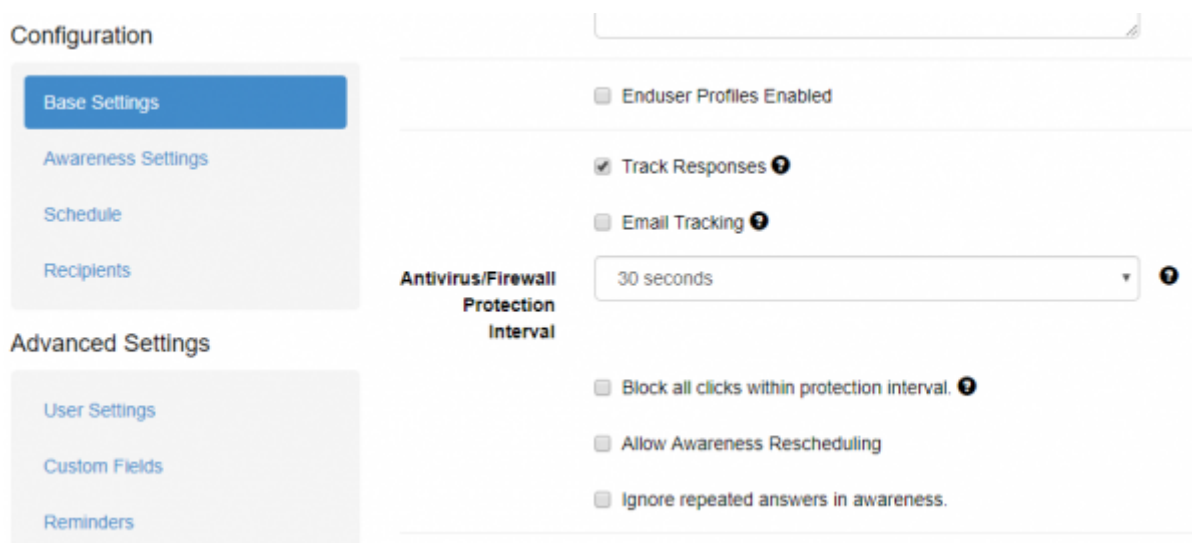


Sometimes a remote Firewall, Spam filter or Virus Filter might automatically scan all the URL's within a link. As a result you end up with false positives and LUCY will show all link clicked (success). To avoid such automatic link requests by some 3rd party application you can enable the antivirus/firewall protection and LUCY will ignore all\* GET requests for the first 30 or 60 seconds:



The screenshot shows the LUCY configuration interface. On the left, there is a sidebar with 'Configuration' and 'Advanced Settings' sections. Under 'Configuration', 'Base Settings' is selected, with 'Awareness Settings', 'Schedule', and 'Recipients' as sub-options. Under 'Advanced Settings', 'User Settings', 'Custom Fields', and 'Reminders' are listed. The main content area shows the 'Antivirus/Firewall Protection Interval' settings. It includes a checkbox for 'Enduser Profiles Enabled' (unchecked), a checked checkbox for 'Track Responses', and an unchecked checkbox for 'Email Tracking'. Below these is a dropdown menu for the 'Antivirus/Firewall Protection Interval' set to '30 seconds'. At the bottom, there are three checkboxes: 'Block all clicks within protection interval.' (unchecked), 'Allow Awareness Rescheduling' (unchecked), and 'Ignore repeated answers in awareness.' (unchecked).

**\*Note:** it starts to work starting from the 2nd recipient that clicks the link too fast. For example, you have 4 recipients, run a campaign, you get the first click within the 1st minute: it gets counted, but the system moves to the alerted state, the 2nd click within 1-minute interval turns on the protection and drops the click. All further clicks under 1 minute will be dropped as well. We are counting the 1st click, because it is useful **for testing purposes**. If you want to ignore **all** clicks within chosen interval, you can tick the "Block all clicks within protection interval" checkbox.



You should enable both options when starting a campaign in production.

## Important notice for Office 365 email customers

If your recipients use **Office 365** with Exchange Online Protection (EOP) and you cannot add Lucy's IP address or sender's email address to the trusted list, then please configure the Antivirus Protection Interval to "1 minute" and activate the option "Block all clicks within protection interval".

Besides, you will have to set up a [Scheduler](#) for your campaign in order to distribute the sending of phishing\awareness emails during a longer period of time and not all at once. This is because Office 365 usually comes with [Advanced Threat Protection \(ATP\)](#) enabled which scans each incoming email for malicious and phishing. Such actions made by ATP might trigger Lucy to count clicks and visits.

From:  
<https://wiki.lucysecurity.com/> - LUCY

Permanent link:  
[https://wiki.lucysecurity.com/doku.php?id=antivirus\\_spam\\_protection\\_interval\\_setting](https://wiki.lucysecurity.com/doku.php?id=antivirus_spam_protection_interval_setting)

Last update: **2019/10/13 11:05**

