The 7 Best Ways to Secure Microsoft 365

Ntiva

Your Success. Secured.

Microsoft 365 is an indispensable platform for many businesses, and is considered the world's most popular office productivity suite. However, this means it's popular with hackers as well!

Most people don't realize that Microsoft 365 comes equipped with many built-in security features that can mitigate risk.

The trick is you have to turn them on!

Learning how to properly configure and deploy these features, coupled with employee training, is the best way to help protect your sensitive business data.

Below you'll find our top 7 ways to secure your Microsoft 365 platform, but keep in mind there is no single solution out there that can completely protect your business.

A layered security approach is the only way to lower your risk, so be sure to consult with a certified Microsoft 365 consultant to get the best advice.

But let's get you started on learning the most important security features that you can take advantage of today on your Microsoft 365 platform!

1. Set up Multi Factor Authentication (MFA)

Typically employees only have one way to verify their identity when logging into Microsoft 365 — their user name and password.

Unfortunately, you can't expect all your employees to be diligent about safeguarding their passwords at all times.

Using Multi Factor Authentication, or MFA, is one of the easiest and most effective ways to increase the security of your organization.

MFA combines two or more factors — e.g., a password, a code, a fingerprint or even a retinal scan — to verify a person's identity and protect against "soft breaches." That means even if a criminal is able to get your password, they can't access your account without the other verification method(s).

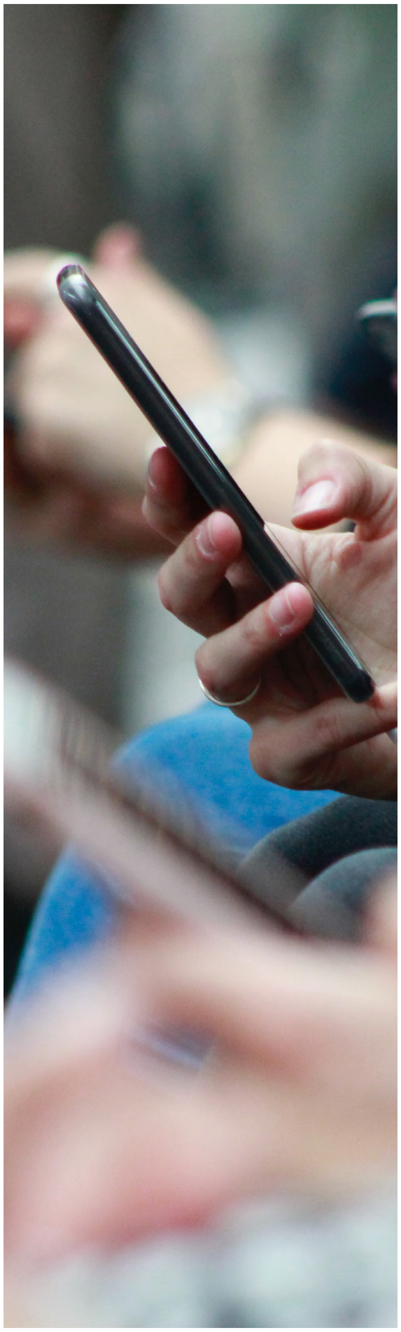
The most common method is a text message that is sent to the user's smartphone every time they try to log in to an on-line application. This is becoming very popular not only with business apps, but consumer apps as well.

For most companies, the built-in MFA option in Microsoft 365 can provide the necessary protection.

It allows you to activate MFA at the user level, which offers several different options for the second verification method.

But don't forget to protect your other business applications as well, such as Salesforce, G-Suite, Dropbox and all the other line-of-business apps you use every day!

There are many MFA solutions on the market, including Duo and others that are great solutions to protect your apps beyond Microsoft 365.



2. Carefully Manage Your Administrative Privileges

Admin accounts are valuable targets for hackers and cyber criminals, as they include elevated privileges.

When the accounts of users with admin privileges are breached, the consequence is often more serious.

Be sure that your Microsoft 365 admins have a separate user account for every day non-administrative use and only use their admin account when necessary.

Additionally, restricting the number of users with admin access can help lower your risks.

However, there are times when certain employees need limited-time admin access for certain tasks.

Azure AD Privileged Identity Management allows you to lower exposure and minimize risks by giving you the ability to assign temporary admin status to specific users.

You can control access based on the information each user needs and the length of time they require admin privileges.

This is a great way to limit your exposure!

3. Take Advantage of Data Encryption

To ensure the security of sensitive information either at rest or during transit, you need to implement an encryption protocol that ensures confidential storage and communication.

This is particularly important if your company handles information such as credit card information, social security numbers, or health records - and you need to meet regulatory requirements which are starting to apply to almost every industry.

Microsoft 365 offers several encryption capabilities by default: BitLocker for files saved on a Windows computer and TLS connections for files on OneDrive for Business or SharePoint Online.

Another cool feature is the ability to send encrypted email messages to recipients outside of the organization, letting them access the messages by signing in with a Microsoft account, using an Microsoft 365 account, or entering a one-time passcode.

4. Deploy Mobile Device Management (MDM)

Whether you have a “Bring Your Own Device” (BYOD) policy or not, your employees are likely to be accessing company data with their phones, tablets or laptops, especially now that we are all working from home.

Even though you can provide the necessary education to employees, you still need to guard against scenarios such as lost devices or someone other than the employee gaining access to the devices.

Microsoft 365 offers a built-in MDM option, which works well for employees accessing email via their company-issued mobile devices.

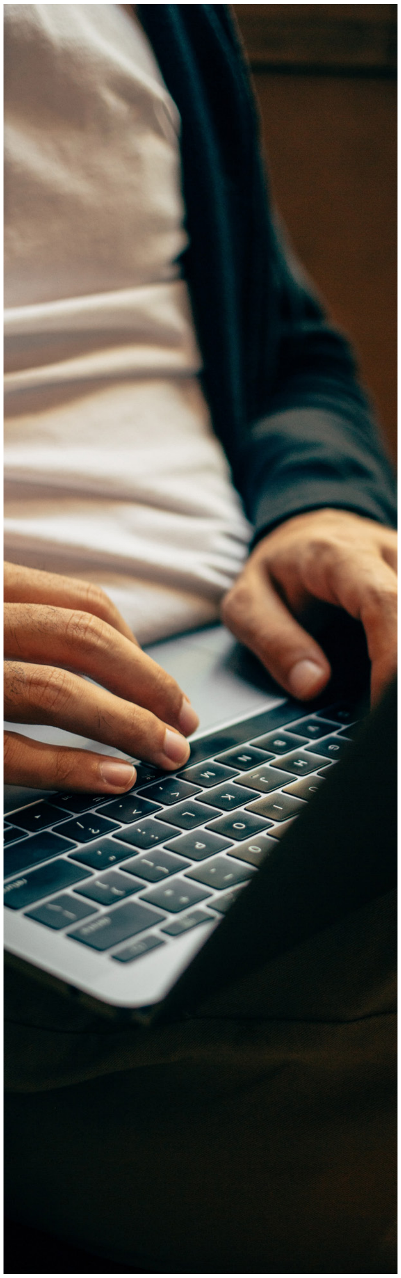
If employees are using their own devices or using applications besides email, Microsoft Intune will give you more control and offer additional protection.

Again, consult with your IT security expert to find out which MDM solution is best for your company.

5. Create a Data Loss Prevention (DLP) Policy

In order to comply with business standards and industry regulations, many organizations will need to create and maintain a DLP policy.

A DLP policy will ensure that sensitive information stays within your organization by monitoring confidential data and preventing users from sending the data to anyone outside of your company.



You can either use one of Microsoft's existing templates that meet regulatory and compliance needs (e.g. HIPAA) — or customize your own policy to specify the location of data and type of information to be protected.

With an Microsoft 365 DLP policy, you can:

- Identify any document containing sensitive information, such as a credit card number, across many locations including Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams.
- Prevent the accidental sharing of sensitive information over email by automatically blocking the email being sent.
- Monitor and protect sensitive files in the desktop versions of Excel, Powerpoint and Word.
- Educate your employees how to stay compliant and how DLP can help them remain compliant by sending them notifications and policy tips.

All in all, DLP is a pretty powerful way to protect sensitive information from being accidentally leaked into the wrong hands!

6. Turn On Advanced Threat Protection (ATP)

One of the biggest cyber security threats comes from phishing emails, which typically spreads ransomware via malicious links and email attachments.

Although you can and should offer employees phishing prevention training so they don't click on suspicious links or attachments, you can't rely on everyone being vigilant at all times.

It takes only one employee to click on one malicious link to cause irreparable damage to your sensitive data—and your reputation.

Advanced Threat Protection helps prevent these links and attachments from getting into your employee's inboxes in the first place.

It does this by opening them in a virtual environment to check for malicious activity before delivering the emails to the recipients.

Remember, although ATP along with the rest of the Microsoft 365 security features above can drastically reduce your chances of being compromised, there is still one very important function that you simply can't ignore.

7. Train Your Employees

Establishing a strong culture of security awareness is a critical part of layered protection.

Teaching employees how to maintain passwords, recognize phishing emails, understand security features on their mobiles and laptops, and most importantly, understand and sign off on company security policies is an absolute must.

Security training is not one-and-done, it's an ongoing requirement.

Whether you do this in-house or outsource it, appropriately trained resources should be tasked with developing, maintaining and updating your security policies and programs - which should include regular employee training.

READY TO UP YOUR MICROSOFT 365 SECURITY?

Get the Most Out of Your Microsoft Investment

TALK WITH AN EXPERT

Ntiva

Your Success. Secured.