City of Milwaukee

Department of Administration
Information and Technology
Management Division

Cavalier Johnson
Mayor

Preston D. Cole
Administration Director

David A. Henke
Chief Information Officer

MEMO

To: Members of the Finance & Personnel Committee
From: David Henke, Chief Information Officer
Date: September 16, 2025

Subject: Response to resolution # 250824, "Communication from the Information Technology Management Division relating to policies and procedures governing the quarantining of e-mail."

Initial Event

On the afternoon of July 31st, 2025, the offices of Ald. Dimitrijevic and Ald. Zamarripa separately reported to ITMD that constituent emails, from July 15th and July 25th (Ald. Dimitrijevic) and July 12th (Ald. Zamarripa), had not been received in their email inboxes. It was subsequently determined that these emails had been identified as a likely threat and placed in quarantine by Microsoft Defender for Office 365. Impacted officials raised concerns relating to the length of time this situation may have been occurring and additional information from ITMD was requested.

Background

Microsoft Outlook has several built-in tools to filter messages that it believes do not belong in the user's main inbox:

Clutter – Designed to filter low-priority email.
Junk Email – Designed to filter traditional spam - innocuous, unwanted emails.
Quarantine – Designed to hold potentially dangerous messages.

The quarantine feature is a built-in part of Microsoft Office 365, which the City of Milwaukee has used for email for approximately 15 years. The most basic email protections for mailboxes prevent broad, volume-based, known email attacks. It restricts and temporarily holds these messages from the domain email system for a default of 15 days before they expire in transit. If a missing email is reported within this timeframe, it can be manually released by an email administrator before it expires.

Additional protections from zero-day malware, phishing, and business email compromise (BEC) come with the use of Defender for Office 365. Microsoft Defender for Office 365 extends basic Exchange Online Protection (EOP) through various tools, including Safe Attachments, Safe Links, spoofed intelligence, spam filtering policies, and the Tenant Allow/Block List. In 2022, the City of Milwaukee began using Microsoft Defender for Office 365 as part of an implementation of the EMS365 security suite that Microsoft provided at no cost for one year as part of its "White House Offer" program. ITMD found the security tools provided with EMS365 to be an invaluable resource to maintaining

security for the Microsoft-based tools used by the City of Milwaukee and has continued to subscribe to this solution, implementing the features provided.

Initial Response (First two weeks)

1. Upon ITMD's receipt of notice of missing emails, all constituent emails still in quarantine were released. Based on the default 15-day expiry of emails, this included all emails from July 16, 2025 to the current date.
2. The next day, August 1st, daily quarantine notices were configured for Ald. Dimitrijevic.
3. On August 6th, a support ticket was opened with Microsoft to investigate if additional emails were being sent to quarantine in error. Additionally, Microsoft was asked about the ability to recover older messages from quarantine.
4. On August 7th, the ability to receive daily quarantine notices and instructions on how to use quarantine was offered to all alders through the City Clerk's office. To date, quarantine notices have been configured for 7 of 15 council members.
5. On August 11th, after escalating the issue, Microsoft responded to the support ticket with findings of the messages being identified as "Spam due to Machine Learning Model."
6. On August 13th, Microsoft indicated they had mitigated the specific issue with the emails provided on July 31st.
7. On August 15th, Microsoft responded that they were unable to recover expired quarantined emails. Additionally, they were unable to provide definitive dates for the "recent" phishing campaign changes that were the root cause of misidentifying the emails originally reported on July 31st. Further, they offered to investigate any future misidentified emails.
8. On August 17th, an additional constituent email was sent to quarantine. This was reported to Microsoft on August 18th and by August 20th, they had incorporated changes to filtering based on this report.

Initial Analysis

The top priorities of ITMD when becoming aware of legitimate messages being stuck in quarantine were to recover these messages and to implement practices to assure this did not happen again. By releasing the known quarantined messages and offering quarantine notices to council members, these objectives were in place within one week of the incident and to the best of ITMD's knowledge, no constituent messages sent after July 15th have been missed. Because some legitimate emails still went to quarantine after July 31st, this has only been possible due to the efforts of council members and their aides reviewing the quarantine.

The secondary objectives of ITMD were to understand what had taken place, why this occurred, and how to ameliorate any past disruption in constituent communications.

Microsoft indicated that quarantine messages that had expired left no record to review and that security restrictions prevented identifying the timeframe for how far back messages may have been lost associated with the "Spam due to Machine Learning Model" misidentification. ITMD knows of a limited number of examples of lost emails that were reported by constituents to their representative and that the representative forwarded to ITMD. While there are likely more lost emails that were not reported, ITMD is unable to say with certainty what emails may have been missed or how many emails may have been missed. However, there are several indicators that can help provide some educated estimates. Because this analysis took some time (and continues to be refined), these indicators are discussed under the "Further Analysis" section.

Further Response

Additional legitimate emails that were quarantined have continued to be identified by ITMD and forwarded from Ald. Dimitrijevic as they have occurred. These have continued to be forwarded to Microsoft for review and remediation. Microsoft continues to adjust its Machine Learning Model and release from quarantine any other emails that may have been affected.

ITMD has extended the default 15-day quarantine expiration to the maximum 30 days where possible. This will allow staff more time to review messages and senders to report a non-response before the flagged email expires.

ITMD, at the recommendation of Microsoft and based on recent events, has adjusted the email filters we control for advanced spam filtering that were established as recommended during a previous professional services engagement.

On September 3rd, ITMD requested a meeting with the Microsoft account team to review the situation and were told, "This matter falls outside the scope of the Account Team." The recommended course of action was to contact Microsoft support, which then responded, "Unfortunately our troubleshooting team does not have SME's [Subject Matter Experts] we can line up for a meeting to have granular discussions on issues." With this, ITMD and the City of Milwaukee were left with only technical support on the tactical issues being addressed.

On September 5th, ITMD published an eNotify message to approximately 30,000 email accounts subscribed citywide notification groups. This message was also later included in an eNotify message for Aldermanic District 14 at Ald. Dimitrijevic's request and ITMD's support to reach a broader audience.

Since this incident, ITMD has responded to a malware email that attempted to spoof a legitimate Microsoft quarantine message. While this was reported by a vigilant employee and remediated by ITMD without incident, it highlights the risk and difficulties in dealing with malicious actors attempting to compromise the system and deceive account holders in any way possible.

Since this incident, ITMD has monitored the use of quarantine and the release of both legitimate messages and those that do not appear to be legitimate messages. ITMD will continue to work with Microsoft to identify and resolve the issues that cause legitimate emails to be quarantined, as well with end users to educate them on when it is and is not appropriate to release emails from quarantine.

Further Analysis

To understand how far back missing emails may go and how current quarantine notification rules came into effect, ITMD reviewed the history of quarantine and notifications.

As noted in the background section, the City of Milwaukee has used Outlook 365 for approximately 15 years. The quarantine feature is believed to have been part of Outlook 365 for as long as the City of Milwaukee has used it. While no ITMD management staff were in their current roles at the time, it is assumed that the system was established with the recommended default settings at the time.

In March 2018, ITMD remediated a broad malware infection across the desktop computers of an entire department. This is believed to have been caused by the opening of a malicious email that rapidly spread among many desktop computers. The response took several days to reimage all infected computers and restore normal operations. As a result of this event, several security enhancements were implemented. A review of phishing protections and policies was likely performed to be more secure and restrictive. The policies in place in July 2025 regarding quarantine and quarantine notifications likely have a basis from those events.

Since 2018, there have been many changes to features, best practices, and user experiences. ITMD has engaged in a number of cybersecurity reviews with Microsoft, its partners, internal audits, and external audits from federal resources in advance of the DNC (2020) and RNC (2024) conventions. These have resulted in implementing new features and the hardening of systems based on those reviews. At no point in those reviews were changes to quarantine notifications recommended. Over the years, only sporadic reports of missing emails in quarantine were reported and ITMD worked with those users to recover emails and adjust rules to allow known senders to be trusted senders. At no time prior to July 31st was ITMD aware of any impacts to elected officials. This approach had worked successfully to the best of ITMD's knowledge up until July 31st.

The balance between cybersecurity and reliable communications had shifted. While Microsoft support provided limited answers due to security, ITMD was able to identify some key relevant events.

In a blog post on November 19, 2024, Microsoft announced "Microsoft Defender for Office 365 now uses purpose-built Large Language Models (LLM) at scale to provide AI-powered email and collaboration security." This was a promotional notice, with no warnings or recommendations to change any settings or monitor for issues. Nonetheless, because emails in July were identified as "Spam due to Machine Learning Model", ITMD believes this category of filtering would not have been possible before November 19th, 2024.

Researching further, in a blog post on May 19, 2025, Microsoft announced "Microsoft Defender for Office 365's new Language AI for Phish model" claiming 99.9998% accuracy in identifying malicious phishing messages. In a blog post on July 1, 2025, Microsoft announced "Microsoft Defender for Office 365 now features large language model (LLM)-powered responses within the submission workflow."

It is clear that Microsoft continues to make changes to its AI filtering tools. With this information, and with the understanding that elected officials and constituents are likely to report communications failures with the proper expectation of quick resolution, ITMD believes the most-likely cause of misidentified emails stems from changes made by Microsoft in July; possibly but not likely since May 19, 2025 if the 99.9998% accuracy is to be believed; and certainly no further back than November 19, 2025 when AI detection models were initially introduced.

Communications with elected officials present a unique challenge. Elected officials receive emails from a broad range of the general public on a broad range of topics and rely on these for timely communications. Simultaneously, due to their public visibility they are particularly targeted for phishing and malware via email. ITMD believes that when we can collaborate with elected officials to find the best balance of reliable and secure communications, the practices established will have a positive impact on all staff and email communications throughout the City of Milwaukee.

Next Steps

The Email Admins team continues to use Microsoft 365 Quarantine to manage email security and support end-user needs. Key use cases include:

- **Reviewing and purging reported phishing emails** to prevent malicious content from spreading internally.
- **Recovering legitimate emails** that were incorrectly flagged as spam, phishing, or bulk mail.
- **Investigating delivery issues** by checking quarantine logs and message traces to determine why an email was blocked or delayed.
- **Monitoring high-risk users** for targeted phishing attempts or business email compromise (BEC) threats.
- **When requested, reviewing quarantined messages** for compliance or legal review, especially in cases involving sensitive or regulated data.
- **Whitelisting or blocking senders/domains** based on quarantine trends and user reports to fine-tune anti-spam policies.

ITMD will continue to review the implementation of the quarantine system for potential improvements. ITMD also requests that email users continue to monitor their quarantine and submit any reports of emails that may not have been delivered to https://mkesdp.milwaukee.gov/. ITMD will submit these reports and quarantine monitoring results to Microsoft to enhance the reliable delivery of legitimate emails and the filtering of malicious emails to the highest standard practicable.