

**10
STEPS**

**to Avoid
Breaches &
Data Leaks in**



Microsoft 365





If you use Microsoft 365, then you will know how important and central a role it plays. It stores not just your sensitive data but email, chat and its sharing features are the central nervous system of your business interactions.

Microsoft 365 has hundreds of thousands of different settings you can switch on and off, and some of them can have a real impact on the security of your company's data.

Therefore, to avoid costly business impacts such as:

- > Account Breach
- > Data Loss
- > Reputation Damage
- > Leak of Intellectual Property
- > GDPR
- > Supplier Payment Fraud
- > Fines (and other legal consequences)

It is vitally important that you secure the information held inside it.

Effectively securing your business can be difficult, time-consuming and costly. There are, however, some straightforward steps that you can take to significantly reduce your risk with minimal effort.

While we don't advocate doing just these things, you should think of them as the first quick wins on your security journey.



Tip 1

Adopt Good Password Practices

Most account breaches occur because passwords are weak or are accidentally typed into somewhere they shouldn't. However, an insecure password is far more subtle than just its complexity. Passwords must be allocated and used appropriately, or the most complex password in the world won't do much good to keep you secure.



Create a company password hygiene policy. It might look something like this:

1. Passwords should consist of letters, numbers, symbols, and be longer than 8 characters. If you are not using a password manager (see next section) then you should adopt passphrases (memorisable sequences of words).
2. Do not base passwords on words/names/addresses which are personal or unique to the user or the company. For example, if your company sells woollen garments, then don't use w00lyjumper123. There are automated toolsets (used by attackers) that have functions built in to do the substitution to dictionary words and then adding common suffixes like 01; 123; !; etc.
3. Create a unique password for every service. Password reuse is one of the most common sources of account compromise.
4. Do not write it down either on paper or insecure digital form. Ever!

The above stipulations create healthy password hygiene; however, **they also create a new problem**. Users could not possibly remember all their unique complex passwords. Don't panic, the solution is straightforward ... read on!



Tip 2

Take Control with a Password Manager

Online password managers such as Bitwarden, 1Password and Dashlane (to name only a few) make it possible to achieve the level of security discussed above. Moreover, they take away the headaches of remembering and retrieving these complex passwords. They add much more on top too, such as support for mobile devices, one-click auto-filling on web pages, linking your business and personal accounts, sharing credentials, the list goes on. Furthermore, they support complex password generation and filling.

“I have no idea how I survived without a password manager before now” – Clare, Operations Director, Stratum Now

You and your employees can simply and quickly generate a new password for each cloud service. The password manager automatically creates a new entry and stores the password securely, giving you permission to instantly forget it. They are worth it alone for the time they save on each login.

Many of these services are free; however, if your business sees fit to pay for a centrally managed business subscription (which is recommended) for your staff then your company has the added advantage of being able to remove all access once the employee leaves your organisation. Business-grade password managers give your team the ability to log in with those passwords, but not to see them, meaning they stay safe and sound.



Tip 3

Use Multi-Factor Authentication (MFA)

User Name	Password	Text Msg Code	App on Your Phone
Authorisation	Authentication (Factor 1)	Authentication (Factor 2)	Authentication (Factor 3)

Multi-factor authentication (MFA or 2FA for Two-Factor Authentication) reduces the likelihood of being breached by orders of magnitude.

For those that don't know, it uses a second factor (e.g. your mobile phone) as a second security check. The hacker would need your password AND your mobile device to log in to a service.

Rolling out MFA to your employees can be a little painful. Not everyone is going to follow the MFA enrolment procedure, and new users will not have MFA enabled by default. Or, it will stop them from logging in, and then you have an unproductive employee.

If you are hesitant about MFA then at least enable it for all your privileged administrator accounts on your tenant. These accounts are very sensitive as they are likely to be able to access large volumes of data, multiple systems and enact potentially damaging configuration changes. These accounts are the ones the attackers go after.



Tip 4

Separate the Privileges from the Person

You may think when you set up new user mailboxes, for administrative employees, that their mailbox users also should have admin rights.

No! They should not, no matter their role. Ever!

Instead create a separate, non-licensed user (remember an unlicensed user on Microsoft 365 won't cost you anything) for each individual requiring admin rights. Give each a similar name to the mailbox in question. For example, `susan-admin@megacorp.com` (assuming their name is Susan) and grant the `susan-admin` account any access required to perform her duty.

The thinking is simple. Regular accounts have internet and email and privileged accounts are disconnected from these things. If the mailbox gets phished or otherwise compromised, it's only a regular account, and so the phisher will only get the regular credentials and access. That way you limit damage to regular user access, not keys-to-the-kingdom stuff. The bottom line is to limit the exposure of Admin Credentials.

In the same vein, go through the company accounts and ask yourself for each admin, is this admin required? If they are, create a separate admin account, remove admin rights from the regular account, or delete it.



Tip 5

Don't Share Admin Accounts

Creating personalised admin user accounts as above should be the only types of admins that you create. No admin accounts should be shared. In other words, each person that requires administrative access should only use a separate and unique admin account. There should be no account called "admin@YourCompany.com" or similar. The reason for this is accountability. If someone in your company, acting in their capacity as an administrator, makes a change you will know who made that change.

Tip 6

Don't Share User Mailboxes

Don't create user accounts for shared functions. Time and again, we see companies creating a real mailbox called "Accounts", "Reception" or "IT support" and then allowing multiple employees access them directly using a single set of credentials. This is very common, but a very bad idea! When something goes wrong, the account gets breached, or you need to track who has access, you will be blind and left putting all employees with access under suspicion. Moreover, staff turnover creates either a risk or the overhead of changing the password.

Instead, use shared mailboxes. These are not user mailboxes and do not have login credentials. In addition, they do not incur a licence cost.

Shared mailboxes allow prescribed users delegated access to log in and send or read mail based on their needs. This way, you can add, remove, and more importantly, audit who accessed sent and read emails. Finally controlling access is easy when employees move departments, or leave the business. No need to re-set the password because there was never a password in the first place.



Tip 7 **Don't use email to transfer files.**

A “no attachments” policy can seem like a strange thing to suggest given the prevalence of file attachment in modern business. How can I send those spreadsheets to those accountants? The issue is that if your mailbox is compromised, all historical data is available, including any attachments ever sent or received.

The solution is to send a link that you control. Microsoft SharePoint and OneDrive supply a straightforward way to share a file through a link.

These links can be made to expire automatically. If you had used expiring links and a mailbox is compromised, all that's available to the hacker is a bunch of expired URLs. Furthermore, links can be made read-only and non-downloadable. Controlling what the recipient can do in this way mitigates the risk that they could misuse the contents, accidentally or otherwise. Lastly, what is currently a good relationship with a recipient might change in the future. In such a case, links can also be manually revoked.

Using links has other great uses beyond the security realm, such as seamless and managed collaboration and versioning.



Tip 8

Configure OneDrive, Teams and SharePoint Link Policies

Are you already using OneDrive for sharing files instead of sending attachments? Great! But what about if that person forwards the link on to someone else? Or they leave the company and take your link with them? Oops!

Using sharing policies, you can control the default link-sharing options given to users. You can also control what types are not allowed (such as anonymous links).

It is a good idea to do this in conjunction with a company policy that nothing sensitive should be sent by email, as described above, so that you guide users to share in the desired fashion.

You can do this in SharePoint Admin Centre. The options are:

1. No external sharing
 2. Existing guests
 3. New and existing guests
 4. Anonymous sharing
- **MOST SAFE**
- **LEAST SAFE**

In addition to the above you can set how long it will take for links to expire. Whilst we cannot say which is the right default choice for you, we would highly recommend (as does Microsoft) not allowing anonymous sharing if links are set to never expire. We also suggest not overly restricting users concerning the types they can use. Otherwise, you may find users returning to using attachments instead of links.

(Please note, SharePoint underpins OneDrive so any sharing choice restricted in SharePoint will also be limited in OneDrive, but not the other way around.)



Tip 9

Configure Calendar Sharing Policies

You may not think of it but when we share our calendar's we may be letting outsiders know sensitive information about all our meetings. This may include sensitive meeting names and not to mention our whereabouts at certain times. The latter is particularly pertinent with the increase in remote working. Furthermore, there has been a dramatic increase in video conferencing use with the move to remote working. Video conferencing is notoriously insecure in its use of links and IDs that allow anyone to join.

In the case of the former, imagine your CFO calling a meeting with the CEO entitled "strategy for lay-offs". Given the wrong sharing settings, this name can then be seen by others who need to check the times the CFO is available to talk about their pension plan. Calendar sharing policies can be created in the Exchange Online Admin Centre. We suggest a policy to share ONLY "Free/Busy information with time only".

Limiting the visibility that can be shared outside of the organisation can also avoid a harmless calendar share today resulting in sensitive information being divulged tomorrow.



Tip 10

Create Suspicion of Unsolicited Links

One of the easiest and most popular ways for attackers to gain control of an account is with phishing emails. Phishing emails may contain links which request the user to log in to their account to do some critical action or read some enticing content. Social engineering tricks make the reason to sign in sound urgent, and imperative. The links in these attacks lead to genuine looking, but entirely fraudulent, pages where the attackers steal the user's credentials.

It can be challenging to recognise these emails since attackers may use source email addresses and content that look entirely convincing. A practical solution is to use a simple rule of thumb when considering clicking a link.

“Did I ask for this request for action? Or is this request unexpected?”

To use an example: I request my bank to update my mortgage details.

I then receive an email from them, with a link to log in and complete a mortgage details update. I have asked for this interaction, so the email from them is likely to be legitimate. However, imagine I unexpectedly get an email claiming to be from my bank, for something I have not asked.

If this email asks me to do something, then at once treat it as suspicious because I did not ask for the interaction.

User awareness training can also be invaluable in showing simple techniques to spot malicious or fraudulent phishing emails.



NEXT STEPS

The above set of steps contain many simple yet effective rules and configurations for your organisation and employees to follow. However, security is a continuous journey, and you should not stop there.

Here are some next steps that we would recommend.

1. Form a Safety-First Culture

Security is responsibility of every employee, but they must have sufficient understanding of the risks and behaviours. The above steps can form a coherent guide for your employees to protect your organisation. Add these rules to your IT security policies.

Why not give this document to your employees? It is a quick read!

Understanding the risks and protections can lead to a maintainable safety-first culture.



2. Turn Off Unrequired (and unsafe) Remote Access Methods

Most of us access our Office 365 data through a few modern methods such as Outlook, Teams and often on our mobile devices. However, unless explicitly changed, your tenant will expose a wide range of access methods that Microsoft allows. Some of these are based on legacy and unsafe protocols such as legacy email communications that send credentials with every request. We have created a blog article on this subject which explains each type, why you might need them, and how they can be configured on an organisational level or on a per user basis, based on their individual business needs.



3. Turn on the Audit Log

While these steps are necessary and will reduce your risks, the sad fact is that most companies (61% in the UK in 2019) experience security breaches. We must be ready to investigate and remediate when a breach occurs. You will need an audit trail regardless of whether you try to investigate it yourself or hire an outside entity.



Microsoft Universal Audit Log provides this, however, it is not turned on by default. We recommend you turn this on right away. It can be done by logging into the Security and Compliance Centre Portal as an administrator and flicking a switch.



Simplify Your Office 365 Security

At Stratum Now we recognise the need for comprehensive security of company data – that's why we've built our products and services around keeping our customers safe and secure.

We appreciate the considerable amount of time it takes to properly secure your company's digital assets: we use policies, procedures and automation to ensure that not only are our customers' information stores secured properly, but they stay that way.

Understanding the complexities of Microsoft 365 is to understand that there's a whole digital world behind the Microsoft 365 admin portal, and one false step can accidentally expose your intellectual property to the world.

If you'd like to talk to us about anything in this guide, or get some help on securing your company's digital assets, please give us a call and we will be pleased to help.





STRATUM NOW

IT solutions • Cyber Protection • Cyber Essentials
Digital Security • Antivirus & Endpoint Protection
Breach Detection • Cloud Migration

Cumbria Businesses,
Claim your bonus FREE tech support package!

Go to register.stratumnow.com for more information



01946 277 000



hey@stratumnow.com



The Bus Station, Bransty Row, Whitehaven, CA28 7XE