

## Landing Pages

<https://campus.barracuda.com/doc/77399024/>

When a user clicks a link you placed in a campaign, they are directed to a landing page – a website you specify that can continue the simulation or serve educational content. Security Awareness Training has a variety of Landing Page templates you can use as is or modify for your campaign. Note that when the Campaign ends, its associated Landing Pages are disabled and are no longer accessible by users. For details, see the [Landing Page Visibility](#) section below. Also, before creating custom content for your campaign, please see [Before You Begin](#).

A legal disclaimer is added to all landing pages as a part of a corporate requirement. See [Legal Disclaimer Examples](#) below. The disclaimer cannot be removed. Because of this, email templates no longer require a legal disclaimer and if you select a template that has one, it can be removed.

## Accessing and Editing Landing Pages


To access Landing Pages in the Content Center:

- From anywhere: Navigate to **Campaigns > Landing Pages**.
- While creating a campaign: In the **Content** section, click **Add New Landing Page**.

Security Awareness Training includes many Landing Page templates. Use the filter in the left navigation pane to locate templates for specific categories, like Login or Education.

To use the filter, select your criteria, then click **Apply**. The matching templates display in the Content Center page.

To edit an existing Landing Page template, including the option to add your own content:

1. Locate the desired Landing Page template and click the Edit button . In the **Content Action** dialog, click one of the following buttons:
  - **Edit** to work with the content of the email template.
  - **Copy and Edit** to create a clone of the email template to edit, so you are not altering the original.

The following options are also available, but do not open the email template editor:

- **Copy and Add to My Recent Campaign** to add a clone of the email template to your campaign.
- **Add to My Recent Campaign** to add this specific template to your campaign.



## 2. Enter the following information:

### General Settings

- **Landing Page** – Enter a familiar, unique name for this template.
- **Description** – Optional. Enter text to describe the email template.
- **Category** – Optional. This value is filled in automatically if you are using an existing template. You can change the value if you choose.
- **Active** – Select to enable this template to be used in campaigns.

If you clear the **Active** check box, the email template will not be available to be used in campaigns. If the campaign is in **Design** mode and you deactivate the email template, you will not be able to **Generate** the campaign.

### Page Design

- **Hypertext {link}** – Enter the address to display for the URL, not the actual URL.
- **Page Title** – Enter the title to display across the top of the browser bar.
- **Page Content** – Use the WYSIWYG editor or click the **Source** button to create or edit your template. Click the Image button  to add images from the Security Awareness Training [Image Gallery](#), or your own images, to the Landing Page template. Use the **Video** button  to add MP4 videos, like tutorials, to your Landing Page. Add links within the email to take users to additional pages for the campaign or other predefined simulation or training pages.

When adding links to your template, it is best to specify sites hosted by Security Awareness Training to maximize tracking and reporting. Security Awareness Training cannot track or report on clicks to sites hosted by others, including non-Barracuda learning management systems.

### Features

- **Enable GPS Accuracy Test** – Select to enable users to be prompted to share their GPS location information.
- **Enable Local IP Detection** – Select to enable the landing page to run logic to identify the user's local IP address location.
- **Enable Form Privacy Logic** – Select to enable the privacy logic on all landing page forms, like a login form or feedback form, so none of the data entered by the user will be collected, transmitted, or stored.
- **Enable Debug** – Select to enable JavaScript or other user-visible debug messages on all web pages using this template.
- **Enable Login Form** – Select to enable a login form to be displayed to the user on the landing page.
- **Login Page Content** – Design the login form here.
- **Login Form User Label** – Enter text to label the User Name field on the mock login page.
- **Login Form User Placeholder** – Enter text to display as an example within the User Name field on the mock login page.
- **Login Form Password Label** – Enter text to label the Password field on the mock login page.

- **Login Form Password Placeholder** – Enter text to display as an example within the Password field on the mock login page.
- **Allow Empty Username and Password** – Select to enable the user to leave the Username and Password fields blank while successfully submitting the login form.
- **Use Password Field as Plain Text** – Select to enable the user to see their password as they type it, without obfuscation.
- **Login Button Label** – Enter text for the label for the Submit button on the mock login page.
- **Login Failed Message** – Enter text to display when the user login "fails".
- **Two Step Login Form *Forgot Email* Label** – Only for pages with two factor authentication. The label to use as the **Forgot Email** text in two step login forms. Helpful for translation.
- **Two Step Login Form *More Options* Label** – Only for pages with two factor authentication. The label to use as the **More Options** text in two step login forms. Helpful for translation.
- **Two Step Login Form *Welcome* Label** – Only for pages with two factor authentication. The label to use as the **Welcome** text in two step login forms. Helpful for translation.
- **Login Unencrypted Warning** – Enter text to display as a warning to the user when the site is HTTP and JavaScript is disabled.
- **Enable Feedback Form** – Select to display a feedback form containing your open text fields on the Landing Page.
- **Feedback Page Content** – Design the Feedback Page here.
- **Feedback Topic Label** – Enter text to label the Topic field on the feedback form. The field is called Topic, but you can change the label to be whatever suits your simulation.
- **Feedback Sender Label** – Enter text to label the Sender field on the feedback form. The field is called Sender, but you can change the label to be whatever suits your simulation.
- **Feedback Message Label** – Enter text to label the Message field on the feedback form. The field is called Message, but you can change the label to be whatever suits your simulation.
- **Feedback Response** – Enter text to display as feedback when a user submits the Feedback Form. This section of the form will be formatted as a multi-line text field.
- **Enable File Upload Form** – Select to enable a file upload form to display on the Landing Page. The file upload form is used to entice the user to upload a file to the Landing Page, thus potentially compromising the organization's data. Note that the file will not actually upload to the Security Awareness Training platform, but the system will record the attempt.
- **Upload Page Content** – Design the Upload Page here.
- **Upload File Label** – Enter text to label the Upload File field on the upload file page.
- **Upload Response** – Enter text to display when the user "successfully uploads" a file.
- **Enable File Download** – Select to display a list of files that can be downloaded.
- **Download Page Content** – Design the page where the downloadable files will be displayed.
- **Enable Captcha** – Select to enforce Captcha authentication on the first page of this Landing Page template. This is most commonly used in combination with a Login Form.
- **Captcha Page Content** – Design the Captcha authentication page here.

- **Captcha Failed Message** – Enter the text to display when a user attempts Captcha authentication, but "fails".
- **Enable Page Exit Popup** – Select to display a popup if the user tries to leave the Landing Page without engaging with the content.
- **Page Exit Popup Text** – Enter text to display in the Exit Popup.
- **Enable Page Exit Content** – Select to display an alternate page if the user returns to the page without exiting after the Page Exit Popup.
- **Page Exit Return Content** – Design the alternate page displayed when the user returns.

### Unsubscribe Design

- **URL File {unsubscribe}** – Displays the page name for the unsubscribe portion of the Landing Page.
- **Hypertext {unsubscribe}** – Enter the text to display for the link, not the actual URL.
- **Unsubscribe Title** – Enter the title to display across the top of the browser bar for the Unsubscribe page.
- **Unsubscribe Content** – Design the Unsubscribe page.
- **Unsubscribe Form Email Label** – Enter text to label the email address field on the Unsubscribe form.
- **Unsubscribe Button Label** – Enter text to label the Unsubscribe button on the Unsubscribe form.
- **Unsubscribe Failed Message** – Enter text to display if the user submits a blank or "invalid" Unsubscribe form.
- **Unsubscribe Response Message** – Enter text to display if a user submits a "valid" Unsubscribe form.

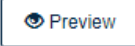
### Attributes

- **Has Quiz** – Select if there is a quiz on this Landing Page.
- **Has Training** – Select if there is training on this Landing Page.
- **Written Language** – Select the language in which the page is written.
- **Spoken Language** – Select the language that is spoken on the page, if present.
- **Created** – The date the template was created. This value is not editable.

### Advanced Settings

- **Template Detail Components** – Add landing page components, such as CSS style sheets.
- **URL Directory {link}** – Enter a **unique** value that becomes part of the URL for this Landing Page. This field is automatically filled with a unique value when you create the Landing Page. You can modify it.
- **URL Template {link}** – Displays what the link will look like to users.
- **Preview Image** – Click **Browse** to select an image to use for this Landing Page template within the Content Center. This image will only display on cards within the Content Center and will not be seen by users.

3. Click **Save** to save your changes.

After you have saved the Landing Page, you can preview your Landing Page at any time by clicking the Preview button  at the top of the page. If you have more than one page – like the main Landing Page and a Login Page – you are able to view each page.

## Landing Page Visibility at Campaign End

When a Campaign ends, any Landing Pages it references are disabled and are no longer accessible by end users.

This section describes Landing Page visibility to end users, when associated with a Campaign. The Landing Page template is still available in the Content Center and locally, if you downloaded it.

When a Campaign containing a Landing Page passes the **Campaign Cutoff Date**, the landing page is locked, or disabled, and appears in a browser as **File Not Found**. In this locked state, the Landing Page still collects clicks for users who click the links, but these clicks are hidden from reporting. If you change the **Campaign Cutoff Date** to a future date before the Campaign goes to the locked state, the Landing Page is immediately re-published and the hidden clicks will be visible in reporting.

After a campaign goes into the **Locked** state, the Landing Page is completely disabled and any clicker activity after that point will be completely ignored and lost. In this state, users who click on the link to the Landing Page will see **404 Resource Not Found** in their browser, because the Landing Page is disabled and is no longer accessible to users.

## Legal Disclaimer Examples

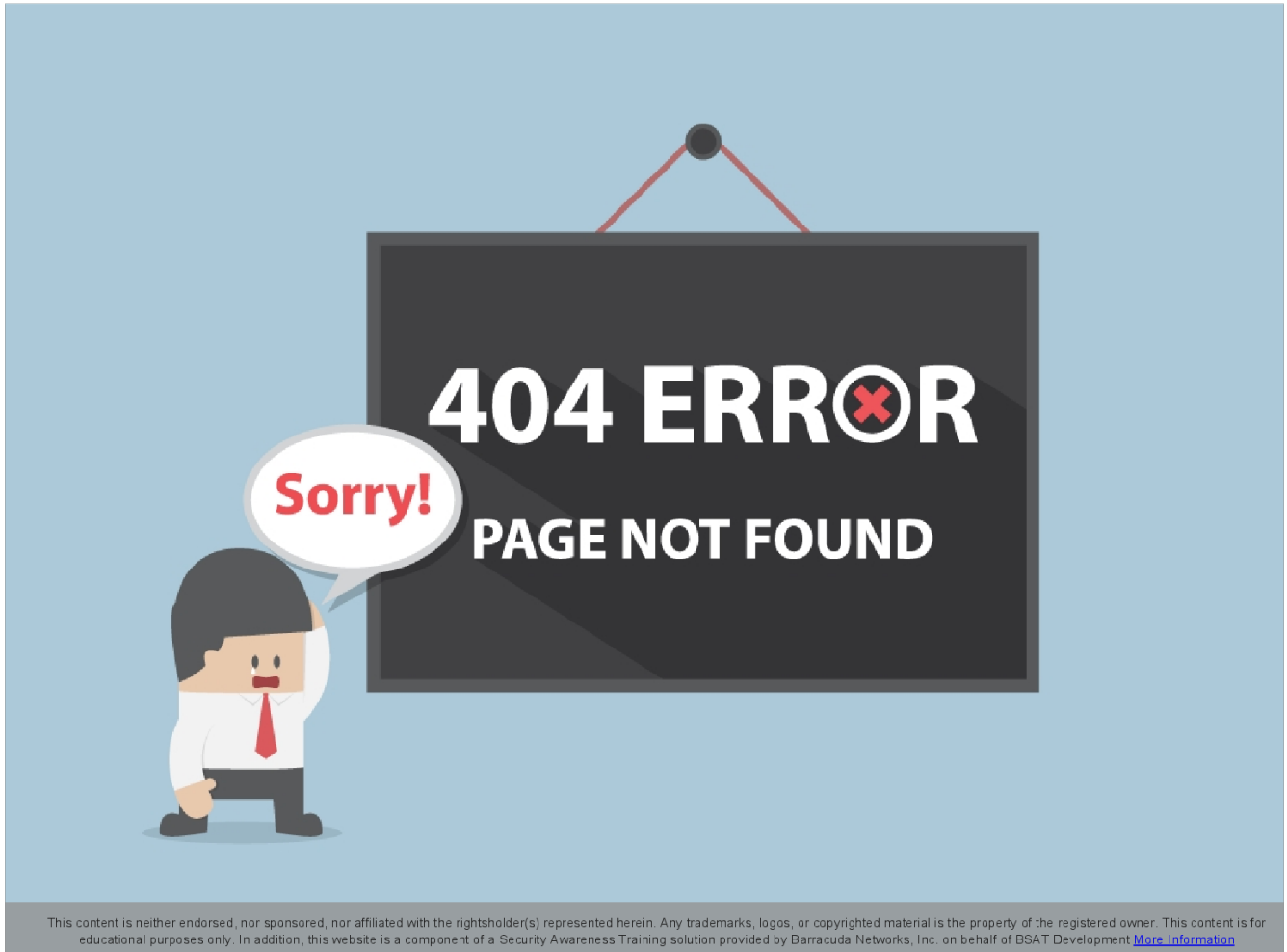
These examples show the placement of the legal disclaimer at the bottom of each landing page.

The text of the disclaimer is as follows:

*This content is neither endorsed, nor sponsored, nor affiliated with the rightsholder(s) represented herein. Any trademarks, logos, or copyrighted material is the property of the registered owner. This content is for educational purposes only. In addition, this website is a component of a Security Awareness Training solution provided by Barracuda Networks, Inc. on behalf of [Customer Name]*  
[More information](#)

*Customer Name* will be replaced by your company name.

*More information* will link to Barracuda Campus.





## Brand Impersonation

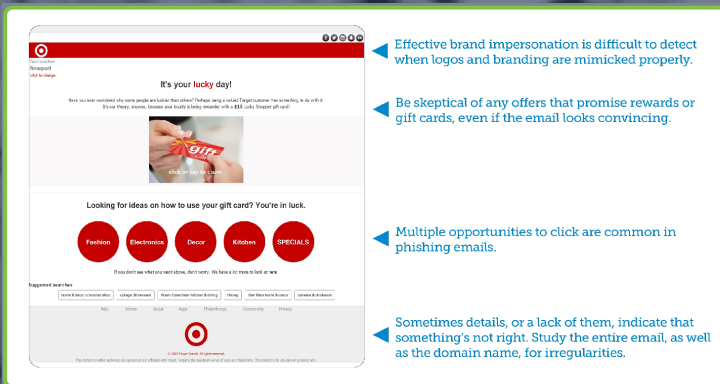
Brand impersonation is designed to mimic a familiar company or business to trick victims into responding and disclosing personal or otherwise sensitive information. Common types of brand impersonation include, service impersonation, a phishing attack designed to harvest login credentials for personal or business accounts, and brand hijacking, whereby fake or spoofed domain names provide the illusion of legitimacy.

Brand impersonation can be difficult to detect when executed well but spoofing a brand convincingly can prove equally challenging for cybercriminals. By paying close attention to things like:

- logo use and placement
- adherence to brand colors and overall design
- copy, tone and overall content
- domain names and web addresses

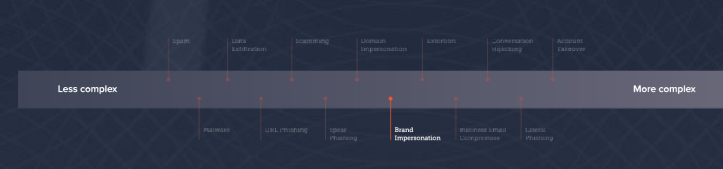
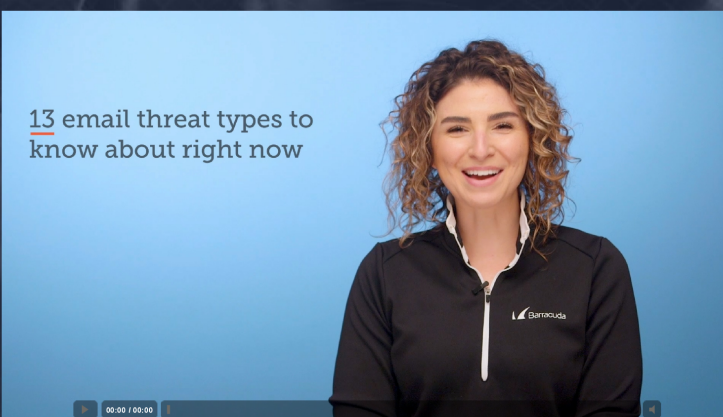
You can spot irregularities and potential spoofing attempts.

The sample shown indicates signs of brand impersonation.



Annotations for the phishing email screenshot:

- Effective brand impersonation is difficult to detect when logos and branding are mimicked properly.
- Be skeptical of any offers that promise rewards or gift cards, even if the email looks convincing.
- Multiple opportunities to click are common in phishing emails.
- Sometimes details, or a lack of them, indicate that something's not right. Study the entire email, as well as the domain name, for irregularities.



Barracuda • 13 EMAIL THREAT TYPES TO KNOW ABOUT RIGHT NOW



This content is neither endorsed, nor sponsored, nor affiliated with the rightsholder(s) represented herein. Any trademarks, logos, or copyrighted material is the property of the registered owner. This content is for educational purposes only. In addition, this website is a component of a Security Awareness Training solution provided by Barracuda Networks, Inc. on behalf of GSAT Development [www.barracuda.com](https://www.barracuda.com)



## Figures

1. editButton.png
2. image.png
3. movie.png
4. previewButton.png
5. legalDisclaimer404.png
6. legalDisclaimerPhished.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.