INFOTANK SECURITY INCIDENT REPORT

Date of Incident: 09/14/26 | Client: Holy Spirit Catholic Church | Affected User(s):ccossio@hsccatl.com | Severity: High

INCIDENT SUMMARY

An attacker appears to have obtained the user's email address and password and attempted to sign in to the account. However, the login attempts were timing out because the required MFA prompt was not being completed.

MFA was preventing the attacker from successfully accessing the account.

Immediate containment actions were taken, including resetting the username and password to secure the account and prevent unauthorized access.

AFFECTED USER

Name	Fr. Cristian Cossio
Email Address	ccossio@hsccatl.com
Role	Parochial Vicar
Department	Administration
Severity	High

InfoTank

SECURITY INCIDENT REPORT

INVESTIGATION SUMMARY & FINDINGS

1. HOW THE INCIDENT WAS IDENTIFIED

The Account Compromise Protection security add-on alerted us to the incident immediately after detecting multiple failed sign-in attempts on the user's account, prompting an investigation.



2. INVESTIGATION FINDINGS

- Multiple failed MFA authentication attempts detected.
- Sign-in attempts originated from a hosting-provider IP in Miami, FL.
- Correct username and password were entered during the attempts.
- MFA prevented the attempted sign-ins from being completed.

3. ACTIONS TAKEN

- Password reset and all active sessions revoked.
- The originating IP was flagged for known threat activity.
- Sign-in activity was reviewed for additional suspicious access.
- MFA remained in place to protect the account from unauthorized access.

5. SECURITY LAYERS IN PLACE THAT PREVENTED THE ACCOUNT FROM BEING COMPROMISED

- Multi-Factor Authentication (MFA): Enabled and in use. MFA prevented the attempted sign-ins from being successfully completed despite the correct username and password being entered.
- Account Compromise Protection: Security software actively monitored the account, detected the suspicious authentication activity, and alerted our team so the incident could be investigated and contained.

6. CURRENT STATUS

The account has been secured, and the user's credentials have been reset. MFA successfully prevented the unauthorized sign-in attempts, and no successful unauthorized access was identified based on the activity reviewed.