ManageEngine
M365 Manager Plus

5 steps to remediate your compromised Microsoft 365 account

Introduction

Although Microsoft 365 adoption has helped organizations increase productivity, these platforms are chock-full of confidential data, and have inevitably become a major target for cybercriminals. Of all the messages sent to Microsoft 365 inboxes in a single month, on average, about 55 billion are spam or bulk emails, and 20 million contain some form of malware.

A popular approach among scammers is to send phishing emails that contain malicious links or attachments. After clicking these links, victims are redirected to fake pages that request their credentials or personal details, giving scammers access to the victims' emails, contacts, files, folders, and more.

Cybercriminals can then use the compromised email accounts to hunt for personally identifiable information (PII) in the mailbox, send unauthorized emails to partners or vendors seeking confidential data, and a lot more.

Real-life case

After the email account of a finance executive at a construction company was compromised, cybercriminals got hold of details of the company's suppliers by accessing the executive's emails. The scammers then sent the executive a spoof email disguised as an email from one of the suppliers—a supplier of electrical equipment—along with an invoice for their latest consignment.

Next, they forwarded the email to the payment officer from the executive's compromised account. The payment officer processed the invoice and transferred funds to the account mentioned in the invoice. The scammers then deleted all the emails to keep the executive in the dark about the transaction; using the compromised account, they also gained access to confidential financial data as well as personnel and payroll information.

Subject: FW: Please initiate payment immediately

Jane Bella [jbella@misceabc.com]

Sent: Fri 03/15/2019 05:56 PM

To: John Morris [jmorris@misceabc.com]

John,

Please check Jacob's email below for new wiring instructions. This needs to be done today.
Have a nice weekend.

Regards,
Jane

Not a real forwarded message

---------- Forwarded message ----------

Jacob Gregory [mailto:jgregory@xyzelectrical.com]

Sent: Fri 03/15/2019 05:30 PM

Subject: Please initiate payment immediately

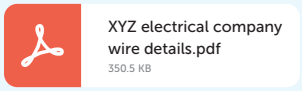
To: Jane Bella [jbella@misceabc.com]

Jane,

Attached, please find the new wiring instructions for Invoice no. 23766.
Please process the payment today.

Regards,
Jacob

1 Attachment | Download as Zip



Reply | Reply All | Forward

Signs of Microsoft 365 account compromise

Hackers know that admins are always busy, and it is difficult for them to keep track of all the activity in their Microsoft 365 setup. Let's assume that hackers have gained access to one of your company accounts and some company data and personal information along with it. In this section, we will discuss some of the telltale signs of a compromised account, which will help with faster detection and enable quicker remediation.

1. Unusual account logins

If a login has occurred from an unusual IP, location, or at an unusual time, this could indicate the account has been compromised. Admins should keep an eye out for such anomalous login events.

Audit user logons during non-business hours

Using M365 Manager Plus, admins can view details, such as the IP from which a user logged on, whether the logon was performed during non-business hours, and more. Learn how to audit user logon activities during non-business hours using M365 Manager Plus.

2. Mailbox manipulation

Admins should suspect an account has been compromised if they receive complaints about emails being deleted from a user's inbox or emails being moved under new folders; new inbox or forwarding rules that weren't created by the user or the admin are suspect as well.

Detect mailboxes with forwarding rules

M365 Manager Plus offers the ability to perform management actions from within reports. With this ability, admins can generate the mailboxes with the External Mail Forwarding report. Then they can disable external mail forwarding for clients who have enabled this capability—all from within the report. Admins can also set exceptions to external mail forwarding with a few clicks.

Learn how to disable email forwarding by clients to external email addresses using M365 Manager Plus.

Advanced mailbox search

M365 Manager Plus' Microsoft 365 content search feature helps you keep an eye on all the emails sent and received by your organization. Using this feature, you can quickly and easily find emails containing personal information or payment requests, and get notified even if the scammers delete or move the emails. This tool also ensures compliance with regulatory mandates that restrict the sharing of certain personal information through emails.

3. Access from unauthorized devices

Scammers often connect their mobile devices to a compromised account in order to send and receive emails from it. Admins should look in their Microsoft 365 setup for any unauthorized devices connected to users' Outlook Web App.

Detect active mobile devices

M365 Manager Plus' Mobile Devices report displays all the mobile devices that are configured to synchronize with users' Microsoft 365 mailboxes. It includes information such as user name, device name, device type, device ID, first sync, and device IMEI number.

4. Inability to access Microsfot 365 account

An unusual increase in the number of failed logins and password reset messages could indicate that a number of Microsoft 365 accounts have been compromised and their passwords reset, preventing actual users from accessing their accounts.

Track logon failures

M365 Manager Plus tracks the number of daily logon failures, and it also categorizes logon failures by user, which helps detect which user accounts may be under attack.

Some of the other signs of compromise include changes in the user's display name in the Global Address List; modification of the user's profile details such as name, phone number, and zip code; or an unusual signature.

Five things to do immediately if you suspect an account has been compromised

In the event of a compromised Microsoft 365 account, you must immediately cut off the hacker's access to your Microsoft 365 setup. The following actions will ensure that the hacker is unable to regain control of your account.

1. Reset the password and enable MFA

If an account compromise is suspected, the first step is to immediately reset the password of the compromised account. This stops the attackers from gaining access next time they attempt to log in; to ensure Microsoft 365 accounts remain secure, admins should also enable and enforce multi-factor authentication (MFA) for end users.

M365 Manager Plus advantage

While Microsoft 365 provides the option to configure MFA, you need to work between different tabs to select users and configure settings. M365 Manager Plus, on the other hand, simplifies this task by allowing you to configure MFA for multiple users from a single console in just a few clicks.

2. Remove mailbox delegates

Delegates can send emails on behalf of another user, read emails from a colleague's inbox, receive copies of meeting invitations, and more. If you suspect there's been a compromise, removing mailbox delegates ensures that malicious entities in your Microsoft 365 setup can no longer send emails or reply on another user's behalf.

M365 Manager Plus advantage

M365 Manager Plus' Mailbox with Delegates report lists the mailboxes that have delegates. The Mailbox Delegation management feature provides the capability to import this list and remove delegate permissions from multiple mailboxes in one go.

3. Remove suspicious mail forwarding rules

After gaining access to an Microsoft 365 account, hackers often set up forwarding rules to send all the emails from the victims' inboxes to their own inbox. Forwarding rules are immune to the usual threat response measures, such as password reset, and they allow hackers to remain in possession of confidential data for a longer time.

M365 Manager Plus advantage

M365 Manager Plus' Mailboxes with External Mail Forwarding report provides the list of user accounts with mail forwarding in place as well as the email ID to which the forwarding is configured. The tool also provides the capability to perform management actions from the report itself so that admins can easily view and disable external email forwarding for all users who have enabled this capability. Admins can also easily set exceptions to external mail forwarding.

4. Remove the suspected compromised account from security and distribution groups.

Microsoft 365 security groups are used to grant a specific set of user accounts access permissions to important resources in the organization. If the compromised account belongs to one of these groups, cybercriminals can access important emails, critical business documents, financial data, PII, and more. Removing suspected accounts from these important groups as soon as possible can help limit the damage to the organization.

M365 Manager Plus advantage

While using the Microsoft 365 admin center, admins have to add users to or remove users from groups one at a time. Instead, by using M365 Manager Plus' **Modify Microsoft 365 Group Members** management feature, you can remove user accounts from multiple Office 365 groups in one go.

5. In-depth review of audit logs

To understand the extent of account compromise, it's vital to review all the activities performed by the suspected account, beginning with the date before suspicious activity occurred to the current date.

M365 Manager Plus advantage

Microsoft 365's Security and Compliance Center only stores logs for 90 days, meaning admins have to export and save audit logs periodically to comply with regulatory standards. Aside from increasing admins' workloads, this takes up a large amount of storage space in the organization's database.

With M365 Manager Plus, you can store and archive audit logs indefinitely. This provides better access to audit logs, which helps a great deal when it comes time for security audits and investigations.

Top Three

M365 Manager Plus security features

1. Comprehensive Exchange Online auditing and reporting to secure your organization from hackers.

   Exchange Online reporting

2. Hassle-free Azure AD auditing and reporting to track users, groups, contacts, and licenses.

   Azure AD reporting

3. Exhaustive reporting on all administrator activities to strengthen your organization's security.

   Microsoft 365 activity reports

ManageEngine
M365 Manager Plus

M365 Manager Plus is an extensive Microsoft 365 tool used for reporting, managing, monitoring, auditing, and creating alerts for critical incidents. With its user-friendly interface, you can easily manage Exchange Online, Azure Active Directory, Skype for Business, OneDrive for Business, Microsoft Teams, and other Microsoft 365 services from a single console.

$ Get Quote Download