

K–12 Phishing and Impersonation Response

A district playbook for the first report through recovery

Use a trusted communication channel, preserve evidence, and treat the account, message campaign, and business process as related but distinct response workstreams.

1. Confirm and triage

- ☐ Record reporter, time, sender, recipient, subject, message ID, links, files, and actions taken.
- ☐ Verify payment, payroll, password, or leadership requests through a known channel.
- ☐ Classify: suspicious message, malicious message, credential entry, execution, account compromise, or financial transaction.

2. Contain

- ☐ Suspend or reset compromised access under district procedure.
- ☐ Revoke active sessions, app passwords, and unauthorized OAuth tokens.
- ☐ Inspect forwarding, filters, delegation, recovery methods, and mail sent by the account.
- ☐ Find related recipients and messages; preserve identifiers before removal.
- ☐ Contact finance and the bank immediately if money may be moving.

3. Investigate

- ☐ Build a timestamped delivery, report, click, sign-in, account-change, and containment timeline.
- ☐ Review authentication, sender identity, reply domains, URLs, redirects, QR codes, and files.
- ☐ Record provider actions, who authorized them, and whether each succeeded.

4. Communicate

- ☐ Tell affected people the exact message, time, action to avoid, and trusted reporting channel.
- ☐ Do not repeat a live malicious link or ask users to forward a dangerous attachment.
- ☐ Coordinate family, staff, legal, insurance, law-enforcement, and regulatory communication through policy.

5. Recover and review

- ☐ Restore access from a known-safe device with strong MFA and approved applications only.
- ☐ Validate payroll, vendor, finance, and recovery information through trusted contacts.
- ☐ Assign an owner and due date to every detection, process, training, and response improvement.