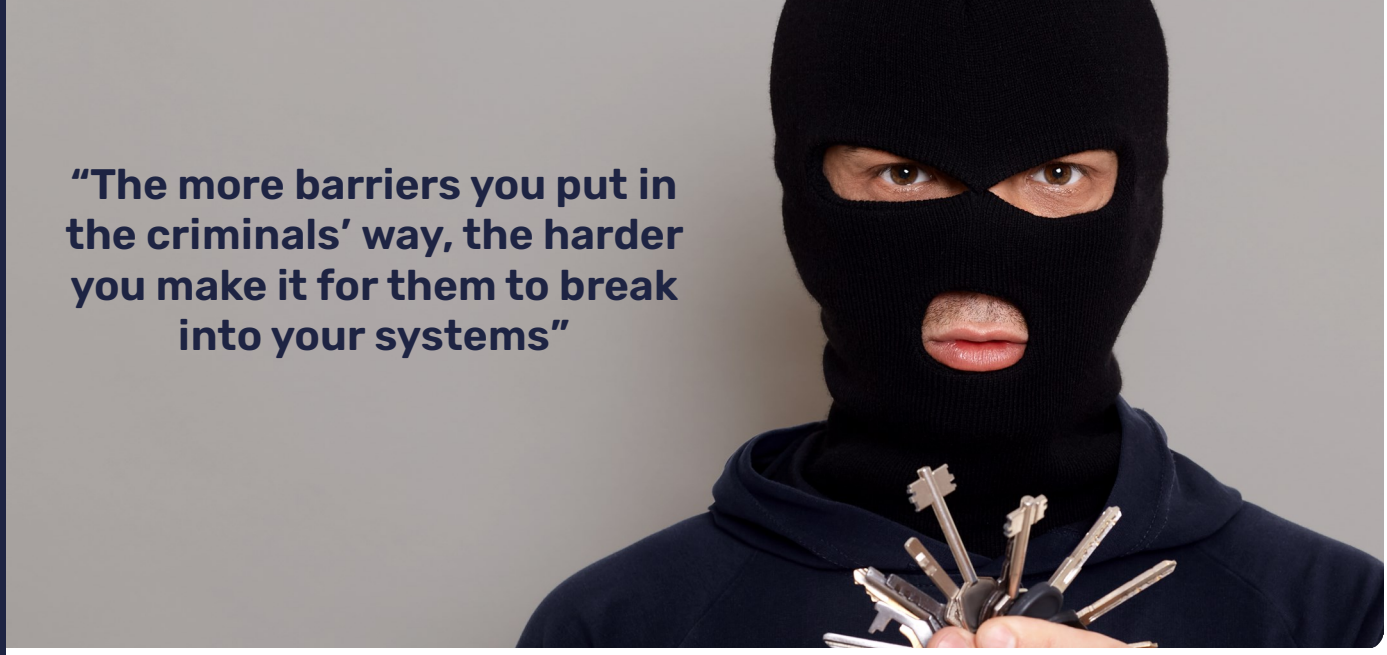
All businesses should adopt MFA. Now

If you haven't upgraded your security, **you could be making life far too easy for an intruder.**

blackstone IT
IT Support & Solutions



If a criminal knew where you lived, and could easily steal the keys from your pocket, it wouldn’t be a lot of work for them to steal things from your home.

But imagine if you kept your keys in a massive locked safe. And not just any safe…

- **A safe that can only be accessed with a security code**
- **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’s really you**

You’ve now put your keys behind layers of extra security, making that criminal’s life a whole lot harder.

What you’ve used here is called Multi-Factor Authentication, also known as MFA. And it has become the standard way to protect your business’s data.

Cyber criminals use increasingly sophisticated techniques to bypass security. So the more barriers you put in their way, the harder you make it for them to break into your systems.

A cyber attack on a small business can be devastating. What would the consequences be for your business if your customers’ private information was stolen and held to ransom?

Can you imagine making that phone call to tell them what’s happened?

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?

Here’s everything you need to know.

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, also called 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, with a view to providing the greatest security.

MFA might use three types of authentication factor:

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. And if it's not implemented in the right way, it can create unintended issues.

For instance, MFA's layered approach to security is what makes it strong. But too many layers can add 'friction' to the log in process. Make your people jump through too many hoops to do what they need to do, and there's a chance that they'll just stop using it. And if people start using their personal email addresses 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 will 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. So it may link team members to their trusted devices. If that matches what's usual, great. Only if it's an unrecognised device, or it seems suspicious, will it 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.

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 6 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 simply won't cut it.

But a recent study showed that, *still,* passwords like '123456' and 'Passw0rd' are amongst the most commonly used. Aargh!

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. Because while cyber criminals may still try to steal your password, 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

Even 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're tricked into entering credentials in this way, the fraudsters still won't be able to access your accounts without another form of authentication. And 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 be honest – how many times have you logged into your email account at the weekend using your 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.

If you use MFA 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

If a criminal steals over-simple 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 amiss.

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

MFA can also act as an alert that your accounts are at risk. If someone attempts to log in, you'll receive a secondary authorisation prompt that you didn't request. This can be immediately reported to ensure everything is safe and sound.

5. It keeps you compliant

When you handle and store sensitive data, your business must comply with **local laws that state you need strong authentication processes in place**. MFA is a strong 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.

Better still, there's 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 prayers. **But it slams the door on the majority of today's cyber crimes.**

So if you don't already have it enabled across your network and its systems, **you might be leaving that door open to a cyber attack at any time.**

MFA solutions are just one of the services we provide to our clients every day. If you're worried about protecting your business, get in touch now.

CALL: 01292 811 810
EMAIL: info@blackstone-it.co.uk
WEBSITE: www.blackstone-it.co.uk

blackstone IT
IT Support & Solutions