paloalto NETWORKS | CRYPSIS A PALO ALTO NETWORKS COMPANY

INFO SHEET

Microsoft Office 365 Best Practices

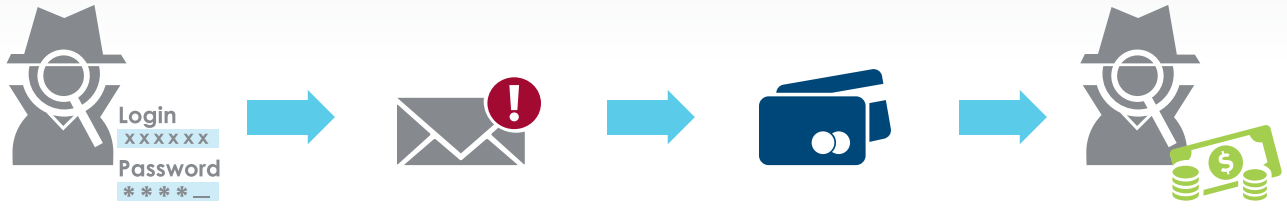
With an increase in the number of cyber security compromises as a result of phishing attacks, it is prudent for companies using Office 365 products to take appropriate steps to prevent or mitigate the damage from these incidents.

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.

Enable Multi-Factor Authentication (MFA) and Disable Legacy Authentication	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. **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 Legacy authentication protocols should be disabled in order to ensure that MFA cannot be easily circumvented by attackers. O365 environments using a premium level of Azure AD can accomplish this through conditional access policies, and non-premium environments can create an authentication policy through PowerShell that blocks all basic authentication.
Enable the Unified Audit Log and Mailbox Audit Logging	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. **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 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. **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 **Details on enabling mailbox auditing and an implementation guide are found here:** https://go.microsoft.com/fwlink/p/?LinkID=626109

Configure and Enable Data Loss Prevention (DLP)	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. **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
Enable Office 365 Cloud Application Security	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. *Note: Office 365 Cloud Application Security is only available to Enterprises Licensees.* **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
Enable Microsoft Secure Score	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. **Details on obtaining, enabling Microsoft Secure Store and an implementation guide are found here:** https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-wide-setup-for-increased-security

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

CONTACT US TO LEARN MORE ABOUT THE CRYPSIS GROUP

703.570.4103 | info@crypsisgroup.com

The Crypsis Group is a security advisory firm focused on supporting our clients as a trusted advisor before, during, and after a breach. The combination of our deep security knowledge, proprietary technology, and methodology allows us to rapidly identify, contain, and eradicate attacks for organizations. Our team's experience spans security monitoring within the intelligence community and advising at the national security level to performing high profile data breach investigations and leading remediation efforts.

© 2021 Palo Alto Networks, Inc.