Eight Steps to Maximise Microsoft 365 Security

Practical advice that will help you shield your business from ransomware attacks

Did you know your Microsoft 365 licences can be leveraged to protect your business from ransomware attacks?

Microsoft 365 has been keeping retailers running in 2020, giving people the tools they need to deliver essential customer services whilst working remotely. But this increased reliance on Microsoft 365 has meant that hackers are targeting it more than ever before to launch ransomware attacks. And as recent high-profile attacks have shown, the damage they can cause to businesses and their customers is significant.

Here's how and what you need to do to protect your staff and customers.

How Hackers Launch Ransomware Attacks

Hackers use a number of methods to launch ransomware attacks against businesses. Here are three of the most common:

Phishing Emails. Hackers send phishing emails that contain links to ransomware payloads.

User credential Leaks. Hackers login to users' accounts and launch ransomware attacks using Microsoft 365 credentials leaked on the Dark Web.

IT estate complexity. Hackers exploit cyber security gaps created by public cloud and SaaS architectures to launch ransomware attacks.

Eight Steps to Maximise Microsoft 365 Security

Your Microsoft 365 licence includes feature-rich, fully-integrated security tools which, when configured properly, can protect your business from ransomware attacks by preventing hackers from targeting you through the methods we listed above.

Here are eight steps your organisation can follow that will help you shield you and your customers from ransomware attacks.

Deploy multi-factor authentication.

1

When your users access systems remotely, make sure they authenticate each login through the Microsoft Authenticator multi-factor authentication app. Multi-factor authentication is one of the main ways your business can ensure the people who access your systems really are who they say they are.

Configure policy-based access to applications.

2

Configure your users' profiles so that they only have access to the tools they need, when they need them. If a user profile is compromised by a hacker, policy-based access to applications will stop them accessing your entire network, limiting the potential damage they can cause if they launch an attack.

Enable document scanning.

3

Ransomware attacks are often launched through phishing emails that include attachments containing malicious malware payloads. Microsoft 365 has the ability to test attachments within a sandbox environment before allowing your users to download them. You'll need to enable this, though – it's not enabled by default.

Use document tagging.

4

Document tagging allows you to apply policies to outbound documents, such as read only, read only for seven days, no printing, no copy and paste and so on. This minimises the risk of your retail business leaking personally identifiable information (PII) for which you may be held liable. You can also enable document encryption on documents going out and at rest.

Use web link scanning and protection.

5

Phishing emails don't just contain dodgy attachments – they can also contain links to malicious websites that can lead to ransomware infection. Microsoft 365 can test links in emails to ensure they're not compromised before your users can click on them. You should combine this with user training so your people are smart about the links they visit.

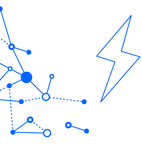
Leverage Microsoft Cloud App Security.

6

Microsoft Cloud App Security lets you know where are people going and what they are accessing. You can use this information to build policies on what they should be able to access. This can help prevent data loss, as you control how your users are able to access and share sensitive documents – for example, by preventing them from accessing online services like DropBox and WeTransfer.

Create surface reduction rules.

7



You can configure Microsoft 365 to minimise the surface through which hackers can attack you. For example, you can stop users from accessing the network until they're patched and up-to-date, preventing unpatched and potentially unsafe machines causing a security event. You should also look to minimise device attack surfaces by turning off unnecessary functions, making sure things like USB devices are managed, and stopping scripts running when documents open.

Monitor everything 24x7.

8

Hackers don't just work nine-to-five – they deliberately launch attacks at inconvenient times in order to cause maximum damage. Use a tool like Microsoft Defender for Endpoint to monitor your systems 24x7, but don't forget you'll need human intervention in order to stop ransomware attacks in their tracks. This is where services like **Managed Detection and Response** from Six Degrees can really elevate your cyber security posture.

Ready to get started? If you'd like to work with our experts to maximise your Microsoft 365 security and shield your retail business from ransomware attacks, we're ready to support you.

Book in a consultation

www.6dg.co.uk
info@6dg.co.uk
0800 012 8060