Contents

Helpful Resources ............................................................................................................................................. 2
List of IPs and custom domains used with Red Herring ................................................................. 2
Configuration ........................................................................................................................................................ 3
COE Admins ....................................................................................................................................................... 3
LEA Admins ....................................................................................................................................................... 3
Settings ............................................................................................................................................................. 4
  Profile ............................................................................................................................................................ 4
Google Gmail Allowlist & Gateway .............................................................................................................. 5
Sender Policy Framework (SPF) - Optional ................................................................................................... 7
Google Service Account .............................................................................................................................. 7
  Enable Admin SDK for Service Account in Google Cloud Console .......................................................... 12
  Grant Access for Service Account in Google Admin ................................................................................... 12
  Trust Red Herring as an OAuth App ............................................................................................................ 13
  Upload JSON and Sync Target Users into Red Herring ........................................................................... 14
Create Red Herring User Group .............................................................................................................. 15
Create Red Herring Template Categories ................................................................................................... 15
Clone a Red Herring User Email Template .............................................................................................. 15
Send a Test Phishing Campaign .................................................................................................................. 16
Helpful Resources

The public SDCOE Cybersecurity webpage has multiple helpful resources that can be found at HTTP://cybersecurity.sdcoe.net


In-page help is also provided and can be accessed by navigating to the page where you need help and clicking the question mark icon at the bottom right of page. The inline help page will close when you browse away from the current page. The inline window can be expanded to its own browser tab to keep it for further reference.

List of IPs and custom domains used with Red Herring

These IP addresses and domains may need to be allow-listed on your email protection service to prevent them from being flagged as phishing or moved to the target user’s quarantine inbox.

192.40.172.4, 192.40.172.139, 20.118.176.15, 20.118.176.58

<table>
<thead>
<tr>
<th>Generic Domains</th>
<th>Regional Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>aditisecurity.com</td>
<td>countyofsd.net</td>
</tr>
<tr>
<td>cstateachers.net</td>
<td>sandiegocoe.net</td>
</tr>
<tr>
<td>highunion.net</td>
<td>sdc0e.net</td>
</tr>
<tr>
<td>schoolunified.net</td>
<td>sdc0es.net</td>
</tr>
<tr>
<td>servicecounty.net</td>
<td>sdcounty.net</td>
</tr>
<tr>
<td>uniondistrict.net</td>
<td></td>
</tr>
</tbody>
</table>
Configuration

**COE Admins**

COE or super admins are able to access the Red Herring portal and perform admin activities at the COE level; such as creating and editing Agency (LEAs), adding and editing COE/LEA admins, and viewing COE reports. An email address is only allowed to be assigned to one COE and additionally to one LEA.

COE admins will first have to create an LEA for their organization so that they can send phishing campaigns to their staff. After adding a COE admin to an LEA they'll have to re-login to see the change.

1. Navigate to Agencies (LEAs)
2. Click +Create Agency
3. Fill in the LEA information
   a. Only assign the necessary amount of licenses to the LEA
   b. Expiration date can't be set pass your COE's expiration date
4. Click Create
5. Click the Admins button next to agency and assign admins to it (see LEA Admins)

**LEA Admins**

Agency admins are able to access the Red Herring portal and perform actions according to their admin level. An email address is only allowed to be assigned to one LEA. After adding a COE admin to an LEA they'll have to re-login to see the change.

We currently have three LEA admin levels

- **Admin** - full admin and can add/modify other admins
- **Template Admin** - can create and edit templates for Emails, Landing Pages, and Knowledge Assessments
- **Campaign Admin** - can schedule and modify simulated phishing campaigns, as well as view the campaign results

**Note:** When you create an admin they are sent a welcome email along with a link to set their password. If they do not set their password within 24 hours you will have to click the Confirm Email button to send them another email request to set their password.

- **Create Admin** - This will assign an admin to the Agency (LEA)
- **Reset Password** - This will send the admin an email requesting that they reset their password
- **Confirm Email** - This button shows if the admin has not yet clicked on the link in their Welcome Email to set their password, clicking it will send them a new welcome email
**Settings**

The Settings page has three sections; Profile, Notifications and Excluded Times.

**Profile**

This is where you can input your organization’s information and logos so that they will automatically appear on any of Red Herring’s LEA Branded templates. Simply enter your agency’s details and click save. You may use the attribute variable on any template that you create or modify.

The available text fields are:

<table>
<thead>
<tr>
<th>Name</th>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Name</td>
<td>{orgname}</td>
<td></td>
</tr>
<tr>
<td>Organization Website</td>
<td>{orgwebsite}</td>
<td></td>
</tr>
<tr>
<td>Organization Acronym</td>
<td>{orgacronym}</td>
<td></td>
</tr>
<tr>
<td>Help Desk Name</td>
<td>{helpdeskname}</td>
<td></td>
</tr>
<tr>
<td>Help Desk Website</td>
<td>{helpdeskwebsite}</td>
<td></td>
</tr>
<tr>
<td>Help Desk Phone Number</td>
<td>{helpdeskphone}</td>
<td>Only numbers are allowed</td>
</tr>
<tr>
<td>Help Desk Email</td>
<td>{helpdeskemail}</td>
<td></td>
</tr>
</tbody>
</table>

The available logo/images are:

<table>
<thead>
<tr>
<th>Name</th>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rectangular Logo</td>
<td>{rectangularlogo}</td>
<td></td>
</tr>
<tr>
<td>Square Logo</td>
<td>{rectangularlogo}</td>
<td></td>
</tr>
<tr>
<td>Text logo</td>
<td>{textlogo}</td>
<td></td>
</tr>
<tr>
<td>Preferred Background Image</td>
<td>{backgroundimage}</td>
<td>Will not display as background image in emails</td>
</tr>
</tbody>
</table>
Google Gmail Allowlist & Gateway

These directions will set up an allowlist and Email Gateway for Gmail to ignore simulated phishing emails from Red Herring.

In Google Admin go to Apps > G-Suite > Settings for Gmail > Spam, phishing, and malware

https://admin.google.com/ac/apps/gmail/spam

1. From the main menu first expand the Apps menu
2. In the Apps section expand Google Workspace and then select Gmail

3. Scroll to the bottom of Settings for Gmail and select Spam, phishing, and malware
4. Under Email allowlist enter the following IP addresses separated by commas:

192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.15

5. Next find Inbound gateway and select Configure or EDIT

6. In the Inbound gateway settings
   a. Enter a short description: Red Herring email gateway
   b. Add the following gateway IPs
      192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.15
   c. Check Automatically detect external IP
   d. Check Require TLS for connections from the email gateways listed above
   e. Check Message is considered spam if the following header regexp matches
      i. Enter a false statement that won’t trigger: X-Spam: this is spam
      ii. Choose the radial for Message is spam if regexp matches
      iii. Check Disable Gmail spam evaluation...

Click Save or Add Setting

7. Return to Red Herring > Configuration > SMTP and enter aspmx.1.google.com for server name, 25 for port number, check SSL box, and leave username and password blank. Then click update and check your Gmail Inbox for an email from noreply@sdcoe.net.
**Sender Policy Framework (SPF) - Optional**

Sender Policy Framework (SPF) is a crucial email authentication protocol that helps prevent email spoofing and enhances email deliverability. These directions are only needed if you plan to use Red Herring to impersonate your organization’s email domain.

Add the following IP statements before the “all” statement of your SPF record on your DNS nameserver.

ip4:20.118.176.15 ip4:20.118.176.58

After you update your SPF records, we recommend that you send yourself a test phishing email that spoofs your domain. If you have successfully added Red Herring to your SPF record, the email should not go to your Spam folder or be flagged as malicious.

**Google Service Account**

These directions will set up a Service Account in Google Cloud and Google Admin to allow you to import target users into Red Herring.

1. Go to [https://cloud.google.com/](https://cloud.google.com/) and login with your Google Admin Account
2. Click Console to go to the Console Page
3. Select APIs and Services
4. On the top panel click **Select a project**
5. Create a **New Project**
6. Choose your Organization and Location

The project could take a while to complete. When the project is ready, it should be listed under your organization.

7. Select the project then click the Credentials menu on the left

8. In the Credentials page, click “Create Credential” and select Service account

9. Input Service Account Information and click Create and Continue then accept the defaults and select Done
11. After creating the service account, copy the Unique ID from Details tab of the Service Account page
   a. Google Cloud > Service Accounts > IAM &Admin > Service Accounts > {Red Herring Service Account}

![Service account details]

12. Go to the Keys tab of Service Account page and select Add Key

![Add Key button]
13. For key type choose “JSON”

14. After successfully creating, the JSON key will automatically download to your computer

15. (Please keep the JSON safe because you won’t be able to download it again)
Enable Admin SDK for Service Account in Google Cloud Console

1. Go to https://console.cloud.google.com/ and login with your Google Admin Account
2. Select APIs and Services > Library
3. On the top panel make sure your sync project is selected from top-left dropdown.
4. Search for Admin SDK API and click on its tile
5. Enable the Admin SDK API

Grant Access for Service Account in Google Admin

1. Go to Google Admin (https://admin.google.com) and login with Google Admin Account
2. Go to Security > Access and data control > API controls
3. Click Manage Domain Wide Delegation
4. Click **Add new** to add new scope for your service account key
5. Input the service account Unique ID (In Service Account Detail page) and the 4 scopes would be:
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.group
   - https://www.googleapis.com/auth/admin.reports.audit.readonly
   - https://www.googleapis.com/auth/admin.reports.usage.readonly

6. Then click **Authorize**

### Trust Red Herring as an OAuth App

1. Go to Google Admin ([https://admin.google.com](https://admin.google.com)) and login with Google Admin Account
2. Go to Security > Access and data control > API controls
3. Click **Manage Third-Party App Access**
4. Open the **Add app** drop-down menu
5. Select **OAuth App Name Or Client ID**
6. Search for: 918725752096-bsbsa9v8kl50op3525s5bl21v2aj8061.apps.googleusercontent.com
7. Hover over RedHerring and press **Select**
8. Check the box next to OAuth Client ID and press the **Select** button
9. Select All Users and press **Continue**
10. Select the **Trusted** radial button and press **Continue**
11. Review the settings and press **Finish**
12. Wait 5-10 minutes for the changes to propagate and proceed with next step
   (Log out of the Red Herring console)
Upload JSON and Sync Target Users into Red Herring

1. Navigate to Red Herring > Configuration > Directory
2. Select +Add new and login to G-Suite with an Admin account
3. Allow sdcoe.net access to sync your users

   ![Google Account Access](image)

4. On the G-Suite sync tile select **Configure Auto Sync**
5. Slide the toggle switch for Auto Sync and choose your sync frequency
6. Upload the .json file and **Save**

   ![Configure Auto Sync](image)

7. On the G-Suite sync tile select **Sync**
8. Choose the groups that you want to sync and press **Sync**

   ![Choose groups to sync](image)
Create Red Herring User Group

Red Herring has 5 groups that are automatically populated with your target users based on their Risk Score. You may use any or all of these groups in your simulated phishing campaigns. We recommend that you create a group for testing purposes to ensure the templates are formatted correctly and that spam prevention is bypassed.

1. Navigate to Red Herring > Groups
2. Select +Create Group
3. Name the group Testing
4. Optionally create another group for All Staff

Create Red Herring Template Categories

Next we will create a folder to house the templates that we clone, modify or create. For the purposes of this guide we will name them Testing, you may choose a different name or rename them at any time. You may skip this step if you have already created a category for each content type.

1. Navigate to Red Herring > Emails > +New Category
2. Name it Testing and click Ok
3. Navigate to Red Herring > Landing Pages > +New Category
4. Name it Testing and click Ok
5. Navigate to Red Herring > Knowledge Assessments > +New Category
6. Name it Testing and click Ok

Clone a Red Herring User Email Template

1. Navigate to Red Herring
2. Search for Google in the top-right search bar
3. Navigate to Red Herring > Emails > +Shared with Me
4. In the Filters box click Deselect all and then check the box for Email Templates
5. Find a template that you like and clone it to your Testing folder (an example of email to landing page click-path is below)
6. Optionally you check the box for Landing Page Templates and clone them so that you may customize them.
   a. You will have to edit the link to the email template if you decide to clone and customize a landing page.
Send a Test Phishing Campaign

We suggest that you use the Send Email menu item for testing your email templates to ensure that spam prevention measures are bypassed, email and landing pages display nicely, and that telemetry works. For telemetry we track email clicks, landing page views, data entered in login fields, video views, and knowledge assessment results. Deleting the email campaign from the Emails Sent menu item will remove your negative Risk Score for clicking on that email campaign.

We suggest that you use the Campaigns menu when sending simulated phishing campaigns to your staff. All the Google email templates are configured to point to a cloned Google Login page, if they enter their login credentials and click the Login button they will be redirected to an LEA Branded user awareness page to help them better identify phishing emails and websites. Your logo and organization will automatically appear on the user awareness page if you have configured the items in Configuration > Settings page.

1. Navigate to Red Herring > Send Email
   a. For User Groups select your Testing group
   b. Choose one of the custom domains such as cstateachers.net
   c. For Email Template Category select your Testing category
d. Finally select the email to send and click Send

![Send Email](image)

2. Find the email in your inbox
   a. Click on any links in email and landing page
   b. Fill out any form fields
   c. View video if present
   d. Complete Knowledge Assessment if present

3. Click on View Report or Emails Sent and then view the Campaign Report for the email you just sent

![Your Emails Have Been Sent](image)

4. Verify telemetry shows in the email campaign report

![Email Sent and Security Alert](image)

5. Delete the Email once test is completed
6. Schedule a department/division/all-staff campaign by navigating to Campaigns > Create New Campaign
a. Here is an example of a quarterly campaign that will randomly send a different email once every quarter

7. Contact securinginfo@sdcoe.net if assistance is needed.