

Microsoft Office 365 Best Practices

With an increase in the number of cyber security compromises as a result of phishing attacks, it is prudent for companies using Office 365 products to take appropriate steps to prevent or mitigate the damage from these incidents.

Microsoft has several tools available that can help an enterprise manage its Office 365 environment. While many of the tools referenced below are freely available, some tools may require a subscription. Crypsis recommends enabling as many of these tools as needed.

<p>Enable multi-factor authentication (MFA)</p>	<p>In conjunction with a strong password policy (password complexity enabled, password rotation etc.) multi-factor authentication adds an extra layer of protection by requiring users to acknowledge an additional challenge to access their account. This lessens the likelihood of a compromise even if a password has been stolen and/or compromised.</p> <p>Details on MFA and an implementation guide are found here: https://support.office.com/en-us/article/set-up-multifactor-authentication-for-office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6</p>
<p>Enable the unified audit log and mailbox audit logging</p>	<p>The Office 365 unified audit log provides a centralized logging facility that includes activities from Azure Active Directory, Exchange Online, SharePoint Online, OneDrive for Business, and other applications. Note that the unified audit log is not currently enabled by default and needs to be manually enabled.</p> <p>Details on enabling the unified audit log and an implementation guide are found here: https://support.office.com/en-us/article/Search-the-audit-log-in-the-Office-365-Security-Compliance-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c</p> <p>Mailbox auditing generates additional logs that include mailbox activities performed by the owner, a delegated user, or an administrator. Note that mailbox auditing is not currently enabled by default and needs to be manually enabled.</p> <p>Details on the mailbox activities tracked by mailbox auditing are found here: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/mailbox-audit-logging</p> <p>Details on enabling mailbox auditing and an implementation guide are found here: https://go.microsoft.com/fwlink/p/?LinkID=626109</p>
<p>Configure and enable Data Loss Prevention (DLP)</p>	<p>Data Loss Prevention allows an administrator to identify and create policies to prevent users from accidentally or intentionally sharing sensitive information. DLP can be implemented across all Office 365 applications, SharePoint, and OneDrive.</p> <p>Details on enabling DLP and an implementation guide are found here: https://support.office.com/en-us/article/overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e</p>

<p>Enable Office 365 Cloud Application Security</p>	<p>Microsoft’s Cloud Application Security enables an administrator to investigate suspicious activities. Office 365 consists of multiple tools that enable an organization to track a number of suspicious activities from unauthorized users, track ransomware activity, and much more.</p> <p><i>Note: Office 365 Cloud Application Security is only available to Enterprises Licensees.</i></p> <p>Details on Office 365 Cloud Application can be found here: https://support.office.com/en-us/article/overview-of-office-365-cloud-app-security-81f0ee9a-9645-45ab-ba56-de9cbccab475?ui=en-US&rs=en-US&ad=US</p>
<p>Enable Secure Score</p>	<p>Microsoft’s Secure Score is a security analytics score that analyzes an Office 365 settings and activities and compares them to a baseline. A score is calculated which shows whether an organization is aligned with best security practices. Secure Score requires an Enterprise subscription and an administrator account.</p> <p>Details on obtaining, enabling Secure Score and an implementation guide are found here: https://support.office.com/en-us/article/introducing-the-office-365-secure-score-c9e7160f-2c34-4bd0-a548-5ddcc862eaef</p>

Cyber Criminals Can Target Business Email Accounts for Financial Gain



STEP ONE

Attacker sends fake login page to victim and steals credentials



STEP TWO

Attacker searches email for financial information and redirects requests for payment



STEP THREE

Attacker [acting as the compromised victim] alters payment instructions/pay to account details



STEP FOUR

Attacker receives funds

The Crypsis Group is a cyber security consulting firm. Our consultants are information security experts with a diverse set of information security skills and experience. We are security engineers, digital forensic experts, malware reversers, penetration testers, and data breach incident responders. We work with organizations to proactively identify and mitigate enterprise risk and to respond to sophisticated network intrusions. We have responded to and managed investigations of complex data breach incidents for global organizations, including attacks by nation-state actors, insiders, and cyber criminals looking to steal confidential, sensitive or proprietary data. In all of our engagements our findings and conclusions are measured against industry best practice, rooted in fact, and designed to withstand opposing party scrutiny.