**Incident:** “Weekly Operations Review” Gift Card Scam

**Date:** October 21, 2025

**Analyst:** Haytham Abouelfaid

**Organization:** Loudoun County Public Schools (LCPS)

**1. Incident Summary**

On October 21, 2025, I received an email sent to my LCPS Substitute Teacher account titled **“Weekly operations review.”**

The message appeared to come from Kevin Lewis, who claimed to want a “direct conversation” regarding a “surprise.”

Shortly after replying to confirm my contact information, I received a **text message from the number +1 (617) 212-9715**. The sender, identifying themselves again as Kevin Lewis, asked me to **purchase Sephora or Best Buy gift cards** for “selected employees as a surprise,” while requesting confidentiality.

I immediately recognized this pattern as a **Business Email Compromise (BEC) / gift card phishing scam**, commonly used to impersonate supervisors or executives. The incident was contained without financial loss or further exposure.

**2. Indicators of Phishing**

The following indicators confirmed that the message was fraudulent:

* The subject line included **[EXTERNAL]**, meaning the email originated outside the LCPS network.
* The sender’s address was [Weeklyoperationsreview@outlook.com](mailto:Weeklyoperationsreview@outlook.com), not an official LCPS domain (e.g., @lcps.org).
* The message contained vague and **unprofessional phrasing**, with grammar inconsistencies.
* The email and text message both used **urgency and secrecy**, urging me to act quickly and “keep it confidential.”
* The sender requested **gift card purchases**, a classic hallmark of BEC scams.
* The sender’s display name “Weekly operations review” was **generic** and inconsistent with normal LCPS naming conventions.

**3. Technical Analysis**

Using the extracted email header data and the MXToolbox Header Analyzer, the following details were observed:

* **Sender Domain:** outlook.com
* **Return-Path:** Weeklyoperationsreview@outlook.com
* **Sender IP:** 2a01:111:f403:d120:: (Microsoft Outlook outbound server)
* **Authentication Results:** SPF, DKIM, and DMARC all passed for Outlook.com — confirming it was sent from a real Outlook account, **not spoofed**, but misused by the attacker.
* **AuthAs:** Anonymous — confirms the email came from **outside LCPS’s trusted network.**
* **Header Subject:** [EXTERNAL] Tue, 21 Oct 2025 — inserted automatically by LCPS filtering system to warn recipients.

**Interpretation:**

The attacker used a **legitimate Outlook.com account** to impersonate a school official. Although authentication checks (SPF/DKIM/DMARC) passed, they only verified the email originated from Outlook servers — not that the sender was authorized to represent LCPS. This aligns with common **phishing through legitimate cloud email accounts** (Microsoft 365 / Outlook.com).

**4. Social Engineering Tactics**

The attacker used multiple psychological manipulation techniques:

|  |  |  |
| --- | --- | --- |
| **Tactic** | **Example** | **Purpose** |
| Authority | Pretending to be “Kevin Lewis,” a supervisor figure | To gain compliance and trust |
| Urgency | “Step out for a bit to take care of a task.” | To pressure quick action before verifying legitimacy |
| Confidentiality | “Would appreciate your confidentiality.” | To prevent verification or discussion with others |
| Financial Incentive | “Buy Sephora/Best Buy gift cards for employees.” | To trick the target into purchasing and sending codes |
| Familiarity | Used a professional tone and internal-sounding title “Weekly Operations Review.” | To appear like a legitimate internal message |

**5. Incident Response Actions**

Immediate containment and response steps taken:

1. **Did not purchase any gift cards or share personal data.**
2. Verified the sender’s legitimacy through domain and phone number — both invalid.
3. **Reported the phishing attempt** to the **LCPS IT Department** (phish@lcps.org).
4. Marked the email as phishing in Outlook to assist spam filter learning.
5. **Blocked the phone number** (+1 617-212-9715) on mobile device.
6. Saved all **evidence (screenshots, headers, message source)** for this analysis.

These actions align with NIST SP 800-61 guidelines for the “Detection and Analysis” and “Containment” phases of an incident response lifecycle.

**6. Lessons Learned**

* Always **verify the sender’s domain** and identity before responding, especially when requests involve money or urgency.
* Even if SPF/DKIM/DMARC pass, **authentication ≠ legitimacy** — always check context and content.
* Never respond to **financial or confidential requests** from unknown or external domains.
* This event reinforced the importance of **employee security awareness** training to prevent social engineering and BEC scams.
* Implementing **domain whitelisting** and enhanced **phishing simulation training** can reduce risk across the organization.

**Summary Conclusion**

This phishing attempt demonstrates a **real-world Business Email Compromise scenario**. The attacker used a free Outlook.com account to impersonate a supervisor, leveraging social engineering to request financial actions under the guise of confidentiality.

By promptly identifying, reporting, and analyzing the attack, the threat was neutralized without escalation — highlighting the importance of vigilance, verification, and incident response readiness in IT and cybersecurity operations.