

# fn-isitphishing for IBM Resilient

---

## Table of Contents

- [Release Notes](#)
  - [Overview](#)
    - [Key Features](#)
  - [Installation](#)
    - [Requirements](#)
    - [Install](#)
    - [App Configuration](#)
  - [Function - IsItPhishing HTML document](#)
  - [Function - IsItPhishing URL](#)
  - [Rules](#)
  - [Troubleshooting & Support](#)
- 

## Release Notes

### v1.0.0

- App Host support.
- Package name changed from `fn_isitPhishing` to `fn_isitphishing`.

NOTE Prior installs: Edit your app.config file to change `[fn_isitPhishing]` to `[fn_isitphishing]`

### v1.0.0

- Initial Release
- 

## Overview

**Resilient Circuits Function that queries isitPhishing.org API to analyze a URL or an HTML document**

### Key Features

- This package contains two functions that call the Vade Secure IsItPhishing Webservice API to analyze a URL or to analyze an HTML document.
  - 3 example workflows and rules to demonstrate how to invoke and use the functions.
- 

## Installation

### Requirements

- Resilient platform `>= v36.0.5634`
- An App Host or an Integration Server:
  - To setup up an App Host see: [ibm.biz/res-app-host-setup](https://ibm.biz/res-app-host-setup)

- An Integration Server running **resilient\_circuits**  $\geq 31.0.0$  (if using an Integration Server)
  - To set up an Integration Server see: [ibm.biz/res-int-server-guide](https://ibm.biz/res-int-server-guide)
  - If using an API key account, minimum required permissions are:

Name	Permissions
Org Data	Read
Function	Read

- Proxy supported: Yes

---

## Install

- To install or uninstall an App using the App Host see [ibm.biz/res-install-app](https://ibm.biz/res-install-app)
- To install or uninstall an Integration using the Integration Server see the [ibm.biz/res-install-int](https://ibm.biz/res-install-int)

---

## App Configuration

The following table describes the settings you need to configure in the app.config file. If using App Host, see the Resilient System Administrator Guide. If using the integration server, see the Integration Server Guide.

Config	Required	Example	Description
<b>isitphishing_api_url</b>	Yes	<b><a href="https://ws.isitphishing.org/api/v2">https://ws.isitphishing.org/api/v2</a></b>	<i>IsItPhishing endpoint</i>
<b>isitphishing_name</b>	Yes	<b><a href="#">name</a></b>	<i>username from Vade Secure</i>
<b>isitphishing_license</b>	Yes	<b><a href="#">license from Vade Secure</a></b>	<i>license from Vade Secure</i>

---

## Function - IsItPhishing HTML document

Analyze an HTML document using the Vade Secure IsItPhishing Webservice API.

Dashboards Simulations Incidents **Create**
Resilient Sysadmin

### Customization Settings

Layouts Rules Scripts Workflows **Functions** Message Destinations Phases & Tasks Incident Types Breach Artifacts

Functions / isitphishing\_html\_document

Name \*  
API Name ⓘ  
Message Destination \*  
Description

isitPhishing HTML document  
isitphishing\_html\_document  
fn\_isitPhishing  
Analyze an HTML document using the Vade Secure IsitPhishing Webservice API.

**Creator** Resilient Sysadmin  
**Last Modified** 12/17/2018 21:37  
**Last Modified By** Resilient Sysadmin  
**Associated Workflows** Example: isitPhishing Analyze HTML document

**Inputs**

incident\_id  
task\_id  
attachment\_id  
artifact\_id

**Input Fields ⓘ**

Search...  
artifact\_id  
artifact\_value  
ArtifactEntity  
attachment\_id  
calendar\_invite\_datetime  
calendar\_invite\_description  
calendar\_invite\_extra\_email\_addr  
calendar\_invite\_incident\_id  
calendar\_invite\_subject

## ► Inputs:

Name	Type	Required	Example	Tooltip
artifact_id	number	No	—	-
attachment_id	number	No	—	-
incident_id	number	Yes	—	-
task_id	number	No	—	-

## ► Outputs:

```

results = {'version': '1.0',
          'success': True,
          'reason': None,
          'content': {'result': 'unknown'},
          'raw': '{"result": "unknown"}',
          'inputs': {'incident_id': 2147,
                    'attachment_id': 259,
                    'filename': 'sample.html'},
          'metrics': {'version': '1.0', 'package': 'fn-isitphishing',
                    'package_version': '1.1.0', 'host': 'MacBook-
Pro.local',
                    'execution_time_ms': 2800, 'timestamp': '2020-11-04
16:29:44'}}

```

## ► Example Pre-Process Script:

```

# Required inputs are: incident id and artifact id.
inputs.incident_id = incident.id

```

```
inputs.artifact_id = artifact.id
```

► Example Post-Process Script:

```
if results.success:
    content = u"IsItPhishing analysis of artifact document {0} :
{1}".format(results["inputs"]["filename"],results['content']['result'])
else:
    content = u"IsItPhishing analysis of artifact document {0} :
ERROR".format(results["inputs"]["filename"])

# Create a note
note = helper.createPlainText(content)

# Add note to the task or incident
if task:
    task.addNote(note)
else:
    incident.addNote(note)
```

## Function - IsItPhishing URL

Analyze a URL using the Vade Secure IsItPhishing Webservice API.

The screenshot shows the 'Customization Settings' page for the 'isitphishing\_url' function in the Resilient platform. The page has a top navigation bar with 'resilient' logo and links for Dashboards, Simulations, Incidents, and a 'Create' button. Below the navigation bar, there are tabs for Layouts, Rules, Scripts, Workflows, Functions (selected), Message Destinations, Phases & Tasks, Incident Types, Breach, and Artifacts. The 'Functions' tab is active, showing the 'isitphishing\_url' function configuration.

**Function Configuration:**

- Name:** isitPhishing URL
- API Name:** isitphishing\_url
- Message Destination:** fn\_isitPhishing
- Description:** Analyze a URL using the Vade Secure IsItPhishing Webservice API.

**Metadata:**

- Creator:** Resilient Sysadmin
- Last Modified:** 12/12/2018 13:34
- Last Modified By:** Resilient Sysadmin
- Associated Workflows:** Example: isitPhishing Analyze URL

**Inputs:**

- isitphishing\_url

**Input Fields:**

- artifact\_id
- ArtifactEntity
- attachment\_id
- calendar\_invite\_datetime
- calendar\_invite\_description
- calendar\_invite\_extra\_email\_addr
- calendar\_invite\_incident\_id
- calendar\_invite\_subject
- Entity Type

► Inputs:

Name	Type	Required	Example	Tooltip
------	------	----------	---------	---------

Name	Type	Required	Example	Tooltip
isitphishing_url	text	Yes	-	-

► Outputs:

```
results = {'version': '1.0',
           'success': True,
           'reason': None,
           'content': {'status': 'PHISHING'},
           'raw': '{"status": "PHISHING"}',
           'inputs': {'isitphishing_url': 'https://www.bill-
netflix.com/index.php'},
           'metrics': {'version': '1.0',
                       'package': 'fn-isitphishing',
                       'package_version': '1.1.0',
                       'host': 'MacBook-Pro.local',
                       'execution_time_ms': 5394,
                       'timestamp': '2020-11-12 17:33:23'}}
```

► Example Pre-Process Script:

```
# Get the URL from the artifact value
inputs.isitphishing_url = artifact.value
```

► Example Post-Process Script:

```
# Get the results and post to an incident note.
if results.success:
    content = u'IsItPhishing analysis of URL {0} :
{1}\n'.format(results['inputs']['isitphishing_url'], results['content']
['status'])
else:
    content = u'IsItPhishing analysis of URL {0} :
ERROR\n'.format(results['inputs']['isitphishing_url'])
note = helper.createPlainText(content)
incident.addNote(note)
```

## Rules

Rule Name	Object	Workflow Triggered
-----------	--------	--------------------

Rule Name	Object	Workflow Triggered
Example: IsItPhishing Analyze URL	artifact	<code>example_isitphishing_analyze_url</code>
Example: IsItPhishing Analyze HTML Document: Artifact	artifact	<code>example_isitphishing_analyze_html_document_artifact</code>
Example: IsItPhishing Analyze HTML Document: Attachment	attachment	<code>example_isitphishing_analyze_html_document</code>

## Troubleshooting & Support

If using the app with an App Host, see the Resilient System Administrator Guide and the App Host Deployment Guide for troubleshooting procedures. You can find these guides on the [IBM Knowledge Center](#), where you can select which version of the Resilient platform you are using.

If using the app with an integration server, see the [Integration Server Guide](#)

### For Support

This is a IBM Community Provided App. Please search the Community <https://ibm.biz/resilientcommunity> for assistance.