Top 4 Office 365 Security Concerns and Best Practices

140,000

Business in UK using Microsoft Office 365

61%

The majority of companies using Office 365 are small Businesses

If a cybercriminal breaks into your 365 account, they can expose your business' sensitive data and take on your email identity to send out malicious emails to both your company and clients.

1 Account Breaches

GET MULTI-FACTOR AUTHENTICATION

MFA should be set up for all user accounts, especially admin. Hackers normally go for these accounts because of their high-level access privileges.

USE A STRONG PASSWORD

Support your MFA with a long non-guessable password. Avoid using the same password everywhere - use a password manager to help keep track.

EDUCATE YOUR EMPLOYEES

Human error is still the main cause of cyber attack. Invest in cyber training for employees and keep employees informed of company security policies.

2 Access Privileges

A common mistake businesses make in Office 365 is being very unrestrictive with access privileges. The more people that can access sensitive data, the more at risk it is of being breached.

MICROSOFT RECOMMENDS 2-4 ADMIN ACCOUNTS

WHEN AN EMPLOYEE LEAVES YOUR ORGANISATION, REMOVE THEIR ACCESS AND DELETE THEIR OFFICE 365 ACCOUNT.

It's the big one. Concerns about data security is a big reason for business' hesitancy to adopt cloud solutions. Poorly secured data is an open door to data breaches.

3 Data Loss & Leakage

USER ERROR

Humans can cause problems simply because of accidental errors like deleting or overwriting files.

CYBER ATTACK

If hackers get hold of your data they may encrypt it with malware or sell it on the Dark Web. Cyber attacks can affect business reputation, disrupt operations, and even have legal and financial repercussions.

BACKUP, BACKUP, BACKUP!

Regularly backup data, either with another cloud provider or locally on an external hard drive or disk. Be sure to monitor these backups and test recovery time!

DATA CLASSIFICATION

Understand the different kinds of data you hold as a company and assign correct labels and access privileges. Managing your data well will help prevent it from falling into the wrong hands.

USE DATA LOSS PREVENTION TOOLS

Office 365 E5 customers can access Microsoft DLP to help monitor and protect your important data. DLP applies rules to classify your data and if they are violated, you'll get alerted.

4 Email Security

With the popularity of Office 365, hackers are getting more sophisticated in attacking these users with phishing emails, spam and ransomware. Initial access will then allow them to scale up the cyber breach from the inside.

REMEMBER TO CHECK...

THE EMAIL DOMAIN

Emails should be from a company email address. Read it carefully in case scammers have spelt the name differently.

MISSPELLINGS

you can spot a scammer by poor spelling and grammar in the content of the email.

LINKS

Make sure the URL looks legitimate and in line with the company website URL. Links and attachments are how scammers like to infect your systems with ransomware.

CONTENT

Are they asking for personal details or bank details? Trying to make things seem really urgent? Scammers will try to make you act rather than think.

91%

91% of cyber attacks start with a phishing email.

Hackers may take control of your email and target colleagues, bosses, suppliers and customers, generally with financial gain in mind.

OFFICE 365 BEST PRACTICES

- Set up multi-factor authentication.
- Train your users.
- Use dedicated admin accounts.
- Raise the level of protection against malware in mail.
- Stop auto-forwarding for email.
- Use Office Message Encryption.

Head to Microsoft 365 Security and Compliance Center for more information.