

# Red Herring FAQs

*Version 2.0 | Updated 2/22/22*

<b>Project Rollout</b> .....	<b>1</b>
Onboarding.....	1
Setup .....	1
<b>Red Herring Functionality</b> .....	<b>2</b>
Accounts/Provisioning .....	2
Simulated Phishing Emails.....	2
User Awareness Training .....	2
<b>Support</b> .....	<b>3</b>
Contact.....	3
Policy.....	3

This document is available at <https://www.sdcoe.net/ITS/cybersecurity-services/Pages/default.aspx>

## Project Rollout

---

### **Onboarding**

**Q: Will Red Herring work in my IT environment?**

A: Yes. Red Herring is hosted at the SDCOE Data Center and you will only need to import your users in order to start sending them simulated phishing emails.

**Q: I am a county office of education and would like to provide Red Herring to my school districts. What are my next steps?**

A: County offices of education (COEs) will have the functionality to set up sub-accounts for school districts and/or schools and allow them a specific number of users. Once a sub-account is created, that account would be able to create an administrative user for the COE to provide a look at the district's internal phishing metrics.

**Q: What do you need from me so that we can use Red Herring at my COE or school district?**

A: SDCOE will need a memorandum of understanding from your COE or district superintendent, and staff from your IT leadership team would need to meet with us. There may be an annual subscription fee required. Please contact the SDCOE Cybersecurity team for further info.

### **Setup**

**Q: Will I be able to import all my users into Red Herring so that I can send them simulated phishing emails?**

A: Yes. Red Herring is able to pull users from a .CSV formatted file, MS Active Directory, MS Azure, and Google G-Suite. Administrative-level permissions would have to be provided to allow the data to be uploaded to Red Herring.

## Red Herring Functionality

---

### *Accounts/Provisioning*

**Q: Will I be able to group users together and send emails to each group?**

A: Yes. In Red Herring, you'll have to place target users in groups and send the simulated phishing email to a group or multiple groups.

### *Simulated Phishing Emails*

**Q: How many users can I send simulated phishing emails to at a time?**

A: You may send a phishing message to all of your users at once. It's a good idea to manage your phishing campaigns in small batches to easier digest the metrics provided on the Campaigns Page.

**Q: How will I know which of my users clicked on a link in a phishing email and what users entered personal info on a phishing page?**

A: Red Herring has a metrics page that shows you what users followed the phishing links. In our next release, we'll show who entered text into a phishing page and who watched the user awareness video.

**Q: Will all of the links in my simulated phishing emails point to redherring.sdcoe.net?**

A: Yes. For the time being, but we have purchased various other domains and you will soon be able to choose from them in the future.

**Q: Who will I be able to send simulated phishing emails to?**

A: Red Herring allows you to send emails to all users under your domain. You may not send phishing emails outside your domain.

### *User Awareness Training*

**Q: How do I use Red Herring to train users to know how to spot a phishing email?**

A: We recommend you identify on the landing page what made your Red Herring phishing email suspicious, have the user watch a cyber awareness video, and optionally take a short quiz in Red Herring.

## Support

---

### **Contact**

**Q: Who do I go to for problems in Red Herring?**

A: Please contact the [SDCOE Cybersecurity](#) team at [securinginfo@sdcoe.net](mailto:securinginfo@sdcoe.net)

Districts and COEs have a designated representative that is authorized to submit trouble tickets using this Service Now Link <https://sdcoe.service-now.com>.

### **Policy**

**Q: Can simulated phishing emails be sent out from a spoofed address?**

A: Yes. We ask that you take care in choosing the spoofed email address that you use in your email template to not reference a real email address or domain name because if the user replies to the phished email it will be sent to the real user. Please misspell part of the email address or use a domain name that is not registered.