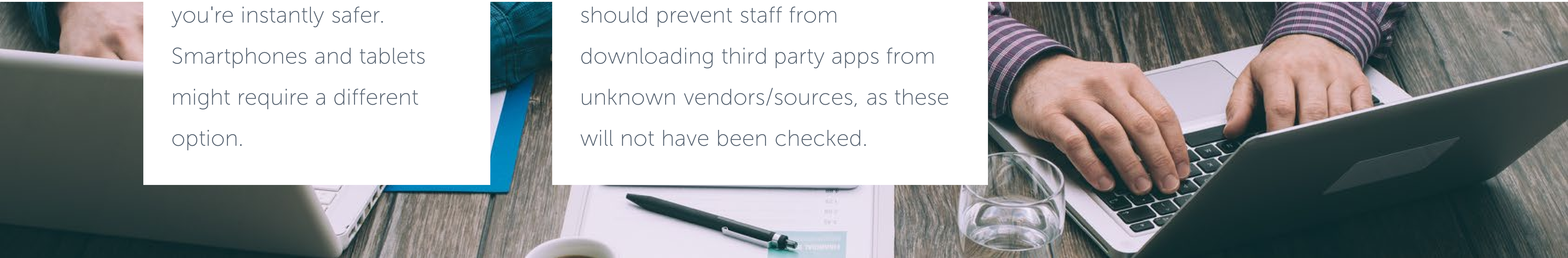
   Antivirus software - which is often included for free within popular operating systems - should be used on all computers and laptops. For your office equipment, you can pretty much click 'enable', and you're instantly safer. Smartphones and tablets might require a different option.

2. Stop staff from downloading dodgy apps

   You should only download apps for mobile phones and tablets from manufacturer-approved stores (like Google Play or Apple App Store). These apps are checked to provide a certain level of protection from malware that might cause harm. You should prevent staff from downloading third party apps from unknown vendors/sources, as these will not have been checked.

3. Turn on your firewall

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



Netitude

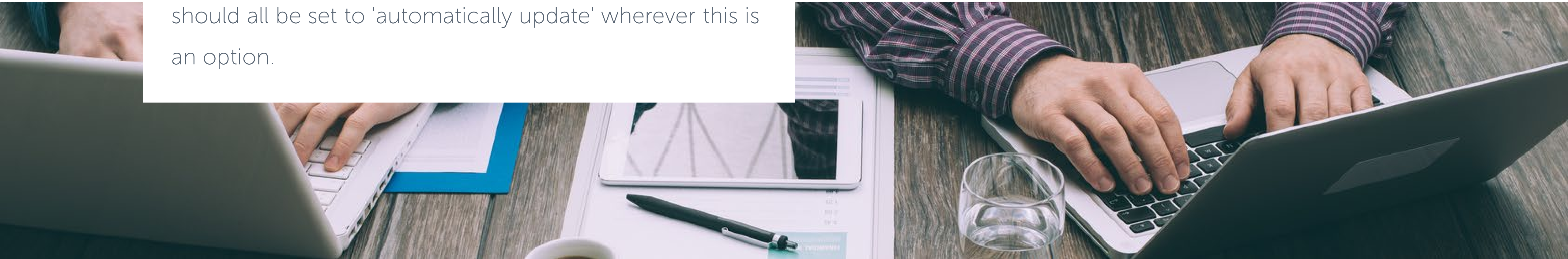
5 GUIDELINES TO HELP PREVENT MALWARE DAMAGING YOUR BUSINESS

4. Keep your IT equipment up to date

For all your IT equipment (tablets, smartphones, laptops and PCs), make sure that the software and firmware is always kept up to date with the latest versions from software developers, hardware suppliers and vendors. Applying these updates (patching) is one of the most important things you can do to improve security.

Operating systems, programmes, phones and apps should all be set to 'automatically update' wherever this is an option.

At some point, these updates will no longer be available (software developers stop supporting older devices), when this happens, you should consider replacing it with a newer alternative.



5 GUIDELINES TO HELP PREVENT MALWARE DAMAGING YOUR BUSINESS

5. Manage how USB drives can be used

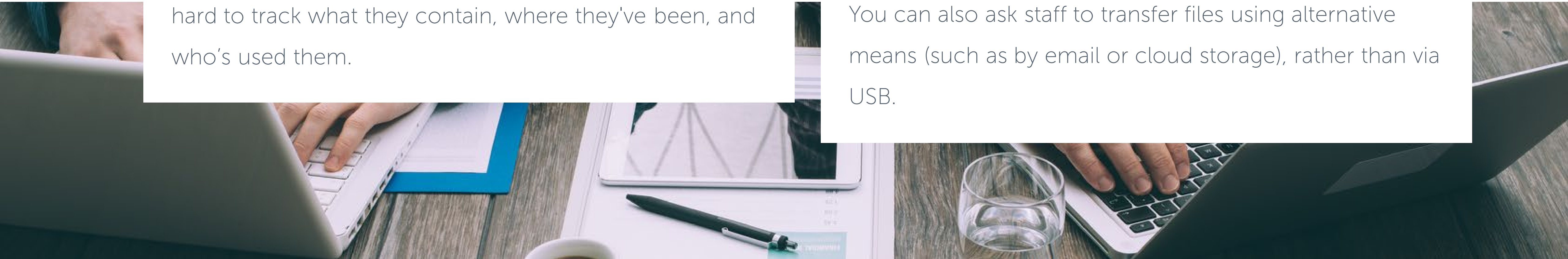
We all know how tempting it is to use USB drives or memory cards to transfer files between organisations and people. But, it only takes a one person to unintentionally plug in an infected stick (such as a hard drive, USB stick or memory card containing malware) to devastate the whole business.

When drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who's used them.

You can reduce the likelihood of infection by:

- ✓ Blocking access to physical ports for most users.
- ✓ Using antivirus tools.
- ✓ Only allowing approved drives and cards to be used within your organisation - and nowhere else.

Make this advice part of your company policy to prevent your organisation being exposed to unnecessary risks. You can also ask staff to transfer files using alternative means (such as by email or cloud storage), rather than via USB.

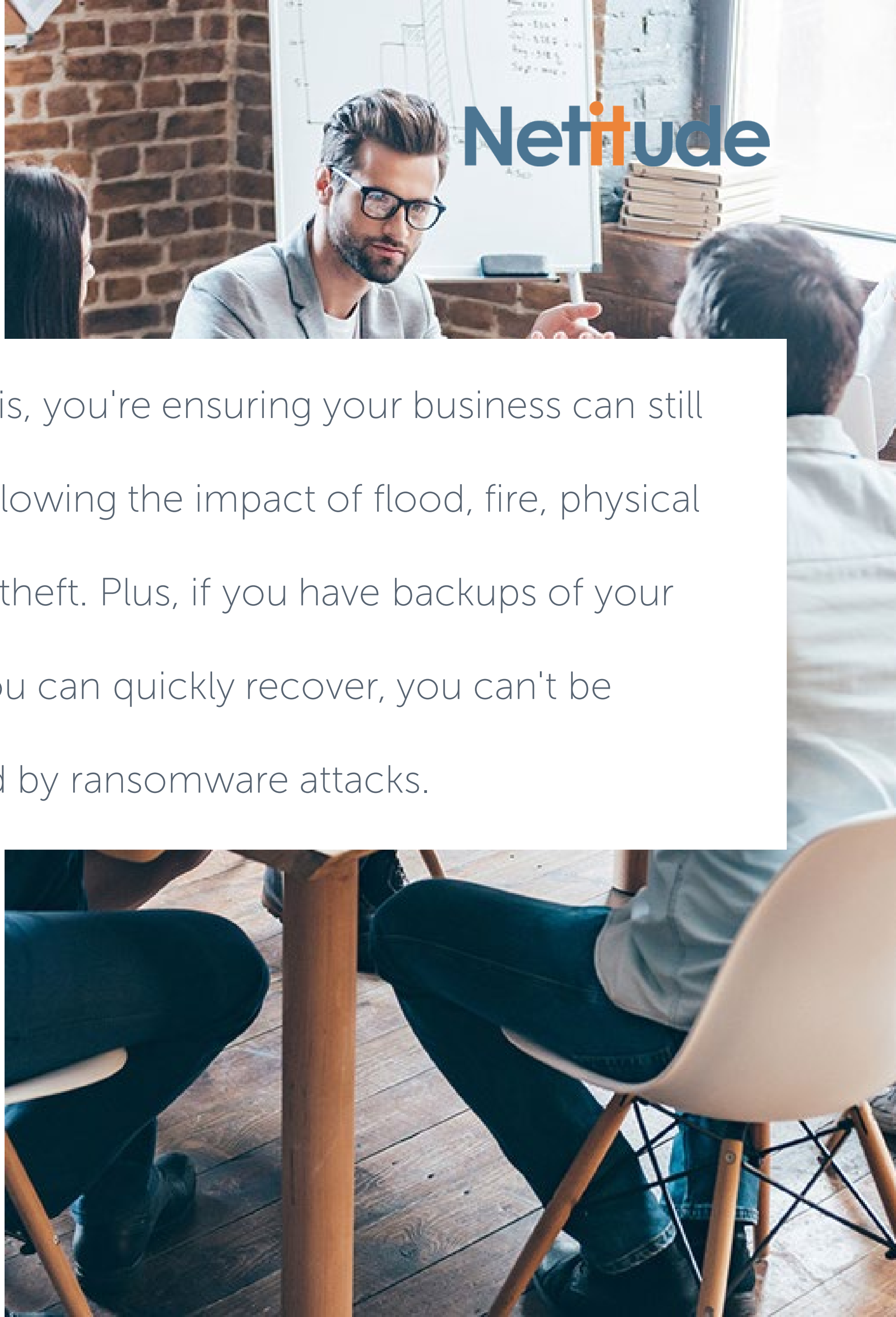


STEP #4 - REGULARLY BACKUP YOUR DATA

Think about how much your business relies on data like customer details, quotes, orders, and payment details. Now imagine how you'd cope operating without them – how long would you last?

All businesses, regardless of size, should make regular backups of their important data, and make sure that these backups are recent and can be restored.

By doing this, you're ensuring your business can still function following the impact of flood, fire, physical damage or theft. Plus, if you have backups of your data that you can quickly recover, you can't be blackmailed by ransomware attacks.



4 CONSIDERATIONS FOR BACKUPS

1. Determine which data you want to back up

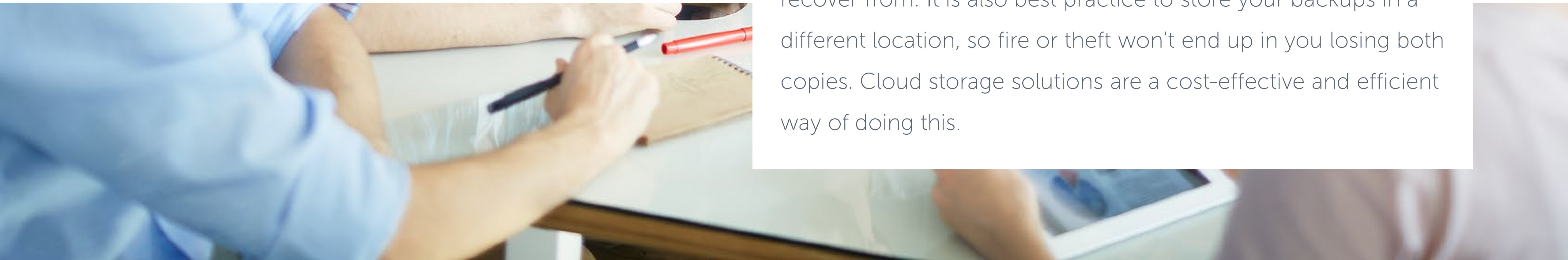
Your first step is to identify your essential data - the information that your business couldn't function without. Normally this will include documents, emails, contacts, and calendars, most of which are kept in various folders on your computer, phone, tablet or network.

2. Keep your backup separate from your computer

Whether it's on a separate hard drive or a different computer, access to data backups should be restricted so that they:

✓ Are not accessible by staff.
✓ Are not connected to the device holding the original copy.

Ransomware (and other malware) is smart and can often move to attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover from. It is also best practice to store your backups in a different location, so fire or theft won't end up in you losing both copies. Cloud storage solutions are a cost-effective and efficient way of doing this.



4 CONSIDERATIONS FOR BACKUPS

3. Consider the cloud

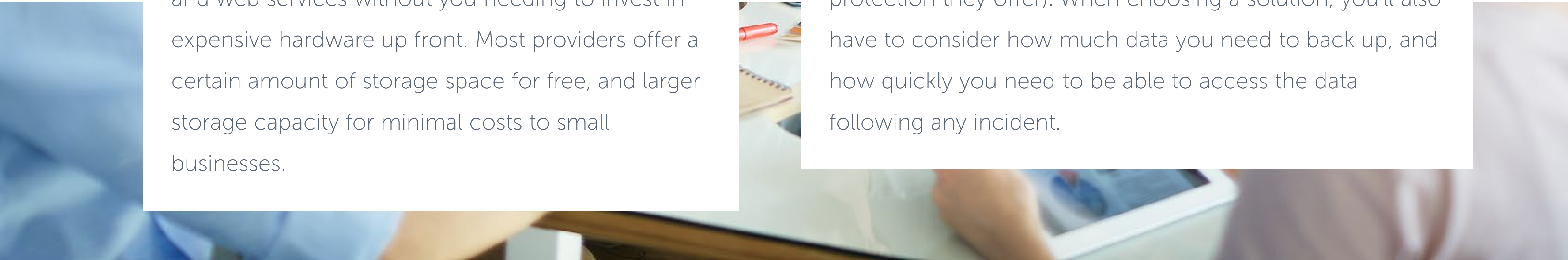
You've probably already used cloud storage during your personal life without even knowing – most smart phone save photos in the cloud automatically.

Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location. You'll also benefit from a high level of availability. Service providers can supply your business with data storage and web services without you needing to invest in expensive hardware up front. Most providers offer a certain amount of storage space for free, and larger storage capacity for minimal costs to small businesses.

4. Back up your data daily

The last thing you want to do is 'waste time' backing up your data, but did you know that the majority of network or cloud storage solutions now allow you to make backups automatically. Using automated backups not only saves time, but also ensures that you have the latest version of your files should you need them.

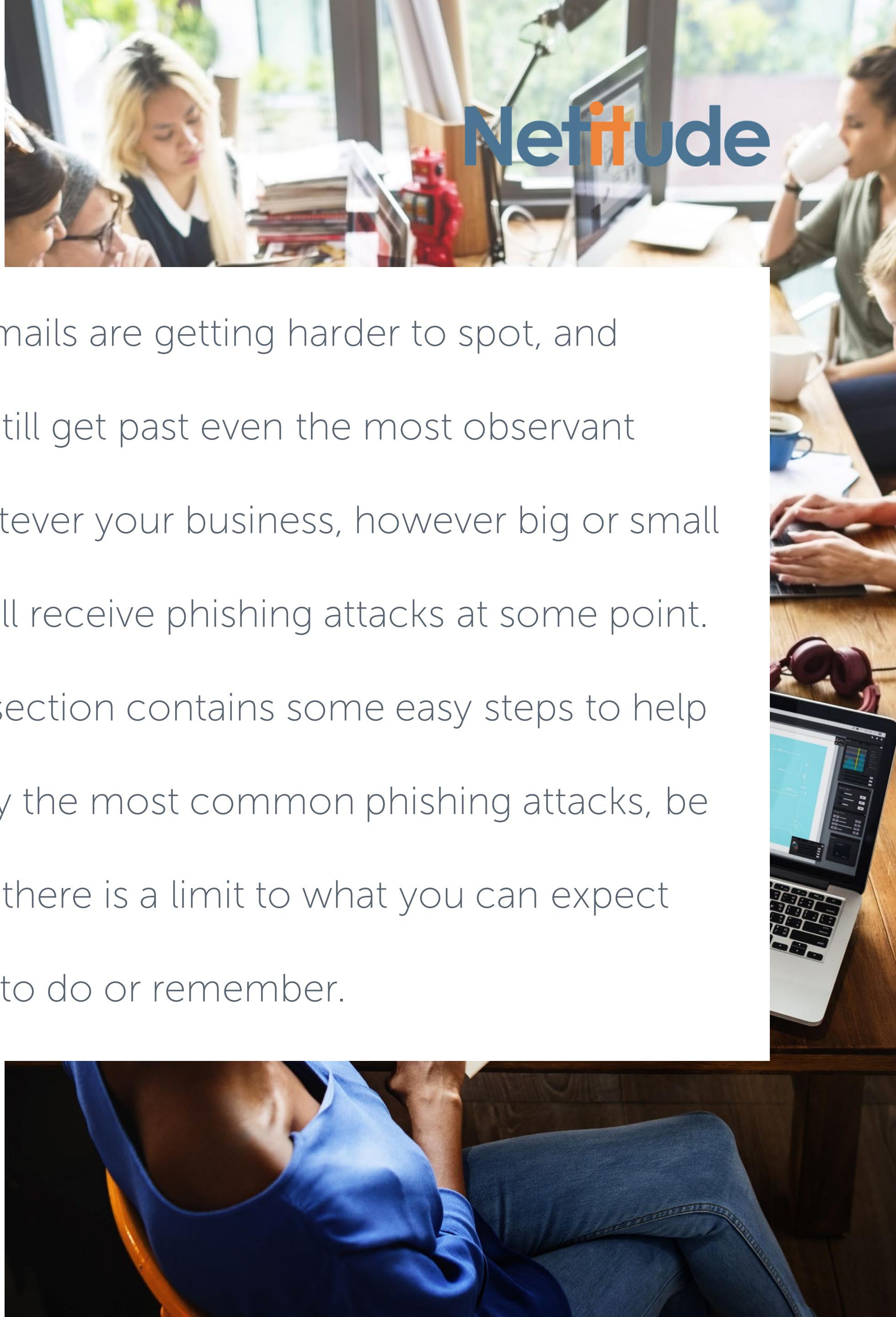
Many 'off-the-shelf' backup solutions are easy to set up and are affordable (when you consider the business-critical protection they offer). When choosing a solution, you'll also have to consider how much data you need to back up, and how quickly you need to be able to access the data following any incident.



STEP #5 – LEARN ABOUT PHISHING

In a typical phishing attack, scammers send fake emails to thousands of people, asking for sensitive information (like bank details), or to click on links to bad websites. They might try to trick you into sending money, steal your details to sell on, or they may have other motives for accessing your organisation's information.

Phishing emails are getting harder to spot, and some will still get past even the most observant users. Whatever your business, however big or small it is, you will receive phishing attacks at some point. While this section contains some easy steps to help you identify the most common phishing attacks, be aware that there is a limit to what you can expect your users to do or remember.



5 TIPS FOR DODGING PHISHING ATTACKS

Netitude

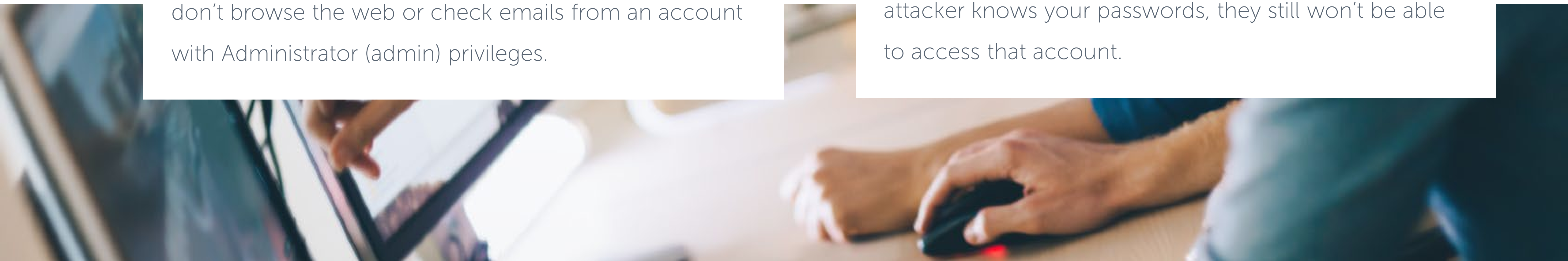
1. Setup accounts to reduce the impact of successful attacks

You should setup your staff accounts in advance using the principle of 'least privilege'. This means giving staff the lowest level of user rights required to perform their jobs, so if they are the victim of a phishing attack, the potential damage is reduced.

To further reduce the damage that can be done by malware or loss of login details, ensure that your staff don't browse the web or check emails from an account with Administrator (admin) privileges.

An Administrator account is a user account that can make changes that will affect other users such as security settings, install software and hardware, and access all files on the computer. So an attacker having unauthorised access to an Administrator account can be far more damaging than accessing a standard user account.

Use two-factor authentication (2FA) on your important accounts such as email. This means that even if an attacker knows your passwords, they still won't be able to access that account.



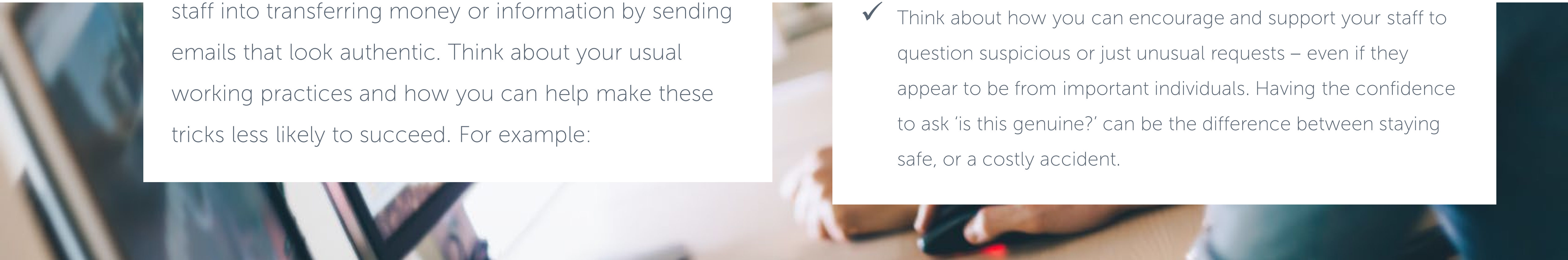
5 TIPS FOR DODGING PHISHING ATTACKS

2. Think about how you operate

Consider different ways someone might target your business, and make sure your staff all understand normal ways of working, so that they're better equipped to spot requests that are out of the ordinary.

Common tricks include sending an invoice for a service that you haven't used, so when the attachment is opened, malware is automatically installed (without your knowledge) on your computer. Another is to trick staff into transferring money or information by sending emails that look authentic. Think about your usual working practices and how you can help make these tricks less likely to succeed. For example:

- ✓ Do staff know what to do with unusual requests, and where to get help?
- ✓ Ask yourself whether someone impersonating an important individual (a customer or manager) via email should be challenged (or have their identity verified another way) before action is taken.
- ✓ Do you understand your regular business relationships? Scammers will often send phishing emails from large organisations (like Microsoft) in the hope that some of the email recipients will have a connection to that company. If you get an email from an organisation you don't do business with, be suspicious.
- ✓ Think about how you can encourage and support your staff to question suspicious or just unusual requests – even if they appear to be from important individuals. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly accident.



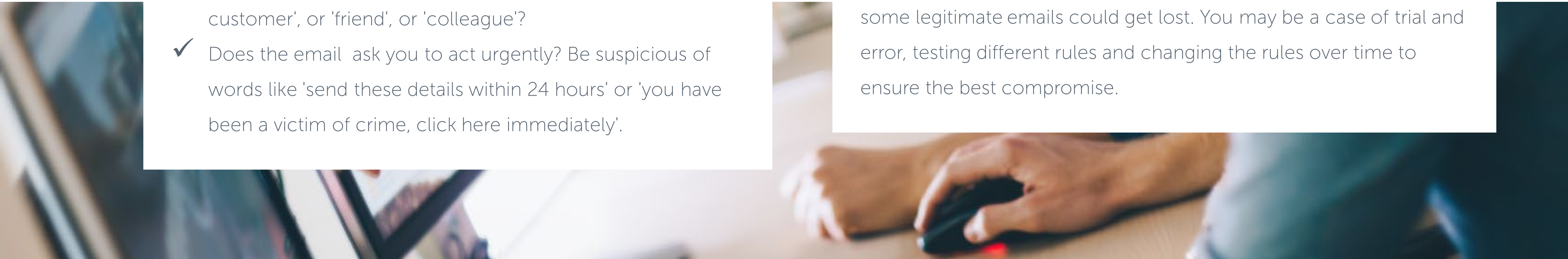
5 TIPS FOR DODGING PHISHING ATTACKS

3. Check for the obvious signs of phishing

Expecting your staff to identify and delete all phishing emails is an impossible request and would have a detrimental effect on business productivity. However, many phishing emails still fit the mould of a traditional attack, so look for the following warning signs:

- ✓ Many phishing have poor spelling, grammar and punctuation. Others will try and create official-looking emails by including logos and graphics. Is the design (and quality) what would you'd expect from a large organisation?
- ✓ Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'?
- ✓ Does the email ask you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- ✓ Look out for emails that appear to come from a high-ranking person within your organisation, requesting a payment is made to a particular bank account. Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- ✓ If it sounds too good to be true, it probably is.

Email filtering services attempt to send phishing emails to spam/junk folders. However, the rules determining this filtering need to be fine-tuned for your business' needs. If these rules are too open and suspicious emails are not sent to spam/junk folders, then users will have to manage many emails, adding to their workload and leaving open the possibility of a click. However, if your rules are too strict, some legitimate emails could get lost. You may be a case of trial and error, testing different rules and changing the rules over time to ensure the best compromise.



5 TIPS FOR DODGING PHISHING ATTACKS

Netitude

4. Report all attacks

Make sure that your staff are encouraged to ask for help if they think that they might have been a victim of phishing. It's important to take steps to 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 will discourage them from reporting in future and can make them so fearful that they spend excessive time and energy scrutinising every single email they receive.

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 cybercrime reporting centre. If you are in Scotland contact Police Scotland on 101.

5 TIPS FOR DODGING PHISHING ATTACKS

Netitude

4. Get to know your digital footprint

Attackers use publicly available information about your organisation and staff to make their phishing messages more convincing – a tactic known as Social Engineering. This is often taken from your website and social media accounts (information known as a 'digital footprint').

- ✓ Understand the impact of information shared on your organisation's website and social media pages. What do your website visitors need to know, and which detail are unnecessary (but could be useful for attackers)?
- ✓ Be aware of what your partners, contractors and suppliers give away about your organisation online.
- ✓ Help your staff understand how sharing their personal information can affect them and your organisation.

WHAT NEXT?

If you want to improve your cyber security further, then you should look into the Cyber Essentials scheme. Achieving the certification will demonstrate to your clients (or prospective clients) that you take the protection of their data seriously. It also helps to win government contracts and offers insurance cover for cyber security breaches. With the certification costing £300 per year, it's a cheap option to keep your business' bases covered.

At Netitude, we guarantee all our Managed IT clients a pass in Cyber Essentials as standard. If you'd like to find out more about our Managed IT options and what else is included, click here.

hello@netitude.co.uk ✉

www.netitude.co.uk 🌐

0333 2412323 ☎