A recent attack on my organization

I currently hold the role of "Infrastructure & Cybersecurity Administrator" at my organization. I have been with this organization for 7 years and started as a Level 1 Helpdesk administrator. We are a small organization with fewer than 250 employees, and our "IT Team" consists of fewer than 4 people on the infrastructure side. We are heavily involved in day-to-day operations.

To provide a little more background, we had a ransomware attack back in 2019, right around Thanksgiving, that took over 3 weeks to fully remediate. As a remediation effort, we moved toward segmenting our environment and implementing mandatory MFA for our users. Administrator accounts have been separated from our employees' name accounts, and these are separate from our regularly used emails to minimize risk. We conduct annual penetration testing to comply with our insurance requirements and maintain awareness of our vulnerabilities. In addition to our annual penetration testing, we also provide mandatory cybersecurity awareness training for all employees.

This is a true and accurate account of a recent cyberattack we experienced that had the potential to cause major damage. However, thanks to the efforts of our team and our quick response time, we were able to reduce future exposure risk by understanding and remediating our vulnerabilities. For the confidentiality of the individuals involved, I have redacted the names of the victims and the response team. I will refer to myself and my participation and roles in this attack as "Admin A". My supervisor, who is "Director of Systems & Network Infrastructure," is "Admin B". Additionally, "Admin C" is our external contractor who has worked with our environment for over 15 years and is consulting with us. Last, our "Senior Director, Enterprise Systems" will be referred to as "Director A". The report included is similar in many aspects to our final report to our CIO regarding the incident.

Incident Response – "User's Identities compromised" 11/13/2025

1. Incident Overview

- Date/Time Detected: 11/13/2025 1:35 PM EST
- Reported By: "Reporting User" (First Point of Contact) and other staff.
- Reported To: "Admin A" , "Admin B" , "Admin C" , "Director A"
- Incident Category: Phishing - Unauthorized access and use of Outlook/Hijack of user account.
- Severity Level: High
- Current Status: Contained

2. Summary of the Incident

- Description: Attackers gained access to "User A"'s account around 11:02 AM EST 11/14/2025. Around 1:26 PM, a mass email is sent from "User A"'s account to internal and external people
- Affected Systems/Assets: Microsoft 365 account. Outlook on the web.
- Business Impact: Data exposure, External exposure, Possible Reputational Damage, and external liability.
- Initial Detection Method: User Report

3. Timeline of Events

Use the table below to document event chronology:

Date/Time	Event Description	Responsible Party
11/13/2025 11:02 AM	Attackers gain access to "User A"'s account. The origin of the attack is unknown. We were unable to find a specific email or web URL responsible.	Attackers
11/13/2025 11:20 AM	Attackers register third-party authentication device with "User A"'s account.	Attackers
11/13/2025 11:39 AM	Microsoft locks "User A"'s account due to "Risky Sign–ins" policy. This was triggered by sign-ins from Amsterdam, Lagos, and North Kansas City, MS.	Attackers
11/13/2025 12:25 PM	Per our "Risky Sign-In" policy, the attackers were able to clear the account block using the unauthorized MFA Software.	Attackers
11/13/2025 1:26 PM	A mass Email was sent to 726 recipients. Roughly xxx were external. Of the 726, 620 were delivered. These Emails contained a PDF that, when opened, posed no immediate threat, but embedded in that PDF was a link that harvested Microsoft credentials and session tokens. Internally, of the Emails that went out, only 1 user was compromised from clicking the link (User Badm).	Attackers
11/13/2025 1:28 PM	"User A"'s MFA methods and active sessions are revoked in Azure AD. Sign in blocked.	"Admin A".

11/13/2025 1:30 PM	"Admin B" sends out correspondence to the entire organization, alerting staff of malicious emails. Instructions are to report back to IT if you open the attachment. 17 users report back, we respond by resetting their passwords and locking their accounts while working on containment.	"Admin B" / "Admin A"
11/13/2025 1:55 PM	User B reports that he clicked the link in the PDF. Account is promptly locked, we remove all MFA methods, and revoke all active sessions.	"Admin A".
11/13/2025 – 2:00 PM – roughly 6:00 PM	We continue to investigate the incident and monitor the sign-in logs of affected accounts. Users who only clicked or opened the attachment did not show any suspicious sign-in activity. The link inside the PDF is responsible for stealing credentials and compromising the accounts.	"Admin A". "Admin B" "Director A"
11/13/2025 6:00 PM – 10:30 PM	• "Admin C" works on a script to purge email from all internal users' inboxes. The script is unsuccessful due to specific processes in Microsoft 365. He opens a ticket with Microsoft to get the script working for a successful purge. • "Admin A". uses a script to pull all authentication methods of users in our directory who have a 365 license. We investigate each account with a "Software Oath" authentication method. Of the 19 people who had this method, 1, User C, has an unusual sign-in attempt that failed. His account is locked and sessions revoked out of precaution. During this time, we rotate the passwords of the affected users who opened the PDF and send them all new credentials via a protected link sent from 1Password. • "Admin A"., "Admin B", "Director A", and "Admin C" modified policies in Microsoft 365 to improve security.	"Admin C" , "Admin A".

	• Our Asia team was notified and took action to contain the incident and verify that users were safe.	
11/14/2025 7:30 AM – 10:30 AM	We began helping individuals with account recovery, including rotating passwords. Even though User C had malicious sign-ins that failed, we re-registered his MFA and changed his password.	"Admin A". , "Admin B".
11/14/2025 10:30 AM -11:30 AM	"User A" specifically assisted with account recovery, including re-registration of MFA devices. Time was spent reviewing her internet history and inbox to identify the origin of the attack, but we were unable to find any relevant information. CrowdStrike was also installed on "User A"'s office MAC at this time.	"Admin A".
11/14/2025 1:40 PM	"Admin C" was successful with his script and the purge of the remaining malicious emails from all internal users' Outlook accounts. Incident now fully contained.	Habib B.
11/14/2025 2:30 PM	Out of precaution, we had "User A" bring in her home MAC for inspection on Monday to review for possible malware. This is an unmanaged device. Additionally, her MFA was re-registered, and her password was changed.	"Admin A". , "User A"

4. Investigation & Analysis

- Root Cause: We were unable to determine the exact link or email that compromised "User A".
- Attack Vector: Phishing, Session Hijacking, Malicious email sent from the affected user's inbox.
- Indicators of Compromise (IOCs): Unauthorized registered devices. Unusual login activity with Authentication. Notification from staff and mass email sent from the affected user's machine.
- Evidence Collected: Sign-in logs with IPs and locations, account audit logs, eDiscovery of E-mails, and Message trace of "User A"'s outgoing email account.

5. Containment

- Actions Taken: Immediately upon notification, we revoked all current sessions, changed the user's passwords, and removed all authentication devices on accounts that clicked

the link inside the PDF. Those who opened the PDF but did not click any links had just their passwords rotated; these users show no suspicious sign-ins or activity. Our teams worked on purging emails from users' inboxes. We inspected all users with more than 2 methods of authentication. Any user with a generic SOATH had the method forcefully removed from their accounts. The original script failed, and a ticket was opened with Microsoft. Emails were purged on 11/14/2025. "User A"'s home Mac was brought into the office for investigation and taken offline on November 14, 2025. 4 new conditional access policies were set up.

- 1. Block risky sign-ins from being re-established via MFA by the user. This will require admin approval and investigation going forward.
- 2. All Office 365 application sessions in a web browser will require authentication every 8 hours for all users.
- 3. All Office 365 desktop applications will require reauthentication every 14 days.
- 4. We set up a "block list" to block Office Application traffic from malicious IP addresses from which the traffic originated. We can add to the list for future incidents.

- Date/Time Containment Began: 11/13/2025 1:26 PM
- Responsible Party: "Admin A", "Admin B", "Admin C", "Director A"
- Effectiveness Assessment: The steps taken were effective in immediately terminating access to the attackers. Purging the emails helped prevent the incident from spreading further. Removing the Software authentication devices would have eliminated any potential for further malicious activity.

6. Eradication

- Steps Performed: Revoked all current sessions and changed passwords of any user who opened the PDF out of precaution. Users who had suspicious sign-in activity had all authentication methods and sessions revoked. Email was purged from all internal users' inboxes.
- Verification of Success: No further sign-in attempts from attackers after initial action was taken at 1:30 PM EST. Review of sign-in logs on the morning of November 14, 2025, showed no suspicious activity.

7. Recovery

- Systems Restored: All user accounts were restored by noon on 11/14/2025. "User A"'s home Mac has not been returned to her pending further inspection.
- Date/Time Restored: 11/14/2025 7:30 AM to 12:00 PM
- Monitoring in Place: Notifications will be set up to alert Microsoft 365 administrators when a new device is registered for MFA for all accounts.

8. Lessons Learned

- What Worked Well:
  - Fast response time. We immediately locked the accounts and prevented any further emails from being delivered to recipients. We had specific users immediately notify

IT, possibly prevent even further spread. Most users who opened the PDF were accountable for their actions.

- What Didn't Work:
  - We did not receive a notification that a new MFA device was registered.
  - Our MFA and risky sign-in policies were misconfigured, which could have prevented access to "User A"'s Inbox.
  - It took us nearly a day to successfully purge emails from our inboxes. This was due to issues with the process outlined by Microsoft.
  - Phishing email was not reported and was used as a point of entry.
- Preventive Actions: Further Training. Implantation of new Conditional Access policies. Purger of Malicious Emails from internal accounts.
- Follow-Up Tasks: Investigate "User A"'s home Mac and determine Work from Home requirements to provide the appropriate managed device.

9. Communications

- Internal Notifications: Leadership Notified.
- External Notifications: Determined by CIO and Legal Team

Conclusion

As stated previously, this is a real account of an actual attack that took place within my organization over the last month. Coincidently, we were also undergoing penetration testing during this time, but it was unrelated. This attack shows how important it is that users undergo awareness training. Additionally, we have seen a spike in methods that allow attackers to capture sessions of currently logged in users. MFA is a strong piece of any organization's policy and has become standard practice. Even though MFA is a strong tool in combating account exploitation, it remains vulnerable to the human factor. Our team also used this as an opportunity to strengthen our back-end rules and change practices that were less than secure. One important piece, by default, office 365 administration allows users to unlock their own accounts after a "Risky sign-in" is detected. Once the attackers had control of User A's account, they could authenticate using their own registered device. We have changed our rules to allow ALL account unlocks to require administrator approval and review.