



When a trusted email becomes a weapon

How an automated account takeover was contained in six seconds

The attack	Time to containment	Data loss
Relay phishing page sent from a real, compromised partner account	6 seconds, fully automated	No evidence any data left the organization

This is not a hypothetical scenario. This attack happened in April 2026 at an organization in Oklahoma. It was handled by Counsel Cyber's founding team at our affiliated managed IT provider, before Counsel Cyber launched. Identifying details have been left out.

"I can't open this Microsoft document. I put in my credentials but it won't open."

The staff member, texting IT for help. An attacker was already inside her account.

She did what anyone would have done

She received an email from a business partner she had worked with for years. It was a real email, from a real person, at a real organization. That partner's account had already been compromised, and the attacker was using it to reach everyone the partner did business with. No misspellings, no suspicious sender, nothing for a filter or a trained eye to catch.

The email linked to what looked like a shared Microsoft document. She entered her Microsoft 365 password and MFA code on what looked like a normal sign-in page. It was a relay: it passed her credentials and code to the attacker in real time, which is how attackers get past MFA. The document never loaded, so she texted IT.

What happened in the next few seconds

This wasn't a person at a keyboard. It was an automated script built to take over an account and dig in before anyone noticed. Within seconds of getting in, it:

- Registered a new authenticator app (software TOTP) as an MFA method, to keep access even after a password reset
- Changed the account's existing MFA settings
- Created inbox rules to forward email to an outside address and hide incoming messages
- Began marking messages as read and deleting them to cover its tracks
- Operated from a datacenter IP address, a common sign of automated attack infrastructure

Why the usual tools didn't stop it

This organization had done the right things: spam filtering, MFA, endpoint security. Each did its job. None of them is designed to watch what happens after a valid sign-in. Once the attacker had a working session, the only thing that could catch them was monitoring of activity inside Microsoft 365.

A compromised Microsoft 365 account rarely stops at email. It can be a stepping stone into accounting, payroll, file storage, and every other system tied to that identity.

Then it was over. In six seconds.

Because this organization had cloud security monitoring in place, the platform detected the behavior and responded automatically, before IT had even read the text:

- Revoked all active sessions, cutting the attacker off
- Reset the user's password
- Removed the MFA method the attacker had just registered
- Deleted every malicious inbox rule



From credential entry to full containment took 6 seconds. The follow-up investigation found no evidence that any data left the organization.

When IT called her back, she said: "I did not get phished. That was a valid email from someone I talk to all the time." She was right about the email. The sign-in page was the trap.

What this means for a law firm

Swap the staff member for a paralegal and the business partner for opposing counsel or a title company, and the same six seconds put privileged communications and payment instructions in an attacker's hands.

Three questions every firm should answer

- Is someone watching our Microsoft 365 or Google Workspace activity 24/7?
- Are our critical platforms behind single sign-on and conditional access, so there is one monitored front door instead of many?
- If an account is compromised today, will we know in seconds, or find out weeks later?

The difference between an incident and a breach is often seconds.

Schedule a confidential security assessment. (737) 325-2520 | hello@counselcyber.com | counselcyber.com
Counsel Cyber, headquartered in Dallas, Texas. Serving Texas, Arkansas, Louisiana, Oklahoma & Kansas.