Understanding Clicks

https://campus.barracuda.com/doc/95262483/

Clicks are an important focus of Security Awareness Training results. While the subject of clicks and clicking might seem obvious, there is more to understand the action than just applying the standard definition.

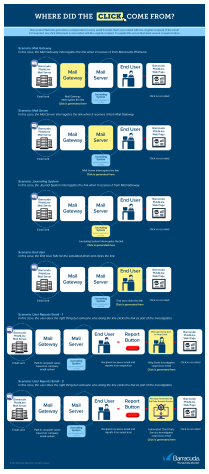
Generally speaking, *clicking* means to use a mouse or other device to interact with an online object, like a link in an email. In Security Awareness Training, the term *clicking* is used to refer to various actions where a user interacts with a campaign, from clicking a link or downloading an attachment in an email. It also refers to activities that do not involve a mouse, but are still interactive, like inputting responses with a telephone keypad in response to a voice campaign. Most of this article is about email campaigns. A user who clicks on a link is called a *clicker*. A user who has clicked links in multiple campaigns is called a *repeat clicker*.

In your Security Awareness Training campaigns, most clicks are registered because one of your users used their mouse to click a link in your campaign emails. Clicks can also come from other interactions that you might not have considered, including:

- The user forwarded the campaign message to your IT organization, reporting it as suspicious. The IT professional clicks the link. See more on this below.
- Other systems in your organization – like mail gateways, mail journaling systems, proxies, and other security systems – might interrogate a link in your campaign message. That action counts as a click.

Links within Security Awareness Training emails are specific to each recipient, so a click from one of the scenarios above will still be associated with the original recipient within your organization.

Download the *Where Did The Click Come From?* infographic for additional scenarios.



What You Can Do

Preventing Clicks

Add trusted domains or IP addresses of campaign emails to your allow list to ensure they arrive to the recipient without interference and additional clicks. For details and instructions, refer to Email Allow List and Best Practices. If you use Microsoft 365 Defender, also refer to Using Microsoft 365 Defender with Security Awareness Training.

Note that Security Awareness Training domains are already allowed by Email Gateway Defense.

Removing Clicks

Use the Address Book Utility to remove campaign clicks based on IP address, ISP, and other factors. For more information and instructions, refer to *Remove Clicks by Machine Click Score* in Address Book Utility.

Communicating with your IT Organization to Prevent Clicks

As described above, your users might consider your campaign email to be suspicious and, correctly, forward it to your IT organization. An IT team member might then click the link to determine if the message is malicious. Even if the link is clicked within a safe environment, the click is still registered to the original recipient of your campaign email.

Consider providing advanced notice to your IT, helpdesk, and support organizations before you send a campaign, so they will be aware of your benign campaign emails and will not need to test them. This results in less work for them and fewer clicks for your campaign.

You can also use custom X-Headers in your campaign emails so your IT organization can easily recognize your emails as internal and benign. Refer to the **Custom Headers** section in Global Settings.

Training Clickers with Automated Campaigns

Users who interact with campaigns are taking unsafe actions and can benefit from safety training. Automated Campaigns are designed to provide clickers with additional training. First, a dynamic address book collects the clickers, then the automated campaign you design ends training content to them. For details, refer to Understanding Automated Campaigns and its associated articles.

Figures