Email Phishing Compromise – Case Study Report

- *August 2, 2025*

Any business can be a target of a phishing attack. In this post, we'll share a recent phishing attempt on a client, how we handled it, and what we did to stop it happening again.

Preliminary Incident Report

Email phishing attacks are more common than most people think—and they don't just target big corporations. They can (and do) happen to any business, and when they do, the impact can be serious. In this post, we'll walk through a recent phishing attempt that targeted one of our clients. We'll break down what happened, how we responded, and what steps we took to prevent it from happening again. The clients name has been removed for security.

15th July 2025 Incident (Email Phishing Compromise) *Last Updated: 2025-07-16*

Executive Summary

- On the afternoon of 15th July 2025, the client received a phishing email from a compromised contact containing a malicious *Microsoft SharePoint* the client subsequently clicked on the link but reported that nothing happened.
- Shortly after interacting with the link, the attacker attempted and eventually succeeded in accessing the client's *Microsoft 365 (M365)* account. Logs recovered suggested the attackers may have compromised his password but were unable to reset his Multi Factor Authentication (MFA)

- However, the attacker was able to bypass the MFA requirement and access some services such as *Azure Active Directory* and It is believed the attacker used a session token from the client's previously authenticated *M365* session, which would have been intercepted when he clicked the malicious link.
- During the intrusion, the attacker created and distributed a malicious file, which was then shared via a link via email to 334 of the client's contacts, and manipulated mailbox rules to conceal activity. The email and link were of a similar nature to the one the the client's fell victim to.
- ANother IT's alerting rules (via their 365 *Saas Alerts* service) were triggered to the attack – specifically the creation of the email rule – and that the user account had been compromised triggering ANother IT to contact the user directly.
- The user did try to email for IT support, when a contact queried about an email apparently sent by him, but this was not received as outbound email had been re-routed by the attacker.
- The issue was reported early on 16th July 2025 by the clients colleague, ANother IT engineers had already reacted by temporarily locking his account and resetting the password and MFA.
- At this time no evidence has been found to confirm that any other user accounts or resources have been compromised. It appears the attacker only used the access to send further phishing emails to the client's contacts.

Detailed Summary

At **13:46 GMT** on 15 July 2025, the client received an email purporting to be from a known contact. The email contained a link to what appeared to be a *Microsoft SharePoint* document.

Following receipt, the client clicked the link but reported being unable to access the document. It is now believed that this was a phishing link designed to steal *Microsoft M365* credentials from the unsuspecting victim.

Beginning at **16:27 GMT,** a series of login attempts from various IP addresses (primarily from the United States and Enfield, UK) were detected. Logs obtained from *Microsoft* suggest that the attacker was able to obtain the correct password for the account and attempted to complete MFA via SMS, phone call, and OATH-based app – all of which were initially unsuccessful or interrupted.

The log entry for the phone call suggests an automated verification call to a phone number ending "83" was made. It is believed the client's own mobile phone number ends in "83", and that this number was linked to his account as an MFA authentication method.

Between **16:31 GMT** and **17:03 GMT** there is no record of attacker activity, but then at **17:03 GMT,** the attacker successfully authenticated using a previously hijacked session token from a UK-based VPN address (geolocated to Enfield).
Between **17:03 and 17:42 GMT,** the attacker accessed *Azure Active Directory* and *OneDrive,* using a rotation of VPN IP addresses (all geographically associated with Enfield, UK). During this period:

- A malicious file *was* created and shared via *SharePoint* with **334 external contacts** – it is believed these contacts were obtained from the client's online address book
- An email inbox processing rule named **"45u5"** was created to mark all emails as read, delete them, and disable further rule processing – a typical tactic to obscure incoming alerts

The attacker's final activity was logged at **17:42 GMT.**

At an alert rule on the *Saas Alerts* application, administered by ANother IT to monitor *M365* activity for the client, triggered at **17:46 GMT,** specifically flagging the creation of the suspicious email forwarding rule. At the time of activation, this rule was just sent to "alert" and not to take any automated action, which was the client's choice on implementation.

At some time after his, the client received contact from a colleague to ask about the validity of a message which had apparently come from him, but to which he had no knowledge of.

At **19:12 GMT,** the client attempted to notify the IT helpdesk – but outbound mail had been redirected.

At **20:00 GMT,** the client's contact emailed various contacts (including the client) to warn that the previous email from their contact was a phishing link and not to click on it.
It was not until **06:39 GMT** on 16th July 2025 that the incident was formally reported to ANother IT by the client.
At **07:46 GMT** on 16th July 2025, remediation actions commenced. ANother IT revoked active session tokens, disabled the compromised account, reset the password, and reconfigured MFA settings to prevent further access. The email rule created by the attacker was also removed.

Anatomy of the Attack

This compromise appears to have been executed using a **reverse proxy-based phishing attack*,** a tactic increasingly adopted by threat actors targeting Microsoft 365 environments. The likely sequence of events is as follows:

1. Delivery of a Phishing Link

The attacker sent a phishing email from the compromised third-party contact, appearing legitimate and containing a link to what seemed to be a Microsoft SharePoint file. The link likely pointed to a fake Microsoft login page, hosted behind a **reverse proxy** (commonly using open-source frameworks such as Evilginx, Modlishka, or Muraena).

2. Adversary-in-the-Middle (AitM) Phishing Page

When the user clicked the link and attempted to log in, the reverse proxy intercepted the interaction in real time, relaying traffic between the victim and Microsoft's actual login infrastructure. This allowed the attacker to capture both the **username, password,** and most crucially, the **session authentication cookies.**

3. Session Cookie Theft and MFA Bypass

With a valid session cookie in hand, the attacker did not need to complete Multi-Factor Authentication (MFA), as the session token was already trusted by Microsoft's services. This bypasses MFA protections entirely, enabling immediate access to Microsoft 365 services such as Azure Active Directory and OneDrive.

4. Partial Access and Limitations

Although the attacker was able to access certain services using the hijacked session, logs suggest that attempts to authenticate through other methods (e.g., fresh logins requiring MFA) were unsuccessful. This indicates the attacker **relied solely on the stolen session token** and was likely unable to escalate access further (e.g. to *Outlook* or administrative controls) due to MFA or other policies blocking full login reauthentication.

Conclusions

- The incident was the result of a **credential phishing attack** originating from a compromised third-party contact.

- The attacker gained access using a **session token,** likely obtained during the phishing process, thereby circumventing MFA protections.
- Once inside, the attacker executed a **malicious file distribution campaign** and **implemented inbox rules** to cover their tracks. However, it appears that no other malicious actions were undertaken (likely because the attacker was unable to fully bypass MFA).
- A significant delay occurred in reporting the incident, allowing the attacker to operate within the environment for over four hours and distribute phishing links to a wide audience.

Client Recommendations

1. Notification of Potential Victims

Notify all users which are believed to have received phishing emails from the client's account, requesting that they do not click on the link.

2. User Awareness Training

Reinforce ongoing user education on identifying phishing attempts, especially those appearing to come from trusted sources.

3. MFA Hardening

With ANother IT, review and strengthen MFA policies by requiring app-based authentication and disabling SMS/voice-based MFA where feasible.

4. Helpdesk Contact Management

Maintain up-to-date contact methods for incident reporting and clearly communicate escalation procedures to all users.

5. Third-Party Risk Management

Consider notifying original sender of the broader impact and conduct a review of exposure to compromised contacts in other client environments.

ANother IT Actions

ANother IT will undertake a thorough review of this incident and implement further security lessons and training, so that the users can be better protected from similar attacks in the future. Some of these actions include:

- Reviewing existing and implementing new *Saas Alerts* rules to detect and automatically respond to potentially malicious actions by immediatley signing the user out of all logged in sessions to make inactive the session cookie if stolen.
- Reviewing current *M365* tenant security standards and working with clients to implement stronger security baselines for all.
- Implementing phising and cyber security awareness training for all users.

Contact us