SpinOne

Office 365 Security: a Checklist for Admins

✓ Office 365 security concerns and best practices to keep Office 365 data safe.

Over six million data records get lost or stolen every single day. The Cost of a Data Breach Study concluded that businesses pay $148 per one lost or stolen data record. Usually, the cost of lost or stolen data items reaches hundreds or even thousands of dollars per company. You can do the math.
How secure is Office 365 in terms of data breaches and data losses? Not as secure as you think it is. Its security depends on whether a business owner can foresee the potential risks and knows how to prevent them.

SpinOne

Contents

1.

Set up a reliable password policy

SaaS Data Protection Guide

One of the main O365 security concerns is password carelessness. According to the Verizon Data Breach Investigations Report, more than 70% of workers reuse passwords. And most of them have passwords a hacker with a mediocre password cracking machine would crack in a few minutes.

It's widespread for people to use the same password for multiple websites. They may also make them too simple so they could remember them easily. This approach puts your data at huge risk.

Imagine for a moment that your employee uses one password to access their profile on Instagram and to sign in to their Office 365 corporate account. What will happen, if someone cracks their password from Instagram? This someone will try this password to enter other systems as well, including your Office 365. At this very moment, your company data gets endangered.

How to make passwords secure:

- The password uniqueness. Your employees' password to your company's Office 365 must be unique;
- The password length. It should include eight characters at least;
- The variety of characters. The password should consist of uppercase and lowercase letters plus digits.
- The semantic complexity. You should never use widespread passwords like "asdqwe123", "abcdefg," "123456", "password," "1111111". Even with adding some digits or letters, these passwords are still as easy as pie for cracking mechanisms.
- The expiration date. The passwords should be changed at least once a year.
- Data backup. Your employee's password to Office 365 might get cracked, but all your data will still be safe, sound, and easily recoverable.

2.

Use Up-to-Date Software

SaaS Data Protection Guide

By “software” we mean using old versions of Office like Office 2007 / 2010 / 2013 and not checking for the system updates and patches in Office 365. If you are guilty of it too, be ready for some security repercussions.

All software has it’s “expiration date.” At some point, Microsoft stops releasing updates for a given product version, and it gets abandoned. Without regular security updates, the software is unable to resist malicious programs that become more and more sophisticated. Some types of ransomware can even spread across computer networks.

In the cloud, you can get the whole system infected with ransomware or a virus. So make sure you don’t leave room for security loopholes.

How to secure your data from malware:

- One of the best practices for Office 365 security monitoring is to get the latest security updates.
- Backup your data with professional backup services. Only those can guarantee you can recover your information quickly and easily.

3.

Secure information privacy

SaaS Data Protection Guide

Employees share links to documents all the time. Sometimes (intentionally or not) these links could be shared with outsiders who will gladly use the information in it for their benefit. If people outside your organization gain access to the links, they are able to watch, save, and edit internal company documents.

Your internal company information is the most valuable asset, and there are many ways outsiders can benefit from it:

- Infect the document with ransomware or malware to ask for a ransom or just do harm;
- Profit from the data itself: sell the list of customers and suppliers, use sensitive information to steal money, exploit the ideas, and so on.

How to secure your data from malware:

To avoid data breaches, you can limit or forbid the external linking to some or all documents. To do so, go to Admin > Service Settings > sites and document sharing. Choose to Turn off external sharing.

4.

Enabled Multi-Factor Authentication

SaaS Data Protection Guide

Until recently, multi-factor authentication (MFA) was considered as an additional layer of security. Now, it is basic for most companies. With MFA enabled, when a user signs in, they have to enter their login and password and type a code that has been sent on their phone number, or answer a phone call. This way, a system ensures only veritable users can get access to the account. By using only username/password credential authentication, you put your data in danger.

How to enable Multi-Factor Authentication:

MFA function is available in Office 365. Just go to the Admin Center, select users and groups, and press Set Up near the Multi-factor Authentication. You can choose particular users or include everyone.

5.

Block Sensitive Information from Being Shared

SaaS Data Protection Guide

Some information should not be shared under any circumstances. It is sensitive information like credit card numbers and personally identifiable information. If this information is leaked, you can face huge legal implications and fees.

How to block sensitive information from being shared:

Define the parameters by which the system can recognize sensitive information. This way the system won’t let this data out or save it to SharePoint/ One Drive. Using Microsoft Office 365 security settings, you can trace and block this type of information from being shared.

6.

Provide a Security Training for Employees

One of the leading Microsoft Office 365 security issues is not cyberattacks – it's human error. Human mistakes let cybercriminals in the system, and this is what makes these mistakes so dangerous.

Security education for employees is like preventive medicine: it works, but often delayed as a secondary concern. Businesses don't care about potential risks until they become urgent problems with tremendous potential losses.

At the same time, human error is on the top of cybersecurity concerns. People's carelessness and ignorance in security matters cause notorious losses for businesses. People are usually the ones who let the cybercriminals and hackers in the system in the first place.

Here are just a few human mistakes that will harm your organization:

- Sharing sensitive and secret company information with third-parties
- Clicking on infected links and attachments
- Accidentally deleting important information
- Being easily tricked by social engineering tactics.

How to educate your employees:

Provide your new-coming employees with security awareness training. You have two options: to instruct your security department to prepare it, or just buy one. And of course, take care of your information security with SpinOne. In most cases, having a backup is what makes all the difference!

Try SpinOne Free →

SpinOne

ABOUT SPINONE

SpinOne is a multi-tenant platform created by Spin Technology and designed to simplify the complexity of cloud data security. As an all-in-one platform, SpinOne combines three solutions that make business data bulletproof from the security breach and insider threats: SpinSecurity, SpinAudit, and SpinBackup.

SpinOne is trusted by over 1,500 organizations worldwide including HubSpot, Vopak, IBT Industrial Solutions. We have more than 1,200,000 business users in more than 100 countries.

Try SpinOne Free →

Spin Technology Inc

2100 Geng Rd Suite 210

Palo Alto, CA 94303, USA

USA and Canada Toll Free:

+1-888-883-2993
(9am to 5pm PST)

EU, CIS and Asia:

+48-22-602-2440
(7am to 4pm GMT)