

5 Ways to Protect Microsoft 365 from Phishing Attacks

Protecting your clients from phishing attacks can be a daily challenge. As phishing attacks increase, they're getting smarter and harder to catch. Microsoft 365 clients are especially vulnerable to these attacks as Microsoft is one of the most spoofed domains and platforms. Here are 5 ways Mailprotector partner **Luke Popejoy of Integrity Computers** protects his M365 customers from phishing attacks:

1. Turn on Azure Security Defaults

Security Defaults are simple to implement and come equipped with pre-configured settings. With a swipe on the Security Defaults toggle, you can protect your organization's account from preventable compromises.

2. Turn on Modern Multi-Factor Authentication

99% of attacks are targeted at end-users. This can be prevented by using MFA. Modern MFA is a Security Default in all subscriptions purchased after 2017. You may have to turn on Modern Authentication in your older subscriptions in order to get this feature.

Tip: *It's a good idea to turn off legacy per-user MFA.*

3. Implement SPF/DKIM/DMARC Protections

These protections, also known as email validation, are a group of standards that works to stop email spoofing:

SPF: *Helps to validate outbound emails sent from your custom domain.*

DKIM: *Used in addition to SPF and DMARC, helps prevent spoofers from sending emails that look like they're being sent from your domain.*

DMARC: *Works with SPF and DKIM to authenticate senders and ensure destination email systems trust the messages sent from your domain.*

4. Layer with Third-party Filtering for Bulletproof Security


Adding dedicated email security (like [CloudFilter](#) from Mailprotector) in front of Microsoft 365 can ensure your client's emails are legitimate and minimize phishing, while also beefing up your spam and virus defenses.

5. Encrypt Sensitive Outbound Emails


Be sure to encrypt your outbound mail with a user-friendly, yet highly secure option, like [Bracket](#) from Mailprotector. Bracket uses multi-layer AES-256 with automatic key rotation will ensure your data is safe.

PHISHING PHACTS


ON THE HOOK
91% of all phishing attacks start with a malicious email.



DEADLIEST CATCH
Only 9% of domains of companies in the Fortune 500 publish strong email authentication policies as of March 2018. The remaining 91% of these companies have a higher chance of receiving spoofed emails!



YOU'RE (NOT) CRACKING ME UP
AES-256 Encryption (like Bracket) encrypts messages and files with so many possible combinations, it would take over 20 years for a super computer to crack!



About Mailprotector

Mailprotector, makers of Bracket encryption, empowers MSPs with a full arsenal of [managed email security services](#) sold exclusively through the channel. We've been a trusted source for innovative and user-friendly email products and services since 2002.

