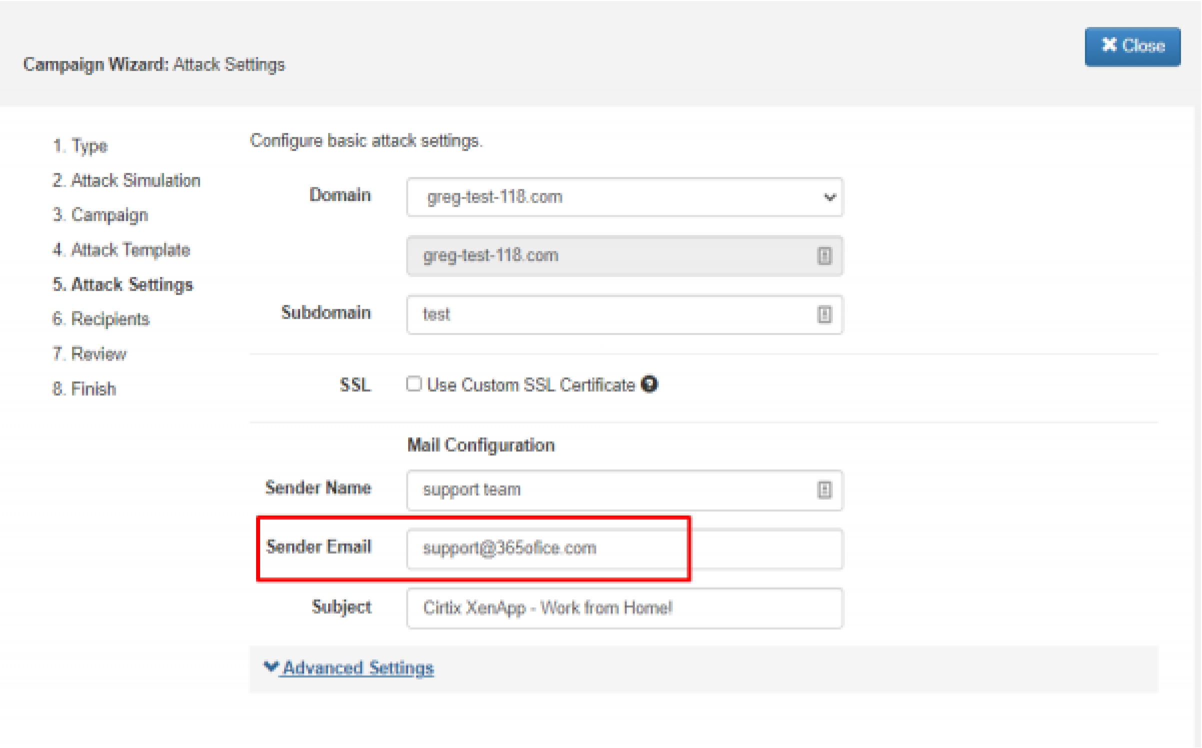
# Sender Email

Lucy provides you with considerable freedom in campaign configuration. That allows users to create sophisticated and content-rich attacks which can repeat actual scam schemes or have a unique structure. However, such freedom is always accompanied by many possible mistakes during campaign configuration. As a result, phishing simulation emails appear in junk folders or get rejected by the recipient's mail server. Poorly configured **Sender Email** address is the most frequent reason for that. Since Lucy specifies that address as a resource of the emails sent to recipients. Thus, any inconsistency might provoke recipient mail server to reject emails which means failed attack

### Where sender email is configured?

Email address can be specified either during the initial campaign configuration in Wizard (screenshot 1) or later under **Attack Settings → Scenario Settings → Message Template** (screenshot 2).

## Screenshot 1



Configure basic attack settings.

Domain: greg-test-118.com

greg-test-118.com

Subdomain: test

SSL: □ Use Custom SSL Certificate

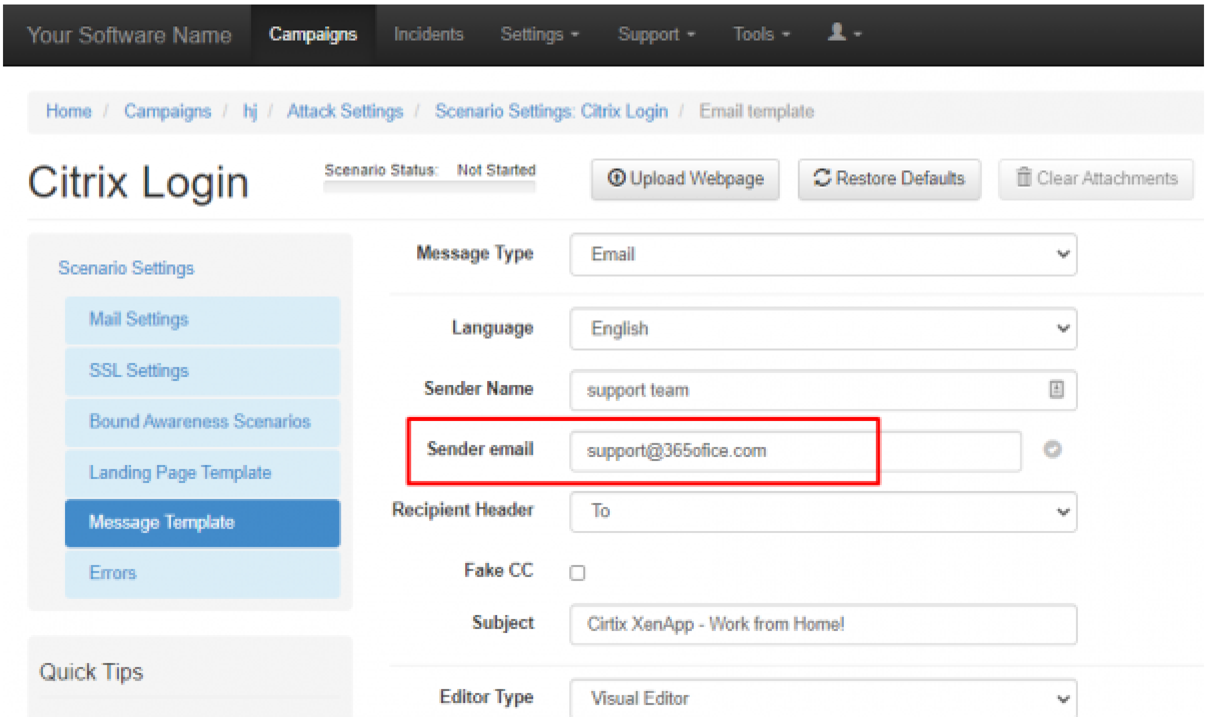
Mail Configuration

Sender Name: support team

Sender Email: support@365ofice.com

Subject: Cirtix XenApp - Work from Home!

## Screenshot 2



Citrix Login

Scenario Status: Not Started

Message Type: Email

Language: English

Sender Name: support team

Sender email: support@365ofice.com

Recipient Header: To

Fake CC: ☐

Subject: Cirtix XenApp - Work from Home!

Editor Type: Visual Editor

### How sender email should be configured?

In order to provide the highest deliverability of simulation emails, it is recommended to specify an existing domain in the email address. The domain should have MX and SPF records pointing to Lucy - this will allow Lucy to send emails on the behalf of this domain. As a result, when the recipient's mail server receives a phishing simulation email and performs DNS lookup, it will not find any inconsistency between the specified sender email address and the actual source of the email.

The domain can be acquired within the Lucy interface or from any registrar. The key to successful delivery is correct DNS records: SPF, MX and DMARC (optional but highly recommended). For domains acquired in Domain configuration (including DNS records management) is described here.

### Common mistakes

Although it is indeed possible to spoof existing domains, it is highly recommended to avoid that and use self-registered domains that contain typos and look like real ones. Most of the mail services have built-in DNS checks which mean that spoofing real domains (especially of big corps like google.com or outlook.com might lead to IP address block from ISPs.