Implement MFA (Multi-Factor Authentication)

If you have not enhanced your security, you may be making it too easy for an intruder to gain unauthorised access.

PiSYS .net

A COMCEN COMPANY

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

If a criminal knew your address and had easy access to steal your keys from your pocket, it would not take much effort for them to steal your belongings.

Now envision a scenario where you secure your keys in an enormous 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**

By doing so, you have added multiple layers of security to safeguard your keys, making it significantly more challenging for the criminal to steal them.

This method is known as Multi-Factor Authentication, or MFA, which has become the industry-standard approach to protecting business data.

By adding extra security layers, you have significantly increased the level of difficulty for a potential criminal to steal your keys.

By introducing more barriers, you can make it increasingly challenging for intruders to breach your systems.

The impact of a cyber attack on a small business can be catastrophic. Have you considered the potential consequences if a cybercriminal were to steal your customers' confidential information and demand a ransom payment?

Can you envision having to make that dreaded phone call, disclosing to them what has occurred?

It is crucial to consider the best methods of safeguarding the information you possess and limiting access to sensitive data by your team members. Alongside comprehensive staff training, Multi-Factor Authentication (MFA) is among the most potent security tools at your disposal.

Here’s everything you need to know.

Relying solely on Single-Factor Authentication is inadequate. It necessitates authenticating your identity utilising only one piece of "evidence," typically your password, to access an application, account, or system.

2FA

2FA, also known as two-factor authentication, is a more secure method. It involves verifying your identity using two different factors, like a password and a unique code that's sent to your phone. This is a form of MFA.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) goes beyond 2FA by requiring two or more forms of identification, in order to provide the highest level of 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 solutions are best for you?

Although MFA is considered the most secure solution, particularly for businesses, it's only as strong as the chosen authentication methods. Improper implementation of MFA can also lead to unintended issues

MFA's strength lies in its layered approach to security. However, adding too many layers can make the log in process cumbersome, creating friction for users. If the authentication process becomes too complicated, people may stop using it altogether, or worse, resort to using their personal email addresses for work-related tasks, which undermines the security of the system. Therefore, it's crucial to strike a balance between the level of security and user experience to ensure MFA's effectiveness.

So a good MFA solution should be unobtrusive and will adapt to different situations.

IMPORTANCE

Small businesses often fail to recover from a successful cyber attack, especially the impact, disruption, and cost associated with ransomware attacks, which can significantly lower their chances of survival.

By implementing MFA, a vast majority of these attacks can be prevented.

Microsoft reports that implementing MFA can prevent 99.9% of automated attacks on its platforms, websites, and online services, and further found that 99.9% of accounts that were compromised did not have MFA enabled.

Microsoft's numbers speak for themselves. Here are our top 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 'Superman' are amongst the most commonly used.

Using weak passwords increases the risk of data breaches.

"Password-dumper" malware, a type of malicious software that steals login information from compromised devices, was responsible for one-third of all data breaches caused by malware in 2020.

Additionally, 80% of breaches caused by hacking involved the exploitation of passwords in some capacity.

MFA can mitigate these risks by requiring multiple factors of authentication, making it more difficult for attackers to access accounts even if they manage to obtain the password.

2. It prevents other methods of password theft

While network intrusion may not be the only method used by criminals to obtain passwords, phishing and pharming attacks can be just as effective. Phishing attempts involve the use of fraudulent emails, SMS, or phone calls to dupe victims into divulging sensitive information, while pharming redirects website traffic to a bogus site run by criminals who steal data or install malware. However, even if you fall for one of these tactics and provide your login credentials, the fraudsters will still need additional authentication to access your accounts. Additionally, since the authentication phase of the login process won't be presented, you'll be alerted to the scam much sooner.

3. Making unmanaged devices more secure

In an ideal scenario, your remote and hybrid workers should work on secure devices and internet connections managed by your IT professional. However, it's important to ask yourself how often you've accessed your email account on your personal laptop over the weekend. While this may seem harmless, it could provide an opportunity for a cybercriminal to gain access to your unmanaged device, your router, and eventually the company network.

By implementing Multi-Factor Authentication (MFA), you can reduce your concern about cybercriminals gaining access through this route, as MFA provides additional layers of security.

4. It allows your other security tools to perform properly

In the event that a criminal obtains simplistic login credentials, they can circumvent firewalls and antivirus software just as easily as an authorized user could with the appropriate knowledge. This grants them the ability to disarm your security measures and cause significant damage, all while avoiding detection.

However, with MFA in place, this type of attack is not possible since cybercriminals lack the capability to pass the secondary and even tertiary identity checks. MFA also serves as an alert mechanism, notifying you of potential account compromises. In the event of an unauthorized login attempt, you will receive a prompt for secondary authorization that you did not initiate. You can then report this incident immediately, ensuring the safety of your accounts.

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

As a business owner, there is always a multitude of concerns to manage. However, implementing robust security measures such as MFA can significantly alleviate the burden. With MFA, concerns about cyber scams, unauthorized devices connecting to your network, and weak passwords can be greatly reduced.
Moreover, the likelihood of an employee accidentally disclosing their credentials to a fake login site decreases. (Nevertheless, regular cybersecurity awareness training is still highly recommended.) This can result in less downtime caused by cyber incidents and decreased costs associated with addressing them.

By implementing MFA and other robust security measures, you can confidently offer your workforce the flexibility to work remotely without worrying about compromising the security of your organisation's network.

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.

At Pisys, we offer a range of services to our clients, including MFA solutions, to ensure the security and protection of their businesses. If you're concerned about safeguarding your organisation, please don't hesitate to reach out to us for assistance. We are ready to help you address any cybersecurity challenges and implement the right solutions to protect your business.

This is how you can get in touch with us:
CALL: 01792 464748
EMAIL: hello@pisys.net
WEBSITE: www.pisys.net

PiSYS .net
A COMCEN COMPANY
We make IT easy