arcsystems

Is your Microsoft 365 secure?

Troubleshoot your weak spots
with our assessment.

If your business runs on Sharepoint, OneDrive and Teams, you'll know how essential the Microsoft 365 suite is to your business.

They're versatile, plug-and-play solutions that just work.

However, if you rely on out-of-the-box email security, backup and antivirus tools that come with MS365, you could be vulnerable to data loss, cyber-attacks... and a lot of time and money to pick up the pieces.

Want to see where your trouble spots are?

Take our assessment to see what you need to do to make your MS365 suite more productive, protected and powerful.

Email Security

1. How do you deal with malicious emails?

A

I delete them in my inbox, or they're automatically sent to a spam folder.

B

Any suspicious emails are intercepted by MS Defender for me.

C

My email security system automatically identifies ransomware links and impersonation attempts.

2. What measures do you take to ensure that sensitive data is transmitted securely via email?

A

I check all emails thoroughly and run them by relevant colleagues.

B

We have a Data Loss Prevention (DLP) policy that stops sensitive information being shared.

C

We have the policy above, but we also have email encryption as standard.

Data Backup

1. How do you keep your business' data backed up?

A

Microsoft 365 handles this for me.

B

We use OneDrive and Sharepoint, which gives us some time-sensitive recovery options.

C

We have a managed backup solution that holds all of our data securely, on and off-site.

2. Truthfully, how easy would it be to recover all of your data in the event of a disaster?

A

If all of my data was wiped or held to ransom, I wouldn't know how to recover it.

B

I might lose data on my device, but we rely on Microsoft's tools to protect our data.

C

Our back-up solution (e.g. Datto Backup for Microsoft 365) lets us recover all of our data swiftly.

Antivirus

1. How would you describe your antivirus protection?

A

We removed MS Defender's antivirus – it's intrusive, and we rarely see threats anyway.

B

We use MS Defender to run scans and block access to malicious sites.

C

We have an endpoint protection solution, including encryption and a managed firewall.

2. Can you monitor your employees' activity for any safety concerns?

A

No, and I wouldn't consider it.

B

No – but we do have blacklists to stop employees from accessing malicious sites.

C

Yes – we can see reports that help us to identify threats, and even time-wasting sites.

Single Sign-on and Multi-factor Authentication

1. Do you have SSO/multi-factor authentication enabled for your MS365 software?

A

No, we just use password protection.

B

Yes, we use the Authenticator app/text message authentication, as well as a BitLocker app.

C

Yes, but we supplement it with other security measures, such as email and firewall protection.

Now find out your results...

Mostly As - Vulnerable

You are very vulnerable to data loss and security breaches. You are using basic security measures, there's a far greater chance of human error, and you don't have a security strategy in place.

Advice: Take immediate action to enable Microsoft-recommended security features, and plan to take broader measures, see advice under 'Mostly Cs'.

Mostly Bs - Basic Protection

You have a good foundation with Microsoft Defender and in-built security and back up tools. However, this only stops basic attacks, and if your data is compromised or lost, it's unlikely that you will recover it all back.

Advice: Ensure you check antivirus, firewall and email security settings immediately, and see advice under 'Mostly Cs'.

Mostly Cs - Good Protection

You are supplementing MS Defender with additional tools such as Mimecast for email, Sophos Intercept-X for end-point protection, and Datto backup for Microsoft 365, which give robust protection against threats to your virtual environment.

Advice: Which areas did you answer A or B? These are your trouble spots that need attention, so even if you've answered mostly Cs, there's more you can do to protect your vital IT applications.

Microsoft 365 is a business-critical tool, but you need to ensure relevant solutions are in place to protect your Microsoft environment. However this assessment went for you, Arc Systems can help.

We partner with industry leaders in email security, backup and cybersecurity to provide solutions that protect your Microsoft 365 suite from the inside out.

Backup

Microsoft 365 retains data for a short time, but if you need it to be always available, Arc can provide managed backup and disaster recovery with Datto-powered cloud backup to protect your data.

Email Security

Block ransomware, prevent data loss and stop impersonation. Mimecast email security is the most advanced email security on the market, and plugs the gaps left by Microsoft 365.

Cyber Security

With anti-virus scanning, intrusion prevention, and synchronised security, Sophos solutions like Intercept-X use advanced AI and Machine Learning to identify and stop threats before they even reach you.

Are you in doubt about where you need to start to protect your IT infrastructure, data and your business?

You can get your free IT Health Check with Arc Systems, or get in touch if you'd simply like to speak to a local IT specialist about IT solutions that could help you be more productive and safe.

You can reach our friendly experts at 01268 288100
or email us at info@arcsystems.co.uk

arcsystems