OFFICE PROTECT

Office 365 Security Best Practices

The only way your organization can effectively mitigate the risks of cyber threats is to be proactive in preventing them. The first place to start? Your Office 365 security settings.

Your first line of defense for increased security is to make sure you set up the features you need. If you want full protection without investing a lot of time, effort and money, find an easy solution that integrates into your Office 365, such as Office Protect. This security tool will make it easy for you to set the following features with just one click.

7 important settings that will increase Office 365 security

1. Audit Log Search

Record user and admin activities. If a security breach happens, you'll have useful information to help you investigate.

2. Email Audit

In the event of a security breach, you can refer to your email audits to figure out what happened.

3. Multi-factor Authorization

Multi-factor authentication validates a user's identity in order to grant access. When activated, users will have to provide a second verification (SMS) to log into their Office 365 accounts.

4. Outbound Spam Notifications

Enable Exchange Online to send you an alert if a user within your organization is flagged for sending out spam. An internal account that is flagged for spam can be a sign of compromised credentials and a breach.

5. Block 'Bad' Files Extensions

There's really no use for sending a .bat file. You'll want to block these types of leery files from ever making it to your inbox.

6. Set Your Password to Never Expire

According to NIST (National Institute of Standard and Technology), passwords that expire regularly only hinder your efforts to prevent breaches. The only time you should change a password is when a breach happens or a potential one appears. Once you change the password policy for your users, they won't be asked to change their password on a regular basis.

7. Unified Event Report

When this feature is enabled, Microsoft will send you reports on a regular basis. It's a good idea to consult these reports to help you identify security issues.