

Binding Multiple Awareness Scenarios to particular Attack Scenarios

In the latest Lucy builds one has the possibility to choose which Awareness scenarios are mapped to particular Attack scenario. Imagine you're currently running a campaign that includes four attack scenarios aiming to test users capability to recognize and avoid various phishing attack types (e.g. data entry, hyperlink attack, or file download).

 <p>Data Entry Attack Data entry attack can include one or more web pages that intercept the input of sensitive information. The available web pages can be easily customized with a Your Software Name web editor. Additional editing tools allow you to quickly set up functions such as log-in forms, download areas, etc. without HTML knowledge.</p>	 <p>Hyperlink Attack A hyperlink-based attack will send users an e-mail that contains a randomized tracking URL to identify the user who clicked the link. There is no landing page involved in this campaign type. But you can redirect the user to any webpage after he clicked the link.</p>
 <p>File Attack File-based attacks allow the Your Software Name administrator to integrate different file types (office documents with macros, PDFs, executables, MP3s, etc.) into mail attachments or websites generated on Your Software Name and to measure their download or execution rate.</p>	 <p>Portable Media Attack Your Software Name offers the option to perform portable media attacks where a file template (e.g., executable, archive, office document with macros, etc.) can be stored on a portable media device such as USB, SD card, or CD. The activation (execution) of these individual files can be tracked in Your Software Name.</p>

In such a case it makes sense to send awareness to users accordingly to the attacks that they failed to recognize. For example, user did not click on a malicious link and avoided entering any data in some attack scenarios but fell into downloading malware simulation file that disguised as an internal document and appeared as an attachment to the fake newsletter. User's result implies that he or she is aware of possible hyperlink attacks but doesn't know how to recognize a file-attack. Thus, there is no need to provide a user with a complete A-Z course on avoiding phishing that will take an hour of his busy schedule. But it makes sense to send him a short awareness describing precisely what a file-attack is and how to detect it. And here comes Awareness scenarios binding.

How to bind attack scenarios

Within the campaign proceed to **Awareness Settings** and choose the scenario to edit. Then proceed to **Bound Attack Scenarios** tab and choose the attack scenario from the **Bind Attack Scenario** drop-down menu. Click on the **Bind** button and the scenario will appear on the list.

First Awaren...

Campaign Status: Not Started

Base Settings
Website
SSL Settings
Message
Mail Settings
Bound Attack Scenarios

Bind Attack Scenario

Hyperlink attack Bind

Search...

Scenario	Template	Type	Risk Level
Data Entry Attack	Access to online surveillance portal / English	Web Based	0

< 1 > 10

Thus users will receive awareness training according to the attack scenario they fail.

Bind ?

Attack victims will get awareness connected with the attack scenario.

On the **Awareness Settings** tab, one can review which attack scenarios are bound to awareness.

multiple aw...

Campaign Status: Not Started

Export + New Awareness

Results

Search...

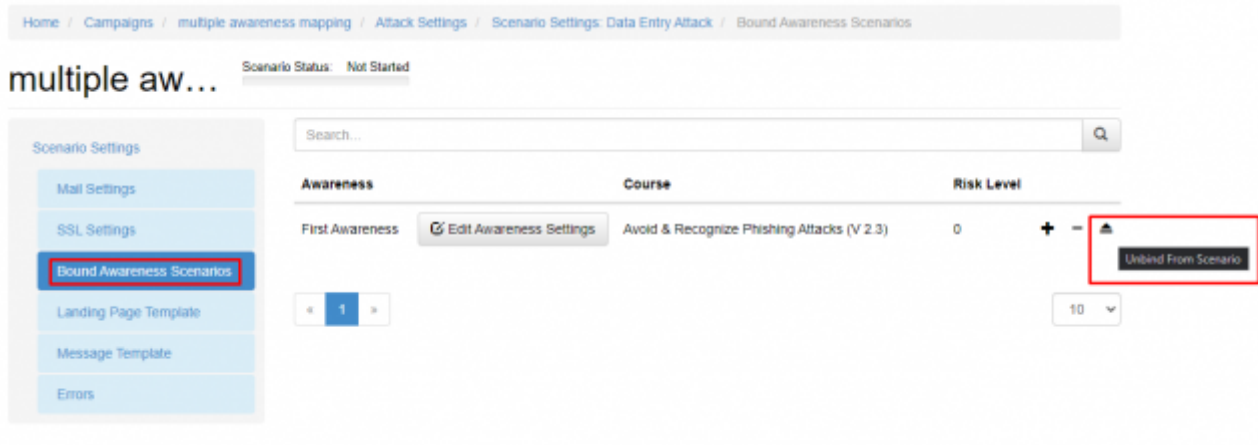
Awareness	Course	Bound Attack Scenarios	Risk Level
First Awareness	Avoid & Recognize Phishing Attacks (V 2.3)	Data Entry Attack	N/A
Second Awareness - Email Only	Second Awareness - Email Only	Hyperlink attack	N/A

Configuration

Base Settings
Awareness Settings
Attack Settings

< 1 > 10

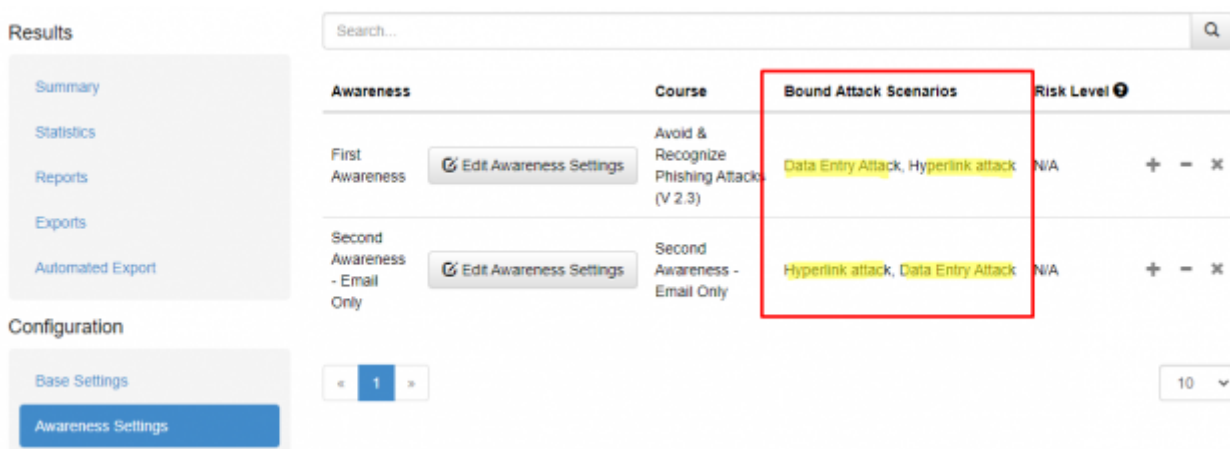
Also, it is possible to review which awareness scenario is bound to the attack scenario. Simply proceed to **Attack Settings** and choose the scenario. Within the scenario proceed to the **Bound Awareness Scenarios** tab. Here you can also unbind awareness scenarios if needed as well as Awareness Settings.



In this section, it is also possible to assign the trainings for the recipients according to their reputation level. More information can be found in the dedicated wiki article [Assign multiple e-learning templates based on user reputation level](#).

How to send several awareness scenarios to one recipient

Depending on the training workflow, one may wish users to get more than one awareness scenario if they fail several attacks. In order to be able to send several awarenesses, you should firstly bound awareness scenarios to the attacks. Make sure that each awareness scenario is bound to the right attacks.



Then you will need to create several copies of the targeted recipient group. The number of groups should correspond to the number of attack scenarios.

multiple aw...

Campaign Status: Stopped

Results

- Summary
- Statistics
- Reports
- Exports
- Automated Export

Configuration

- Base Settings
- Awareness Settings
- Attack Settings
- Schedule
- Recipients

Advanced Settings

- User Settings

Group:

Group Name:

<input checked="" type="checkbox"/>	Email/Phone	Full Name	Language	Staff	Location	Division	Comment	Last Tested
<input type="checkbox"/>	support@lucysecu...	Support	N/A					X
<input type="checkbox"/>	wiki@article.com	Wiki	N/A					X

10

Mapping:

Distribute users over selected scenarios.

Scenarios: Select All

Data Entry Attack (Web Based)

Hyperlink attack (Hyperlink)

Please note: In case **End User Portal** feature is involved in a training process there is no need to create several recipient groups, bound pieces of training will appear in **Portal** at the moment user fails an attack. The feature is rather complex to embrace, especially when talking about sophisticated campaigns and never-ending employee education process. So make sure you have a rigid plan of what awareness goes after what attack and to which recipients and test your structure before running a campaign!

From: <https://wiki.lucysecurity.com/> - LUCY

Permanent link: https://wiki.lucysecurity.com/doku.php?id=binding_multiple_awareness_scenarios_to_particular_attack_scenarios

Last update: 2021/08/16 08:03

