The Basics
Office 365 Configurations for Phishing Prevention

Introduction

Recently, Sedara has noticed an increase in Office 365 phishing incidents. In some incidents, the attacker logs into a compromised account and sends phishing emails to other organizational users. Office 365 is often a large and tempting attack surface, since it is ubiquitous and often Internet-facing. To help you enhance your security, we're creating a series exploring ways to prevent phishing attacks in Microsoft Office 365.

In this paper, we're exploring the most common ways administrators can configure Office 365 to block or alert on phishing attacks.

A note about MFA: Multi-factor authentication (MFA) is a best practice to prevent attackers from logging in to Office 365 accounts using compromised credentials. Ideally, MFA should be enabled for all users of Office 365; if that's not possible, MFA can be administered in phases or for the most critical users.

Microsoft Office 365 Protection Options

EOP is a cloud-hosted email filtering service built for spam and malware protection and to implement custom policy rules. It is included in any Microsoft 365 subscription that contains Exchange Online mailboxes or as a standalone product for on-premises email environments.

To configure anti-phishing policies in EOP, follow the directions in this link:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-anti-phishing-policies-eop?view=o365-worldwide

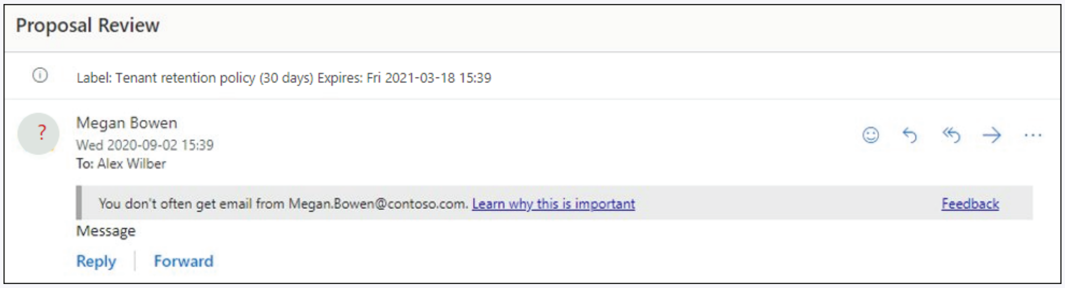
Additionally, EOP contains a section for spoof settings, which can be configured with these instructions:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#spoof-settings

Office 365 Anti-Phishing Configurations

First Contact Safety Tip

The "Show first contact safety tip" setting in EOP enables a message upon the first time a sender sends an email to a recipient within the organization, as shown below.

Since this setting doesn't prevent emails from coming through, it's best paired with a user education program; first contacts are a higher security risk and should be scrutinized carefully.



Proposal Review

ⓘ Label: Tenant retention policy (30 days) Expires: Fri 2021-03-18 15:39

Megan Bowen
Wed 2020-09-02 15:39
To: Alex Wilber

You don't often get email from Megan.Bowen@contoso.com. Learn why this is important Feedback

Message

Reply | Forward

SPF, DKIM, and DMARC

This trio of methods authenticate outbound email sent from your domain using records associated with DNS. Though this practice does not prevent inbound email phishing attempts, it provides reputation protection and is considered a best practice for email security.

SPF verifies an email sender's IP address against the owner of the sending domain, preventing spoofed emails that appear to come from your organization. To configure SPF, an administrator must make an SPF TXT record in external DNS for any custom domains or subdomains. To find out more, review the steps in this link:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-spf-in-office-365-to-help-prevent-spoofing?view=o365-worldwide

DomainKeys Identified Mail (DKIM) lets you add a digital signature to outbound email messages in the message header. To configure DKIM for your domain, use these instructions:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email?view=o365-worldwide

DMARC is automatically configured for inbound mail that your organization receives in Microsoft 365. If you have a custom domain or are using on-premises Exchange Servers along with Microsoft 365, you do need to set up DMAC for your outbound mail using these instructions:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide

Office 365 Anti-Phishing Configurations

Block by Location

In many cases, attackers log in to accounts from countries other than the US and Canada. Sedara has seen some success in blocking logins from countries that are unlikely to authenticate to the target.

To create a conditional access policy that blocks by location, see these instructions:
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location

For most US-based small organizations, it is appropriate to block all countries other than the US and Canada.

Though this would not prevent a determined attacker from moving their IP address, it can slow the attacker down enough to alert the security team on the account.

Detecting Phishing with LogRhythm

In addition to using native Office 365 security settings, phishing or stolen credential attacks can also be detected with SIEM platforms like LogRhythm. SIEMs have the benefit of providing additional context, like thresholds for activity across users or for the same user over time.

Detecting Unusual Logins

Although Office 365 has some alerts for unusual logins, LogRhythm can serve as an additional alert or it can track thresholds of behavior. Examples might include:

- Authentication Success from locations outside the US
- 10 or more logs with authentication failures, indicating a guessing or brute force attack
- Detected DLP, malware, or phishing activity (from Office 365 or other application logs)

Detecting Auto-Forwarding

In many cases, threat actors who have already compromised an account will set Office 365 to auto-forward emails to their own account in order to continue the compromise even after they are discovered. It's simple to discover this change by monitoring for a "Set-Mailbox" event where the value "DeliverToMailboxAndForward" is set to "True". Threat actors can also use inbox rules to automatically forward mail; this is detected with a "New-Inbox Rule" event.

For more information on using LogRhythm to prevent phishing, check out
https://explore.logrhythm.com/top-blogs/detecting-and-preventing-auto-forwarding-and-phishing-attacks-in-office-365

Limitations

Like all automated detection, anti-phishing measures can fail in the face of a customized or advanced persistent threat (APT) attack. Even if the above tips are followed, there are three cases in which it may be difficult or impossible to flag a phishing attack:

- The attack falls within what's configured to be "normal" by the organizational policy (for example, the login originates from the USA or Canada)
- The sender uses novel subject lines or content within their email
- The attacker is sending email from a legitimate, trusted internal or external email address

In these cases, it is helpful to have a well-documented incident response plan to limit the scope and time length of the attack.

Scan the code below for more info on this topic and to download a digital version of this document.

Or Visit:
sedarasecurity.com/office365