Hardening your Office 365 configuration: Best practices for preventing email account takeovers

Office 365 email account takeovers show no signs of slowing down in 2019. Organizations responding to these attacks often must deal with compromised credentials, unauthorized wire transfers, and expensive remediation.

How do account takeovers happen?

In the first phase, the cybercriminal sends a phishing email, often requesting the employee use the link provided to review a document. The link takes the employee to a website that requests his or her credentials. Once an employee provides credentials, the cybercriminal can start to leverage access to the account in several ways.

How does an account takeover put you at risk?

With access, the cybercriminal can search for information on wire instructions, electronic payments, or vendor invoicing. They may engage in other reconnaissance—monitoring traffic to the inbox, watching the relationships between the parties, and observing the details of their communications—to determine how to steal funds. Theft may occur when the criminal issues fraudulent payment instructions, impersonates a vendor, or diverts the employee's direct deposit.

If the employee has no responsibility for payments, the cybercriminal will use the inbox as a platform to phish other employees. Access to the organization's address book often provides details about whom to target in finance or accounts payable. Using a legitimate email account, the cybercriminal appears to be an employee and can defeat safeguards such as flagging of external emails. And of course the compromised inbox may have years' worth of emails that include sensitive data.

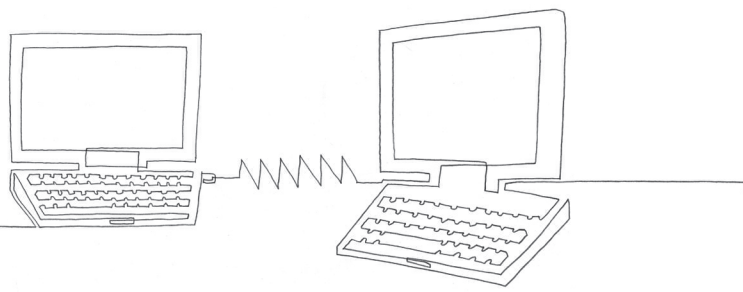
A cybercriminal who uses the account to communicate with other parties, posing as the employee, will usually create forwarding rules to cover their tracks, while the employee remains unaware that communication is taking place.

Email account takeovers are one form of business email compromise (BEC). For more on BEC generally and how to protect your organization, see Business email compromise best practices.

How to harden your 0365 configuration

To help reduce the frequency and severity of these attacks, 0365 administrators should take the following steps to mitigate the risk of a successful attack in the Office 365 environment:

- require multi-factor authentication
- limit or disable remote access
- use Microsoft's Secure Score
- manage message forwarding
- turn on audit logging and mailbox auditing



1. Require multi-factor authentication (MFA)
The most important thing you can do to protect your organization is to require MFA for users to log in to O365. Microsoft provides guidance for O365 administrators:

- Set up multi-factor authentication for Office 365 users
- Plan for multi-factor authentication for Office 365 deployments
- Users should select the MFA mobile app for authentication. SMS (text message)-based MFA is no longer regarded as secure because of SIM swaps and other social engineering risks.

2. Limit or disable remote access
The majority of email compromises occur through Outlook web access (OWA). Disabling OWA for the organization or enabling it only on an as-needed, per-user basis offers additional protection to your organization.

LMG Security also notes that "By default, Office 365 allows access via POP3, IMAP, MAPI, EWS, OWA, and ActiveSync for every system user. However, users rarely need access using all of these methods. Does your organization use POP3 or IMAP for email connections regularly? If not – disable them."

3. Use Microsoft's Secure Score
Built into O365, the Secure Score analytics tool looks at the security settings you have enabled, suggests areas for improvement, and walks you through how to make changes.

- Microsoft Secure Score

4. Manage message forwarding
Cybercriminals often set up inbox rules to forward messages to an external account or to delete messages in order to hide them from the inbox owner. Sometimes the only sign of an account takeover is the presence of unauthorized mailbox rules.

- From an administrative level, you can configure O365 to alert you every time a user sets up a new inbox rule, which can then be followed up on to check the legitimacy of the rule.
- If there isn't a business need for them, it's even more secure to disable forwarding and deletion rules for all users and enable them as needed only for specific users
- Office 365: Determine accounts that have forwarding enabled

5. Turn on audit logging and mailbox auditing
If your organization does experience an account takeover, it's essential to have the right logs. Without them, you have to assume the bad actor accessed everything, which can lead to having to provide notification to individuals whose information may not even have been affected.

To provide useful logs, you need to 1) turn on audit logging and 2) enable mailbox auditing for each user mailbox. You need to turn on both before you experience an incident for the logs to be helpful. Starting in 2019, Microsoft plans to enable mailbox auditing by default, but you should check to see whether it's enabled, especially if you've made changes to the default audit configuration.

- Search the audit log in the Office 365 Security & Compliance Center
- Enable mailbox auditing in Office 365
- Consider extending the retention time for logs beyond the default 90 days or using a security information and event manager (SIEM) for long-term storage of the logs.

Tools to manage configuration changes
Microsoft provides information about how to use Powershell to manage your O365 configuration.

- Manage Office 365 with Office 365 PowerShell
- Connect to Office 365 PowerShell

LMG Security has a useful blog post with additional information. They have also developed an open-source script to help automate the process.

- Secure Your Office 365 Accounts
- https://github.com/LMGsec/O365-Lockdown

CBSL569_US_01/19