You might not be allowed direct access to the internet via a web browser. Instead you may be allowed access to the internet using a physical different PC or a different infrastructure (e.g. accessing the internet via Citrix etc.). As a result, a link sent in a mail can’t be opened). The only way to conduct a phishing attack in such an environment, without having the user type a long randomized URL into a different system, is by setting a directory within the URL manually. This can be done in the recipient file. There is a variable which you can set called “Link” – a unique link part for the landing page. If you specify this, please make sure it is unique across all recipients in the scenario and does not contain any special characters. If you skip this, the link will be generated automatically. You can choose a simple name for a link for a group of recipients (keep in mind that you can upload different recipient groups per scenario).

Please find more info here.

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=links_in_mails_in_my_company_cannot_be_opened&rev=1448645098

Last update: **2019/07/25 12:52**