

One Click, Total Access: Stopping Email Account Takeover

How one phishing email can compromise Microsoft 365, and the controls that stop it.



Karen was having a bad day.

Her kids woke up late which meant she was rushing through traffic to get to the school drop off and in the dark she almost ran into a middle schooler crossing in front of her in the school parking lot. Slamming on her brakes, she spilled coffee on her new slacks. By the time she arrived at the credit union she was ten minutes late and so low on gas she didn't know if the car would make it to the nearest gas station after work.

Signing onto her computer in the accounting office, there was an urgent email from the CEO requesting an immediate \$50,000 wire to a building contractor to start the branch expansion project the credit union announced the previous week. There was a link in the email to the contractor's invoice where there would be further instructions.

Karen clicked the link.

She was presented with a Microsoft logon page and instructions to use her network credentials and MFA code. She followed the instructions and was presented with the invoice, which she downloaded and printed a copy for her records. Then she logged into the wire transfer web site and initiated the transfer to the builder. She then responded to the CEO's email saying she had sent the money as requested.

At the nine o'clock executive stand-up meeting, Karen was horrified to learn the CEO hadn't sent the email and never asked her to send money to anyone. Panicked, she ran out of the meeting directly to the IT administrator's office.

Anatomy of the Attack

Unfortunately, this is a common occurrence in too many corporate offices. This is an example of an **email account takeover**.

A bad actor took advantage of a known announced event at the credit union (the branch expansion) to target the CFO with a phishing attack. They setup a man in the middle "reverse proxy" website in front of the Microsoft login page and the link they sent was to that site. It looked exactly like a Microsoft logon page, but was programmed to intercept the username, password, and MFA codes from Karen and pass them along to Microsoft and steal the resulting session token, which allowed him to stay persistent in her account.

Once Karen entered this information, the attacker had her credentials and access to her online email account where he configured inbox rules to hide himself and intercept sensitive emails including password resets and financial notifications. He also used her credentials to access the credit union's SharePoint system where he downloaded the entire member contact file including account bases, balances, social security numbers, names and addresses. Additionally, he was also able to impersonate Karen by sending phishing emails to recipients in her address book. He scammed another \$25,000 from them using similar tactics.

How do you defend your credit union from email account takeovers?

Business email account takeovers are common with Microsoft 365, but they can be prevented through a layered approach that includes continuous management and oversight.



Question urgent requests

Train your users to be suspicious of urgent sounding emails. Do not automatically trust emails, even if they appear to be from a trusted source. If in doubt, follow up out of band (i.e. a phone call) with the sender.



Enforce MFA for everyone

Force multi-factor authentication for all users and educate users to scrutinize each prompt so they only approve ones they know they've initiated.



Require dual control

Ensure multi-layer controls (such as wire transfer approvals) are effective and working. Don't allow single individuals to transfer money.



Report unexpected MFA prompts

Educate users to alert security teams if they receive unexpected MFA prompts. Do not approve unexpected prompts and change your passwords if you receive one.



Limit access to managed devices

Properly configure conditional access and session controls so users can only access 365 data from company managed devices.



Block unapproved locations

Block access from unapproved locations. For roaming employees, require Continuous Access Evaluations to immediately revoke sessions if their IP address changes to an untrusted location.



Shorten sign-in sessions

Reduce sign-in frequency and force sessions to re-authorize and re-verify device health on a frequent basis.



Enroll devices in Intune

Enroll authorized devices in Intune and require them to be encrypted, up to date, and password protected prior to allowing connections.



Block external auto-forwarding

Block automatic external email forwarding to prevent a compromised mailbox from routing emails to external attacker domains.



Restrict third-party app consent

Configure Entra ID to prohibit users from granting permissions to unverified third-party applications.



Harden Defender policies

Enable spoof intelligence, strict preset security policies, and first contact safety tips in Defender.



Automate risk response

Enable Entra ID Governance and Identity Protection to automatically force a password reset or block access if it detects elevated user risk.



Audit for shadow inbox rules

Audit for shadow rules in inboxes that move items to obscure folders or delete messages containing financial keywords.



Classify and encrypt data

Encrypt sensitive data everywhere. Use data classification policies for all online stored data and restrict access to only those that need it to do their jobs.



Tag external email

Mark external emails with a warning banner that advises recipients not to trust links or attachments without further verification.



Next Steps

Microsoft 365 is a powerful productivity suite, but it's also very complex and difficult to maintain secure configurations over time. Regularly audit your environment or use a centralized management toolset leveraging configuration templates and regular reporting to ensure the environment remains securely configured and surfaces areas for improvement. Finally, continually train your users to be suspicious of emails, slow down, and think before clicking. A common refrain: **"If in doubt, throw it out!"**