Carleton Email Spoofing Detection and DMARC Posture Assessment

Prepared by Mohamed Elsaban
Date: August 20, 2025

Executive Summary

While building a departmental form, I observed that the form could send email notifications with any Carleton address set as the visible sender. This meant a student or an outside actor could submit the form and make the message appear to come from any person or unit at the university. A domain check showed that the DMARC policy for the Carleton domain had p equal to none. A policy of p equal to none only asks for reports and does not block failed authentication. This combination created a high risk of executive or department impersonation and could be used to deliver convincing phishing or social engineering attempts. I reported the issue to my manager with a set of fixes and it was escalated for remediation.

Methodology

1. Reproduced the behavior in a test submission by setting the visible From field to a known Carleton address.
2. Inspected message headers to verify whether SPF and DKIM were passing or failing on the receiving side.
3. Queried the public DMARC record for the domain to confirm the policy value and reporting addresses.
4. Outlined practical detection steps, including SIEM queries that look for header anomalies and unusual sending patterns from web form infrastructure.

Findings

- The DMARC policy was set to p equal to none which requests aggregate reports but does not quarantine or reject messages that fail alignment.
- The form platform allowed the visible From address to be set to any Carleton address which made spoofing trivial through the form workflow.
- Monthly DMARC reports went to a shared mailbox which provides aggregate insight but not timely blocking or alerting on specific spoofing events.
- There was no enforcement of DKIM alignment for messages generated by the form, which weakened trust in the visible sender when viewed by recipients.

Recommendations

I proposed a set of changes that would materially reduce the risk and increase confidence in university mail.

- Move DMARC from p equal to none to p equal to quarantine for a short observation period and then to p equal to reject once alignment rates are confirmed.
- Ensure DKIM signing for mail sent by the form system using a trusted relay or a dedicated authenticated mailbox so that the envelope sender aligns with the visible sender or the domain policy.
- If a department name must be visible, use a reply to header for the department and keep the real sender as a centrally managed mailbox that is DKIM signed and aligned.
- Harden SPF so that only approved relays can send on behalf of the domain and remove stale includes.
- Create alerting on spikes in authentication failures and on unusual From values coming from form infrastructure.
- Publish a short guidance note for staff that explains how to verify the real sender and how to report suspected spoofing.

Outcome and Next Steps

I documented the issue with screenshots and header evidence, briefed my manager, and provided a step by step remediation plan. The issue was escalated to the appropriate team for action. I also shared sample SIEM queries and a simple dashboard concept so that security staff can watch authentication health in near real time. I remain available to assist with testing once the new DMARC policy and mail routing changes are in place.

Risk if Unaddressed

An attacker could send messages that appear to come from respected leaders or critical departments. This could cause credential theft, payment fraud, or reputational harm. Since a policy of p equal to none does not block spoofed messages, recipients might see messages that look authentic even when they are not.

Appendix: Practical Detection Ideas

- Search for messages that show a Carleton visible sender while the path clearly originates from web form or non standard infrastructure.
- Create a trend line of SPF or DKIM failures by sender domain and surface unusual spikes.
- Flag messages where the reply to address does not match the visible sender when sent by a form system.