


3 MIN READ

6 WAYS SMALL BUSINESSES CAN STAY SECURE

 Blead Cyber Security | Janine Griffiths



6 ways small businesses can stay secure

With the prevalence of cybersecurity attacks, all businesses are at risk of a cyberattack, regardless of the size or industry. Although some hackers may target larger businesses as the reward is more lucrative, many threat actors prefer to go after small-medium businesses as it is often the path of least resistance. Smaller businesses often spend less time and money on cybersecurity and have access to large amounts of customer information, therefore making them an attractive target. To make matters worse, if an SMB falls victim to an attack, they are less likely to be able to pay ransom for ransomware attacks and may not have systems in place to recover quickly from an attack resulting in potential lost revenue and custom.

Thankfully many SMBs understand the importance of staying secure and are starting to make cybersecurity a key focus in their wider business plans. In this article we will discuss 6 ways small businesses can increase their security posture

and reduce the chance of an attack.

Enable Multifactor Authentication

For many years the best method of keeping an account secure was to have a strong password. This is still true now and employees should have long and complex passwords, however it should not be the only line of defence to stop a hacker gaining access to an account. Multifactor authentication (MFA) is an authentication process where a user must provide two or more forms of identification to login to their account. There are different options businesses can use to enable MFA including the use of an app, a text message, or biometrics to authenticate a login. If MFA is enabled on Azure Active Directory, it is also possible to use single sign on. This allows employees to log in to their Microsoft account securely, and all other Microsoft accounts and SaaS applications are logged in at the same time. This increases security and creates a better user experience for employees of an SMB.

Provide awareness training for employees

One of the best methods of cybersecurity protection is education, awareness, and a strong security culture within an organisation. Through education of cybersecurity fundamentals and awareness of common attack vectors employees are better equipped to notice an attack attempt before it is too late. When implementing awareness training within an SMB it should be a constant process to ensure employees retain the information and it should be delivered in an engaging manner. As part of this training, businesses can run simulated phishing attempts to ensure employees would be able to spot a real attempt. Through regular education businesses can start to develop a stronger security culture which decreases the risk of a security incident and leads to more engaged employees.

Keep software and systems up to date

One of the easiest ways to keep your business safe from an attack is to keep all software and operating systems up to date. Many cyberattacks, especially those of ransomware, can be easily avoided by ensuring systems are up to date, however many users delay patches and updates for convenience. Most devices now have automatic updates turned on by default, but it is important for employees to understand that they should not delay patches for longer than is necessary. It is acceptable to delay them whilst employees save their current work, but all updates should be run as soon as possible to keep a business safe.

Stop phishing attempts in their tracks

Phishing attacks are one of the most common attack vectors and have been for a long time now. Some phishing attempts can be easy to spot due to poor spelling and grammar and the sender being unknown to the receiver. However, some phishing attacks can be difficult to notice as they have highly targeted messaging and complex domain spoofing. In order for businesses to safeguard themselves from these more sophisticated phishing attempts it is beneficial to have software in place that stops phishing emails before they even reach an inbox. Mimecast uses AI to provide protection from impersonation attempts, malicious URLs, address sender spoofing and malicious attachments.

Set appropriate access levels

A common mistake that SMBs make is allowing employees access to all company data. This is dangerous as if a hacker gets access to any employee account, they then have access to all the company's data and its customers' data. SMBs should use the principle of least privilege access. This concept states that a user should be given the minimum level of access or permissions required to do their job. This not only reduces the cyber attack surface, but it also can stop the spread of malware and streamline compliance and audits.

Have a disaster recovery plan in place

In the world of cybersecurity, it is best practice to avoid an attack in the first place, rather than recover from one after the fact. However, even the most security conscious of businesses may make a mistake and fall victim to an attack. To minimise downtime and ensure business continuity, SMBs should have a disaster recovery plan in place. This plan describes how an organisation can quickly resume work after an unplanned incident. This incident could be anything from simple hardware failure to a widespread ransomware attack. The most important factor to any disaster recovery plan is a backup strategy. Using a product such as Acronis Cyber Protect not only handles backup, but also have built in ransomware protection with automatic rollback to ensure that an SMB

If you are an SMB owner, there is too much at stake to not start focusing on protecting your business from a cyberattack. If you want to find out how to implement any of the methods above, or if you want to find out more about how to protect your business, get in touch today.

([//www.bleamcybersecurity.co.uk/blog/the-6-worst-cyberattacks-of-2021](https://www.bleamcybersecurity.co.uk/blog/the-6-worst-cyberattacks-of-2021))

The 6 worst cyberattacks of 2021

([//www.bleamcybersecurity.co.uk/blog/the-6-worst-cyberattacks-of-2021](https://www.bleamcybersecurity.co.uk/blog/the-6-worst-cyberattacks-of-2021))



Bleam Cyber Security

([//www.bleamcybersecurity.co.uk/blog/author/bleam-cyber-security](https://www.bleamcybersecurity.co.uk/blog/author/bleam-cyber-security)) : May 3, 2022 10:15:00 AM

2021 was a year of digital transformation for all businesses. The widespread adoption of remote and hybrid work has resulted in employees being more...

Cyber security

([//www.bleamcybersecurity.co.uk/blog/tag/cyber-security](https://www.bleamcybersecurity.co.uk/blog/tag/cyber-security))

Read More ([//www.bleamcybersecurity.co.uk/blog/the-6-worst-cyberattacks-of-2021](https://www.bleamcybersecurity.co.uk/blog/the-6-worst-cyberattacks-of-2021))

(//www.bleamcybersecurity.co.uk/blog/91-of-cyber-attacks-start-with-an-email)

91% of cyber attacks start with an email
(//www.bleamcybersecurity.co.uk/blog/91-of-cyber-attacks-start-with-an-email)



Bleam Cyber Security

(//www.bleamcybersecurity.co.uk/blog/author/bleam-cyber-security) : Mar 21, 2022 2:01:59 PM

Email is the most common type of threat vector, and 23% of people click on malicious emails. It only takes one click for your whole network to be...

Cyber security

(//www.bleamcybersecurity.co.uk/blog/tag/cyber-security)

Read More (//www.bleamcybersecurity.co.uk/blog/91-of-cyber-attacks-start-with-an-email)

(//www.bleamcybersecurity.co.uk/blog/an-exciting-update)

An exciting update...

([//www.bleamcybersecurity.co.uk/blog/an-exciting-update](https://www.bleamcybersecurity.co.uk/blog/an-exciting-update))



Bleam Cyber Security

([//www.bleamcybersecurity.co.uk/blog/author/bleam-cyber-security](https://www.bleamcybersecurity.co.uk/blog/author/bleam-cyber-security)) : Feb 28, 2022 11:20:37 AM

Bleam Cyber Security has undergone an exciting acquisition. We are thrilled to announce that we have been acquired by Simpson Associates, (<https://www.simpson-associates.co.uk/>) a leading...

News ([//www.bleamcybersecurity.co.uk/blog/tag/news](https://www.bleamcybersecurity.co.uk/blog/tag/news))

Read More ([//www.bleamcybersecurity.co.uk/blog/an-exciting-update](https://www.bleamcybersecurity.co.uk/blog/an-exciting-update))

SERVICES

Managed Services

Managed Detection & Response for Email

(//www.bleamcybersecurity.co.uk/email-detection-response)

Managed Detection & Response

(//www.bleamcybersecurity.co.uk/managed-detection-and-response)

Managed Sentinel

(//www.bleamcybersecurity.co.uk/managed-sentinel)

Managed Secure Access

Managed Private Access

(//www.bleamcybersecurity.co.uk/managed-secure-access)

Managed Internet Gateway

(//www.bleamcybersecurity.co.uk/managed-secure-private-access)

Microsoft Security

Managed Azure Sentinel

(//www.bleamcybersecurity.co.uk/managed-sentinel)

Azure Security Assessment

(//www.bleamcybersecurity.co.uk/azure-security-assessment)

PROFESSIONAL SERVICES

Penetration Testing

(//www.bleamcybersecurity.co.uk/penetration-and-security-testing)

Retained Incident Response

(//www.bleamcybersecurity.co.uk/retained-incident-response)

Security Standard Readiness Services

(//www.bleamcybersecurity.co.uk/security-standard-readiness)

Information Security Programme

(//www.bleamcybersecurity.co.uk/virtualciso)

Cyber Essentials (//www.bleamcybersecurity.co.uk/cyber-essentials)

COMPANY

About Us (//www.bleamcybersecurity.co.uk/about-bleam-cyber-security)

[Careers \(//www.bleamcybersecurity.co.uk/careers\)](https://www.bleamcybersecurity.co.uk/careers)

[FAQs \(//bleamcybersecurity-25176453.hs-sites-eu1.com/frequently-asked-questions-1\)](https://bleamcybersecurity-25176453.hs-sites-eu1.com/frequently-asked-questions-1)

[Blog \(//www.bleamcybersecurity.co.uk/blog\)](https://www.bleamcybersecurity.co.uk/blog)

[Events \(//www.bleamcybersecurity.co.uk/events\)](https://www.bleamcybersecurity.co.uk/events)



[twitter \(https://twitter.com/BleamCyber\)](https://twitter.com/BleamCyber)

[bleamcybersecurity.co.uk \(//www.bleamcybersecurity.co.uk\)](https://www.bleamcybersecurity.co.uk)

[in \(https://www.linkedin.com/company/bleamcybersecurity\)](https://www.linkedin.com/company/bleamcybersecurity)

[Privacy Policy \(//www.bleamcybersecurity.co.uk/privacy-policy\)](https://www.bleamcybersecurity.co.uk/privacy-policy)

[Cookie Policy \(//www.bleamcybersecurity.co.uk/cookie-policy\)](https://www.bleamcybersecurity.co.uk/cookie-policy)

© 2022 Bleam Cyber Security is a wholly owned division of Simpson Associates Information Services Ltd. Regency House, York Business Park, Poppleton, York, North Yorkshire YO26 6RW 0114 303 5130 info@bleam.co.uk