

The background of the entire page is a blurred, bright office interior. In the foreground, a woman with glasses is seated at a table, working on a laptop. In the background, a man in a plaid shirt stands with his hands on his hips, and a woman in a white shirt and blue jeans stands near a counter, looking at a tablet. The office has large windows, modern furniture, and several pendant lights hanging from the ceiling.

ILUX[®]

Multi Factor Authentication



Think of your data security in the same way that you keep your car safe: if you left your keys for anyone to use, your car is more likely to be stolen.

But imagine if you kept your keys in a locked safe:



that can only be accessed with a security code



with a code that changes all the time



you can only access the code from a secure phone app



which needs your fingerprint or face to verify that it is really you

Your keys are now behind layers of extra security, making the potential criminal's life harder.

This is effectively what Multi-Factor Authentication (MFA) is, and it has become the industry standard way of protecting your company's data. The latest research demonstrates that cyber criminals are using increasingly sophisticated techniques to bypass security.

A cyber attack on your business is potentially devastating. What would the consequences be for your business if your customer or employee private data was stolen and held to ransom?

Are you prepared for the reputational damage a data breach can cause? Or the phone calls to your clients?

That's why it's vital to think seriously about how best to protect the information you hold, and about the data your team members are able to access.

Along with good staff training, MFA is one of the strongest security tools available.

But how does MFA work in practice? And what does it actually mean for your business?



The more barriers you put in the criminals' way, the harder you make it for them to break into your systems"

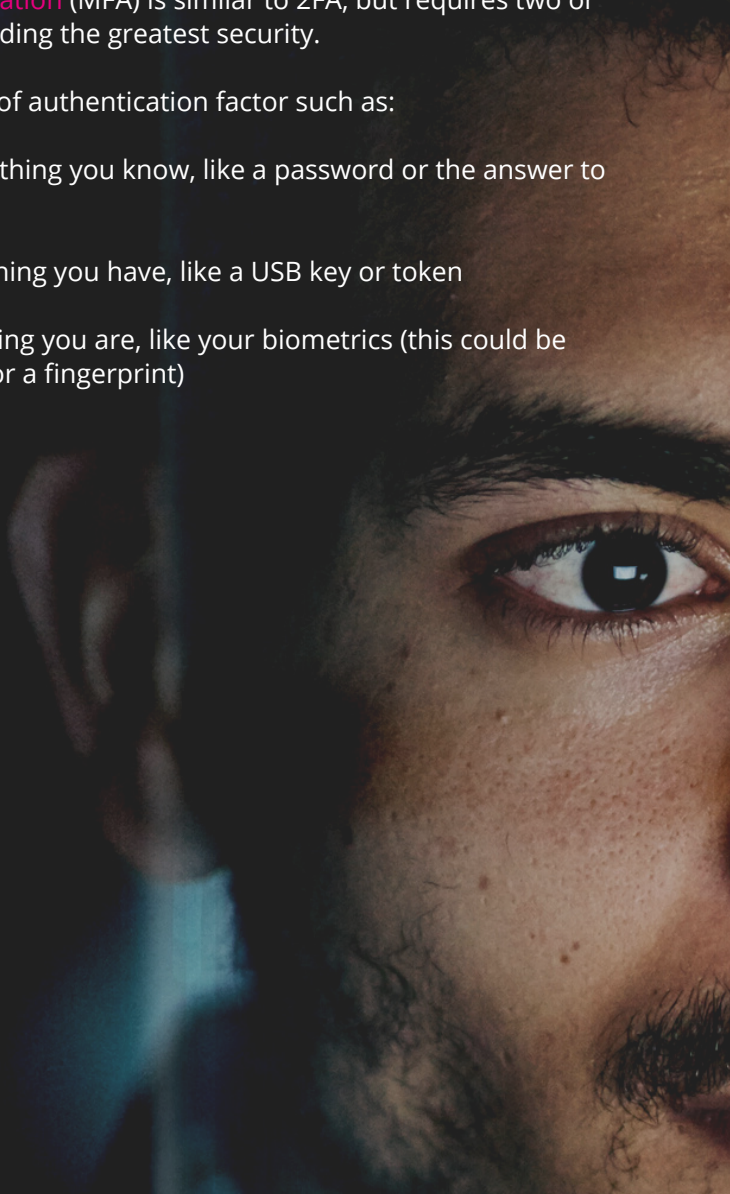
Single-Factor Authentication is not enough. An application, account, or system requires you to authenticate your identity using just one piece of 'evidence'. Usually, this is your password.

Two-Factor Authentication or 2-step verification, is better. 2FA requires you to identify yourself using two different factors, such as a password plus a single-use code that's sent to your phone. 2FA is a form of MFA.

Multi-Factor Authentication (MFA) is similar to 2FA, but requires two or more identifiers, providing the greatest security.

MFA uses three types of authentication factor such as:

- Knowledge - Something you know, like a password or the answer to a question
- Possession Something you have, like a USB key or token
- Inherence Something you are, like your biometrics (this could be facial recognition or a fingerprint)



Which is the **right** solution for you?

Theoretically MFA is the most secure solution, especially for a business. However, MFA is still only as strong as the authentication methods you choose. If it's not implemented in the right way, it can create unintended issues.

MFA's layered approach to security means it is effective. But it needs to be balanced; too many layers can add 'friction' to the log in process.

By making your people jump through too many hoops there's a chance that they will find a way to by-pass it. If people start using their personal email addresses, for example, because it's too much of a pain to log in at work, that's the opposite of solid security.

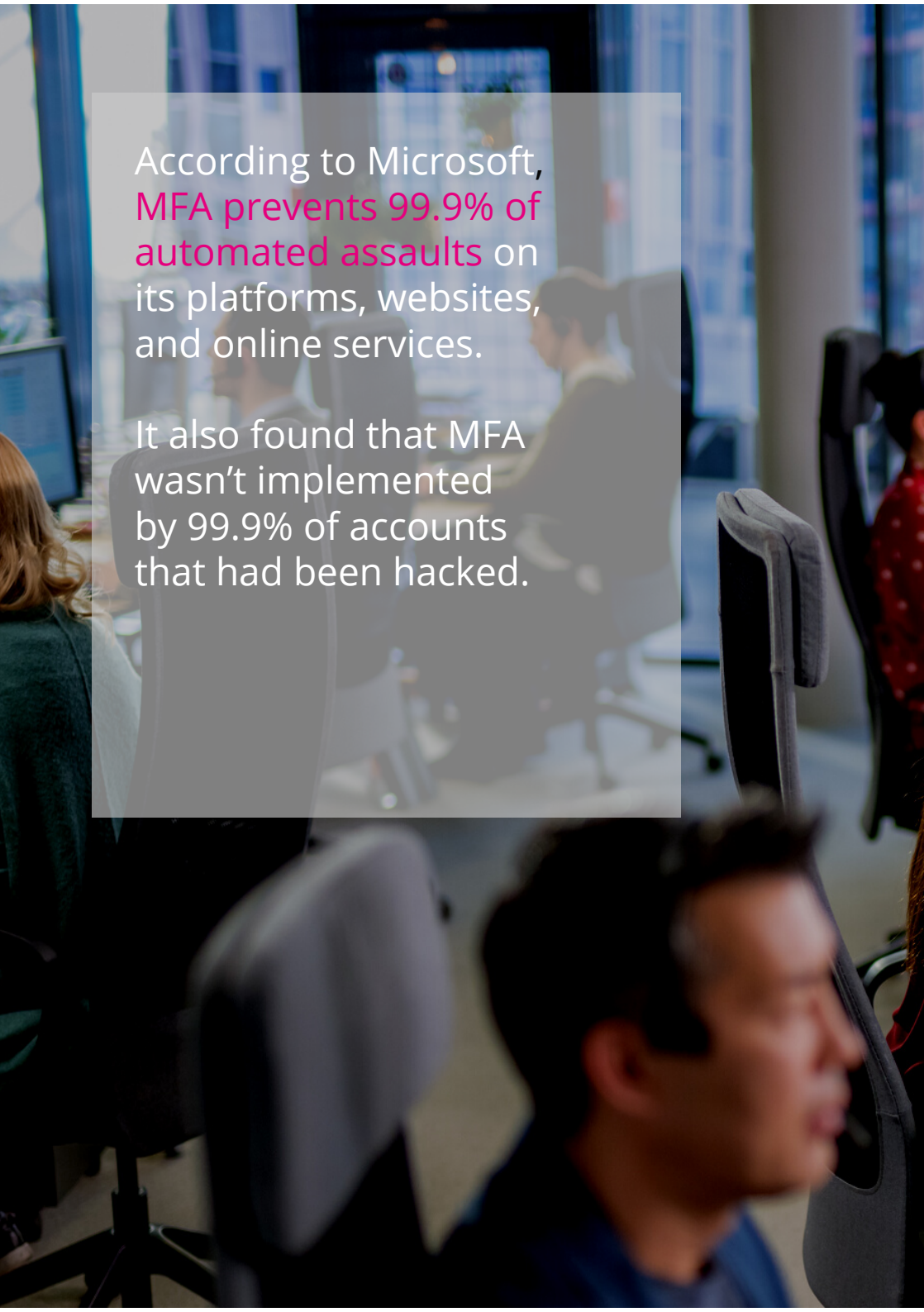
So a good MFA solution should be unobtrusive and adapt to different situations. For instance, it could be set up to apply different levels of authentication depending on the nature of each login attempt.

It could link team members to their trusted devices. If that matches what's usual, great. However, if they log in using an unrecognised device, or it seems suspicious, the system will ask for further information.

Why is it so important for you?

Many small businesses simply don't survive a successful cyber attack. In particular, the impact, disruption and cost of ransomware attacks can devastate your chances of survival.

But implementing MFA can prevent the vast majority of these attacks.

A blurred office scene with several people working at computers. The background shows office desks, chairs, and large windows. The text is overlaid on a semi-transparent grey box.

According to Microsoft,
MFA prevents 99.9% of
automated assaults on
its platforms, websites,
and online services.

It also found that MFA
wasn't implemented
by 99.9% of accounts
that had been hacked.

Microsoft's numbers speak for themselves. Here are our top six reasons to adopt MFA in your business, today.

1. It can protect your business from weak passwords

We talk about this all the time – weak employee passwords are a real risk to your business. However, a recent study still shows that passwords like '123456' and 'Passw0rd' are amongst the most commonly used.

Weak passwords open the door to all kinds of data breaches.

'Password-dumper' malware, which steals login credentials from victims' devices, was involved in a third of malware-related data breaches in 2020. And 80% of hacking-related breaches involved passwords in some way.

MFA prevents this. The cyber criminals may still try to steal your password but they are less likely to have access to your second and third factors of authentication – such as your fingerprint.

2. It prevents other methods of password theft

If a criminal can't break into your network to steal passwords, they have other methods that are equally successful. 'Phishing' attacks trick victims into giving away sensitive information using scam emails, SMS, or phone calls. And 'pharming' involves redirecting a website's traffic to a fake site, run by the criminals, where they steal data or install malware.

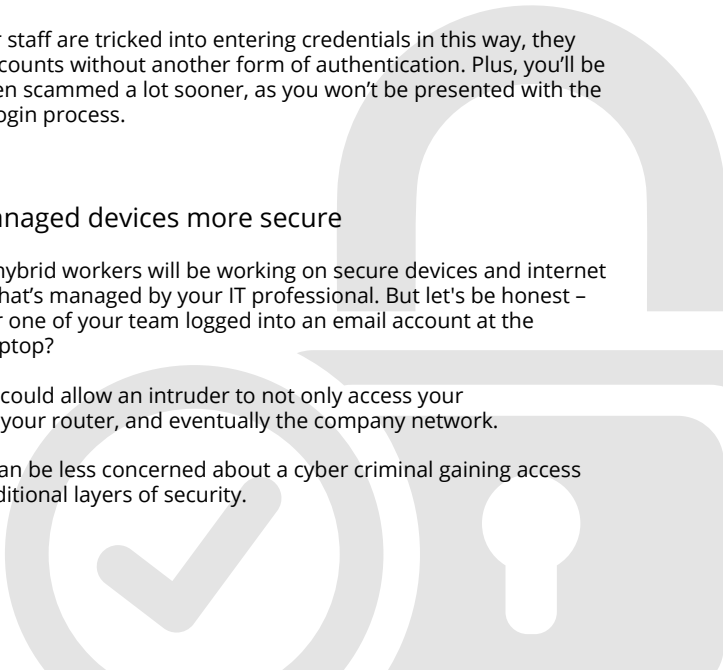
So even if you or one of your staff are tricked into entering credentials in this way, they are unable to access your accounts without another form of authentication. Plus, you'll be alerted to the fact you've been scammed a lot sooner, as you won't be presented with the authentication stage of the login process.

3. It makes using unmanaged devices more secure

Ideally, all your remote and hybrid workers will be working on secure devices and internet connections, using security that's managed by your IT professional. But let's be honest – how many times have you or one of your team logged into an email account at the weekend using a personal laptop?

It might feel harmless, but it could allow an intruder to not only access your unmanaged device, but also your router, and eventually the company network.

Using MFA means that you can be less concerned about a cyber criminal gaining access in this way, thanks to the additional layers of security.



4. It allows your other security tools to perform properly

Once a criminal has stolen over-simplified login credentials, they can bypass antivirus software and firewalls in the same way that an authorised employee could – with a bit of knowledge. This allows them to disarm your security and wreak havoc, all without you noticing anything is wrong.

With MFA in place, this cannot happen. Cyber criminals can't use stolen credentials to access your network, because they don't have the ability to pass these second or third identity checks.

MFA can also act as an alert that your accounts are at risk. If someone attempts to log in, the user will receive a secondary authorisation prompt that wasn't requested. This can be immediately reported to your IT team.

5. It keeps you compliant with your regulators

When you handle and store sensitive data, your business must comply with legislation that states the need strong authentication processes to be in place. MFA is a tool to keep the private data of customers, suppliers, and employees out of the wrong hands.

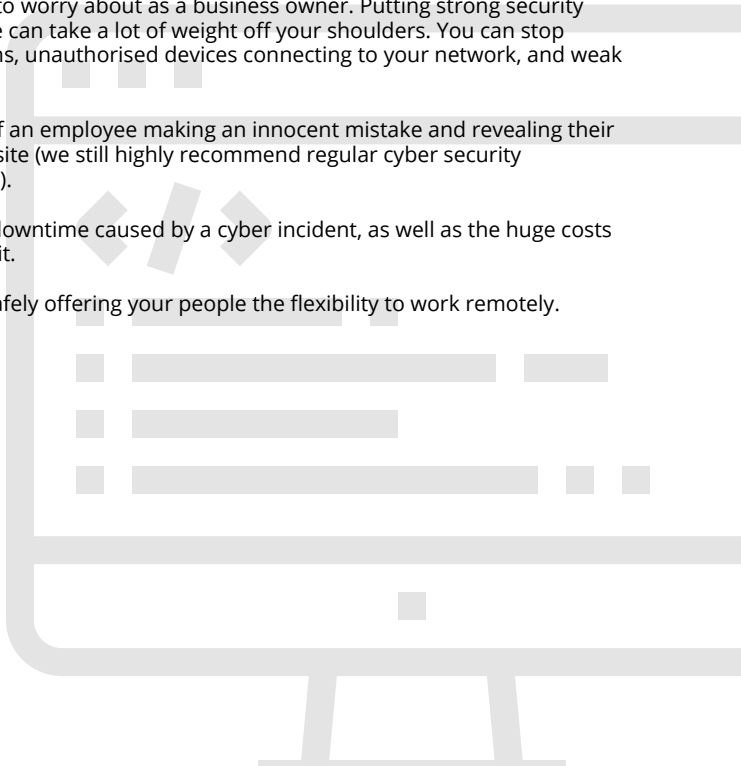
6. It can save a lot of stress

There's always something to worry about as a business owner. Putting strong security measures like MFA in place can take a lot of weight off your shoulders. You can stop worrying about cyber scams, unauthorised devices connecting to your network, and weak passwords.

There is also less chance of an employee making an innocent mistake and revealing their credentials to a fake login site (we still highly recommend regular cyber security awareness training though).

You can worry less about downtime caused by a cyber incident, as well as the huge costs involved with dealing with it.

And you can relax about safely offering your people the flexibility to work remotely.



MFA isn't the answer to all your cyber security concerns, but it slams the door on the majority of today's cyber crimes.

If it is not enabled across your network and its systems, you might be leaving that door open to a cyber attack at any time.



ILUX[®]

IT that powers success

T: 0333 311 0109

www.ilux.co.uk