

Client-side Phishing Quick Guide



Thank you for using Core Impact™! This Quick Guide will step you through a basic Client-side Phishing test. To perform these steps, launch Core Impact and open a valid workspace.

Before continuing, make sure you are authorized to perform penetration tests on your perspective target users and systems.

This quick guide is meant to serve as an introduction to the penetration testing capabilities of Core Impact. There are many variations of Core Impact's functionality that are not represented here. For more details, use the Help link within Core Impact.

Client-side Phishing Summary

The Client-side Phishing test is comprised of three steps which, when run in sequence, provide a way for you to test your users and their awareness of Phishing tactics. You will learn how secure your user community is from social engineering attacks.

Client-side Information Gathering - This step uses multiple sources (e.g. search engines, LinkedIn) to locate email addresses of potential target users - the same way a potential attacker would. The email addresses are stored in the entity database and can then be used in the Phishing step of the RPT.

Attack Phase: Phishing - Using the details from the previous step, Core Impact will send an email to your selected email targets. If recipients of the email take action, you will learn that they are susceptible to Phishing attacks and you can even capture their sensitive data to use in subsequent tests.


Client-side Report Generation - As with all Core Impact RPTs, the Report Generation step provides detailed reports on information gathered during the previous steps. These reports are essential in compiling vulnerability data and developing ongoing prevention and remediation strategies.

Run a Client-side Phishing Test

TIP:

Before beginning the test, you will need the domain of the users you wish to target, and the connection info (address and port) for a valid SMTP server.

Client-side Information Gathering:

1. Click the **Client Side RPT** button  .
2. Click the **Client-side Information Gathering** step.
This will launch the Information Gathering wizard.
3. Click the **Next** button to get started.
4. Select **Search Engines** for the **Email Address Gathering** and click the **Next** button.
These are public sources. You can also import your own list of email addresses.

NOTE:

The Core Impact User Guide has further details on how to use LinkedIn to discover potential Client-side targets.

5. Type the domain that corresponds to the email addresses you would like to target.
For example, **mycompany.com**.
6. Leave the default options for Web Crawling and Search Engine Options and click the **Next** button.
7. Leave the default options for the Client-Side Information Gathering Setup and click **Finish**.

The Information Gathering step will launch the necessary modules - you will see these modules and can monitor their progress in the Executed Modules pane. When the modules are completed, look for new email addresses in the Client Side tab of the Entity Database, then move to the Phishing step.

Client-side Attack Phase: Phishing

1. Click **Phishing** (under Attack Phase) step to launch the Phishing wizard.
2. Click the **Next** button to get started.
3. Select **Web Page Redirect** on the **Phishing Type Selection** page and enter the URL of where you want a user redirected if they click your emailed link. Click **Next**.
4. Click the **From:** button and select an email address that will serve as the sender of your attack email, then click **OK**.

If the email address you want is not yet in the Entity view, you can right-click in the list to create a new one.

5. Click the **To:** button and select one or more email addresses that will be the recipients of your attack email, then click **OK**. Click the **Next** button to proceed with the test.

6. On the **Email Template Selection** step, use the default settings and click **Next**.

You will use a predefined email template but could import one from Outlook or Thunderbird.

7. On the **End User Experience** step, use the default settings and enter a **Subject** for your email. Click **Next**.

These settings form the email that is sent to target users. The email needs to appear legitimate and entice the reader to take action.

8. Leave the options un-checked and click **Finish**.

You can set advanced actions for mail sending, web server setup and more.

The Phishing step will launch the necessary modules, sending an email to everyone you selected in the wizard setup. If a user clicks the link in the Phishing email, this information is captured and you will know to what extent your user community is vulnerable to actual Phishing attacks.

Client-side Report Generation:

1. Click the **Client-side Report Generation** step to launch the Client-side Report Generation wizard.

2. Click the **Next** button to get started.

3. Select the report you wish to run, then click **Next**. See below for report types and descriptions.

4. Each report will have one or more additional options - use the default settings for now and click the **Next** button (or **Finish** button if applicable).

Depending on the report type, you may have to select one or more workspaces.

5. Click the ellipsis button  to view and select the workspace(s) for which you want a report.

6. Select the workspace(s) on the left and click the **Add** button to select them. Then click **OK** to return to the wizard.

If you select any workspaces that are not currently opened, you will need to enter the workspace password.

7. Click the **Finish** button to run the report.

The report will open in a new window and can be printed or exported in multiple formats such as PDF, HTML and RTF.

Available Client-side Phishing Reports

- **Client-side Phishing Report:** A detailed report about Phishing tests.
- **User Report:** A detailed report about all the users that were discovered and targeted.
- **Delta Report:** A report showing a side-by-side comparison of test statistics for any 2 workspaces.

FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey.

Learn more at fortra.com.