Malicious Email Playbook

When a suspected Phishing Campaign is underway, there are a number of communication and technical actions that need to take place which is triggered by the recognition of an employee reporting a suspicious email. Once reported, verifying of the suspected email needs to take place to determine whether the situation is a false report or a confirmed malicious campaign.

These steps should be followed in the order as much as possible to ensure a thorough investigation.

Upon report:
-Copy link to a new phishing Ticket so it is not lost or retracted within the mail system later on
-Copy the Subject Line to the same ticket
-Copy sender and recipient information
-Continue to document findings along the way

Confirm or dismiss the report:
This can be done in a number of ways but the simplest way is to investigate the link to a non-production workstation that is not on a school network such as a hot spot or public wifi. Another method is to use the Windows sandbox to open the link in a sandboxed environment.

If the link appears safe, inform the user they are cleared to proceed. (End investigation)

If the link has suspicious redirects, false login pages, initiates unwanted downloads, is flagged by the browser etc., this is likely a malicious email campaign. (Continue investigation) Even a campaign that is not asking for credentials could be malicious as the attacker is hoping for users to click. Credential phishing campaigns are still the most common.

Email Partner Districts' Technology Directors about the situation
Include:
- Subject line of malicious email
- Sender(s) email address of malicious email
- Time/Date of malicious email
- Request district to block the malicious URL(s) in firewall as this protects shared staff in their districts
- Intention of malicious email if known
- Let them know when you will follow up with an update

Email All Staff about the situation
Include:
- Let staff know the Technology Department is aware of the situation. This will reduce countless emails telling you about the email and make searches less cluttered later on.
- Subject line of malicious email
- Warn against clicking the link

- Stress importance of not entering Google Credentials anywhere other than the official Google sign-in page where the URL is starting with accounts.google.com (Found by hovering over link)
- Ask users to self-report if they clicked the malicious link or entered credentials and not continue to use their computer or do any self-password resets
- Let staff know when you will follow up with an update

Communicate to the sender domain
Include:
- Inform the organization that as a courtesy, information about a malicious email sent from their domain is being included
- Subject line of malicious email
- Sender(s) email address of malicious email
- Recipient in your district that received the malicious email
- Time/Date of malicious email

Prepare for the following scenarios
- Incoming emails/phone calls to perform password resets
- If users are reporting their credentials were entered, their account should be immediately locked until further review and remediation of the domain is completed.
- All affected accounts should be added to the Ticket.
- All password resets should come from the Technology Department and be performed on a "clean" machine. The reason for not allowing password resets is that if the machine is infected by a malicious link, the machine could be compromised until it is checked and looked over by a technician.

Block future emails from that sender
In effort to reduce repetitive retractions of emails, blocking of the suspected email should be done first. This can be found in the following location of admin.google.com: *Apps > Google Workspace > Gmail > Spam, phishing, and malware*. Select the relevant OU. In most cases, you will want to apply this at the root level. Under the category “Blocked senders,” select Add Another Rule. The first field is for a Short Description. Always name this “Phishing - [Date].” Keeping this rule separate from existing rules will avoid confusion and allow tweaking of controls without impacting previous rule sets. Under section 1, choose “Create or edit list” and uncheck “Bypass this setting for messages received…” Select “Add Blocked List.” Name the address list “Phishing [Date],” add the sender email in the address list and click “Add Address.” Click Save.

In this list, prepare to add any outside accounts that are observed sending phishing emails as well. Set a calendar reminder for 1 day to revisit removing them from the list and inform the other district Technology Department you have blocked their user temporarily. Wait for confirmation from the Technology Director before allowing the user to be unblocked.

Block all similar messages or recirculating messages
It is now important to block messages that may be coming with the same subject line but from other users/districts. From admin.google.com, navigate to *Apps* > *Google Workspace* > *Gmail and choose the category "Compliance."* Find the category "Content compliance" and select "Add Another Rule" Name the rule to phishing [date]. Under section 1, select all four checkboxes. Under section 2, click "Add" and change the drop down from "Simple content match" to "Advanced content match." Change "Location" drop down to "Subject" and "Match type" to "Equals." Under content, enter the subject exactly as it appears without putting the phrase in quotations. Under section 3, change the "Modify message" drop down to "Quarantine message." Click Save.

For additional measures, under section 2, "Advanced content match" could be modified by changing "Location" drop down to "Raw Message" and "Match type" to "Contains text." Under content, enter the URL to a malicious website without putting the phrase in quotations.

Retract emails from inboxes
It is now important to retract emails sitting in inboxes as users are still at a risk of clicking the emails and links.

Within admin.google.com, navigate to *Security* > *Overview and select the category "Investigation tool."* From the "Data source" drop down, select "Gmail messages" and click the "Add Condition" link and from the "Attribute" drop down, select "Subject" and in the "Subject" field, type the subject line copied from the investigation document and click "search"

Do not attempt to delete messages based on Message ID as each subsequent user impacted will send out an email using a new message ID. This page will display all the recipients matching your search. Select the checkbox next to the work "Subject" and choose "Select results on all pages." Select "Action" and click "Delete messages." Follow the prompts on the next screen to confirm deletion.

The subject line should be searched in this section every 15 minutes to ensure rules are being enforced properly for at least an hour.

Block the URL(s) in Chrome Managed Browser
This will block managed Chrome sessions from accessing the URL, but not unauthenticated sessions or other browsers.

Within admin.google.com, navigate to *Devices* > *Chrome* > *Settings*. From there, the categories under "User & browser settings" should be displayed. Find "Content" and the item "URL Blocking." Click that item and then select your OU. In most cases, this will be the root OU. Under Configuration > Blocked URLs, you will see the current list of blocked URLs. Add the malicious URL from the investigation document to this existing list.

Block the URL(s) at the Firewall
Depending on your firewall, the ability to block full addresses may be limited. For instance, the site, bad.site.com/sinwidnw/eininef$#.somwd, the firewall may require bad.site.com to be entered. Ensure the domain being entered is not being used by the district as this will block all URL paths for that domain.

This will block all users from navigating to that site while on the school network.

GAM view/remove rules
(If you do not use GAM, another method can be used found under the Release the user account/Verify settings section found below)

Filter rules - Used by attackers to manipulate incoming emails and direct messages as desired
View user's filters rules:

gam user user@domain.org show filter

Delete user's filter rules if suspicious filters are detected.
This will remove the user's specified filter rule:

gam user user@domain.org delete filters ANe1BmXXXXXXXXXXXXXXXXXX

Forwarding rules - Used by attacker to keep persistent access to incoming emails
View user's forwarding rules:

gam user user@domain.org print forward

Delete user's forwarding rules if suspicious rules are detected.
This will remove the user's forwarding rule to another email account:

gam user user@domain.org delete forwardingaddress attacker@gmail.com

Delegates - This should be checked to ensure a malicious actor does not have access as a user's delegate going forward:
View user's delegates:

gam user user@domain.org show delegates

Delete user's delegates if suspicious delegates are detected.
This will remove the user if their inbox was delegated to another user:

gam user maliciousdelegate@domain.org delete delegate user@domain.org

Reset Sign-in Cookies
Under the *User Accounts* > *Security* > *Sign in cookies*. From there, select Sign-in cookies and select "Reset"
This will sign the user out of all accounts within devices and browsers.

Revoke Connected applications and devices
Under the *User Accounts* > *Security* > *Connected applications and devices*. From there, select the Connected applications and devices and hit the trash can to remove the access for each app. Take note of any suspicious apps and add those to the investigation.

This will force all apps to request permissions from Google once the affected user attempts to sign into applications again through OAuth.

If a malicious application is identified, the app can be globally blocked by navigating to *Security > Access and data control > API controls > Manage App Access*. From there, select View list under "Accessed apps" and "Configured apps." Search for the malicious app, select it and select "Access to Google data." From there, select "Blocked."
This will prevent all users in your domain from granting access to this malicious app in the future.

Review Logs
Google logs - To conclude the investigation, there must be a log review to see if the malicious actor successfully logged in with users' credentials. At this point, the user that was sending out emails should still be disabled. To review logs in admin.google.com, navigate to *Reporting > Audits and Investigations > User log events*. By default, the Date is set to look at the last week. This is fine as the logs are also categorized by newest entries at the top. Click "Add Condition" and change "Attribute" to "User" and change "Contains" to "Is." In the "User" field, type the full email address of the impacted user. Click "Search" The first thing to look for is IP addresses on the far right that are out of the ordinary. (136.228.X.X is the ISD/LEA network) Most users have a home IP that is also common to see. If suspicious IP addresses need to be investigated further, click the three dots that appear next to the IP and pivot to items that an attacker may be interested in; Drive log events, OAuth log events, Takeout log events etc. If this is an Admin account, ensure Admin log events are investigated.

Depending on preference, this process can also be accomplished by going to the user's profile and selecting "Investigate" at the top. "View Logs" appears next to each category on the right-hand side.

Review accounts recovery information by also going to the user's profile and selecting "Security" and take note of recovery information and add to Incident Ticket. Most users do not utilize this but a malicious person could enter their information here to re-acquire access after a password reset. Clear all information.

Release the user account/Verify settings
Connect with the affected user and look for malicious applications/extensions on their workstation. (if credentials were entered on the workstation) Re-enable their Google account. Verbally provide a new password and enforce a change. Verify Gmail filters and email forwarding to ensure there are no malicious entries added to the account. These can be found in Gmail by clicking the Gear icon in the top right corner selecting "see all settings" and selecting "Filters and Blocked Addresses" Clear suspicious filters. When completed, click "forwarding and POP/IMAP" and clear any suspicious forwarding rules.

Final Communication

After the situation appears to be under control, with emails removed from inboxes and future emails with that subject line prevented, inform the district technology directions and all staff that the situation appears to be under control. In the email to staff, remind staff that questionable emails can always be forwarded to the Technology Department for analysis before clicking. Report users who did not follow best practice to their supervisor. Share all relevant incident details with Technology Directors.

CHECKLIST
Google Workspace Investigation

(Some items may require the Education Plus plan)

Documentation

- ☐ Start documenting necessary information
- ☐ Verify malicious links in sandbox
- ☐ Confirm report of malicious email
- ☐ Record Metadata/date/time
- ☐ Communicate to partner organizations about the situation
- ☐ Communicate to your own organization about the situation
- ☐ Communicate to the domain owner informing them a malicious email was sent from the domain

Containment

- ☐ Block future emails from sender
- ☐ Disable users who are sending out malicious emails
- ☐ Change passwords of users who are sending out compromised accounts
- ☐ Verify there are no suspicious filer rules
- ☐ Verify there are no suspicious forwarding rules
- ☐ Verify there are no suspicious delegates
- ☐ Block messages containing same subject line
- ☐ Block messages containing malicious URL
- ☐ Retract emails from inboxes
- ☐ Block URL(s) in managed Chrome Browser
- ☐ Block URL(s) at Firewall
- ☐ Block URL(s) at any webfiltering solutions

Investigate

Review Logs in Google Workspace under the User's profile and under the tab Investigate

- ☐ Files shared externally

- [ ] External content copied
- [ ] Files downloaded
- [ ] Suspicious sign-ins
- [ ] Suspicious activity by user detected
- [ ] Admin log events
- [ ] Chrome log events
- [ ] Context Aware Access log events
- [ ] Contacts log events
- [ ] Device log events
- [ ] Drive log events
- [ ] Gmail log events
- [ ] Groups log events
- [ ] OAuth log events
- [ ] SAML log events
- [ ] Takeout log events
- [ ] User log events

Conclusion

- [ ] Summarize Incident
- [ ] Evaluate response
- [ ] Test/Implement necessary changes
- [ ] Close Incident