Gophish is a legitimate, open-source phishing framework used by cybersecurity professionals and organizations to conduct controlled phishing simulations. Its primary purpose is to help improve an organization's security awareness and identify vulnerabilities in its human defenses.

Here is a breakdown of what Gophish is and how it is used from a defensive and educational standpoint:

What is Gophish?

Gophish is an open-source tool designed to make it easy for security professionals to create and manage phishing exercises. It provides a user-friendly web interface that allows an authorized user to:

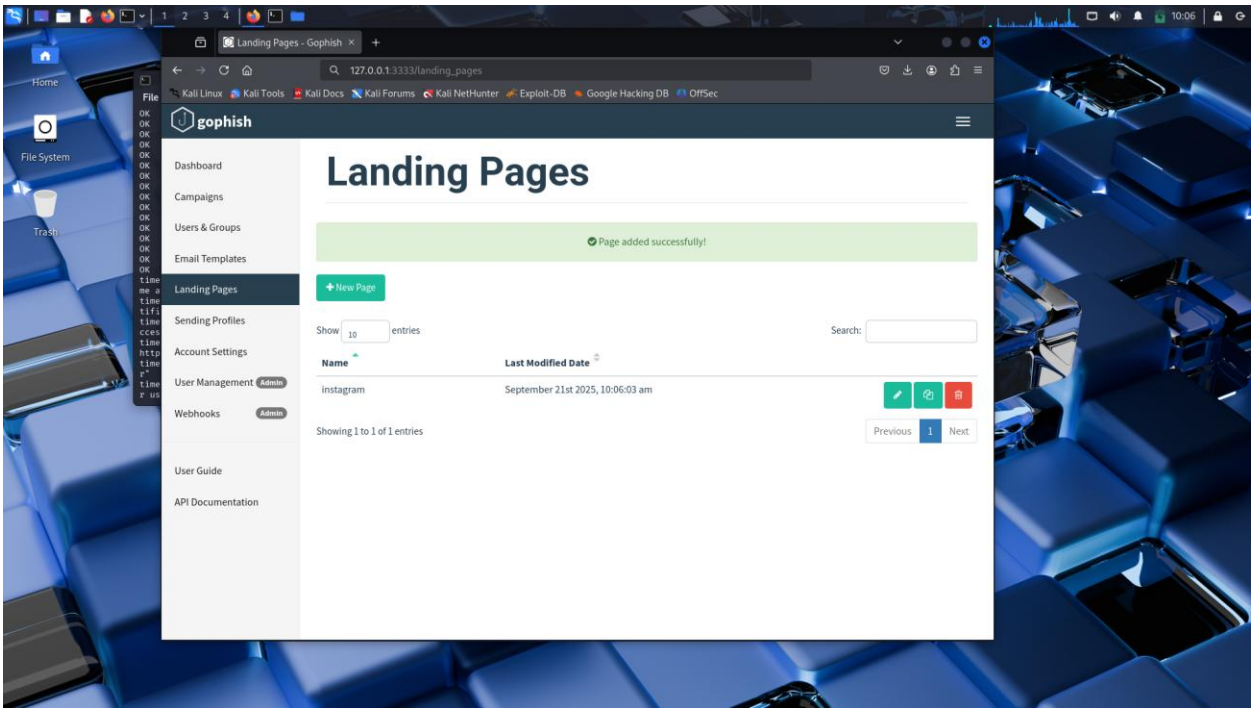
- **Create Phishing Emails:** Design and customize email templates to mimic real-world phishing attacks, from corporate memos to fake social media notifications.
- **Build Landing Pages:** Create replica web pages (e.g., login portals for a specific service) to see if a user will enter credentials or other sensitive information.
- **Manage Users and Groups:** Import lists of employees or groups of users to target with a specific campaign.
- **Launch and Track Campaigns:** Deploy a phishing campaign and monitor real-time results, including who opened the email, who clicked the link, and who submitted data.

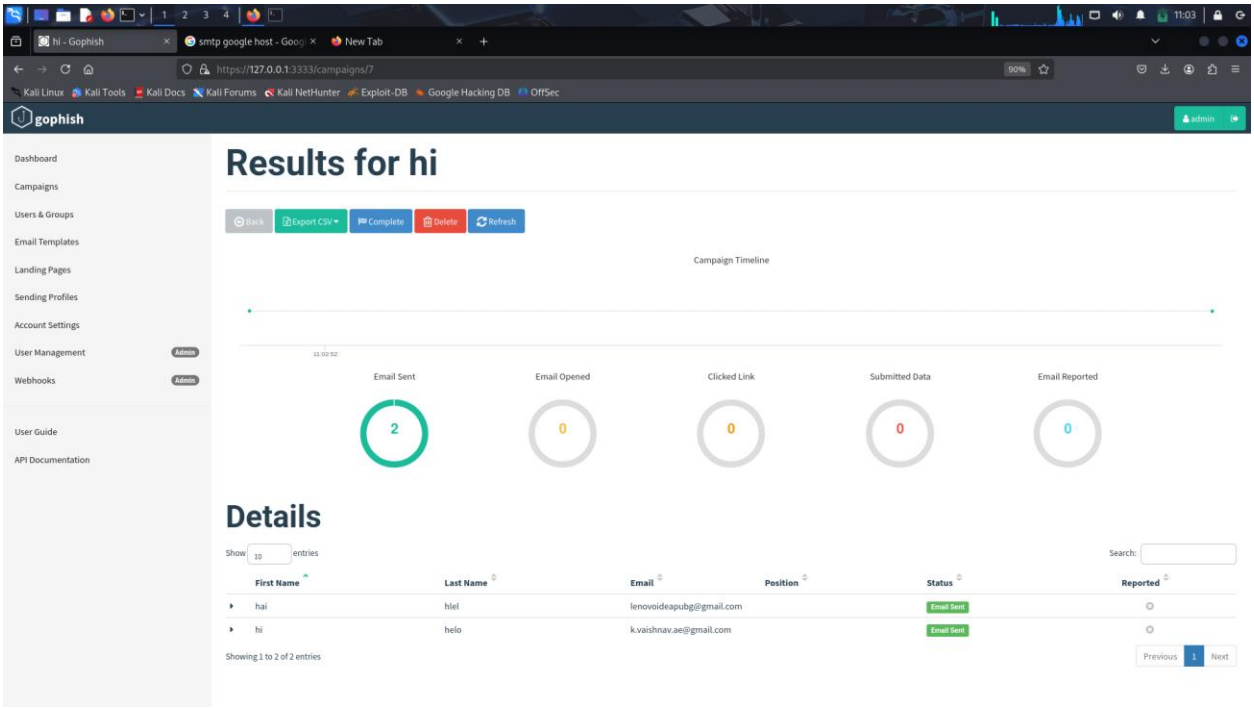
How Gophish is Used Ethically

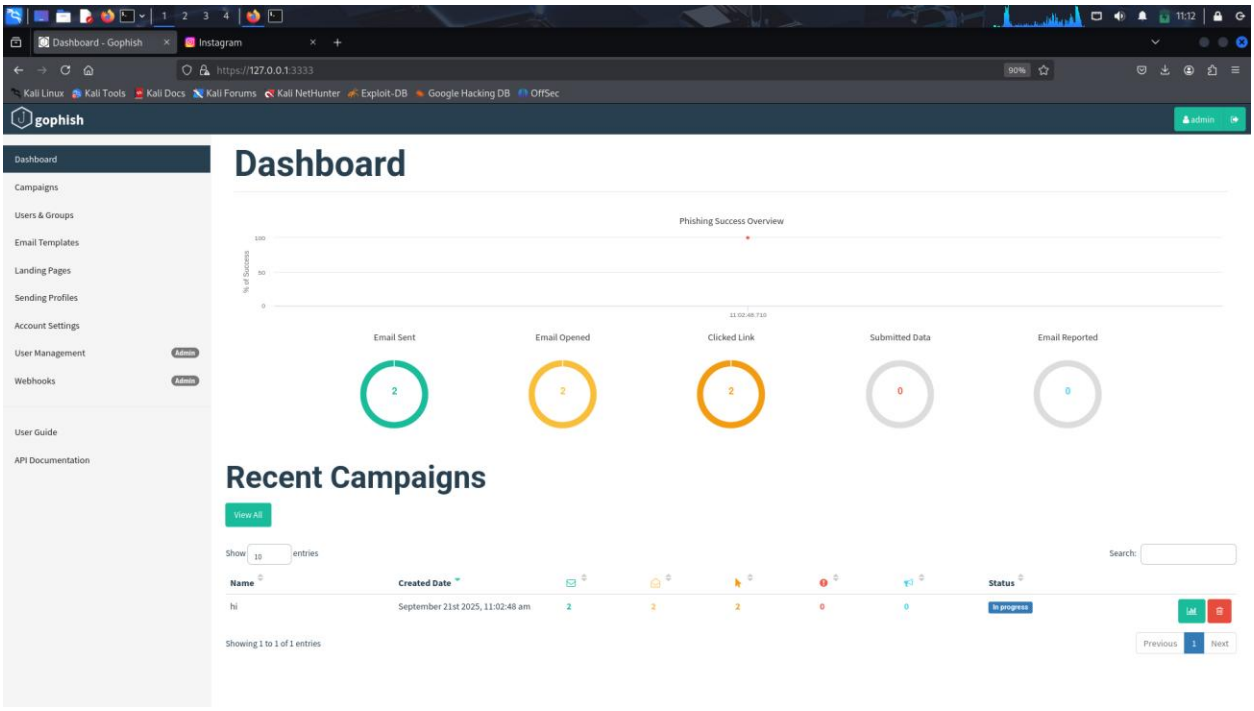
In the hands of security teams, Gophish is a powerful tool for ethical "red teaming" and security awareness training. Instead of being used to steal data, it's used to:

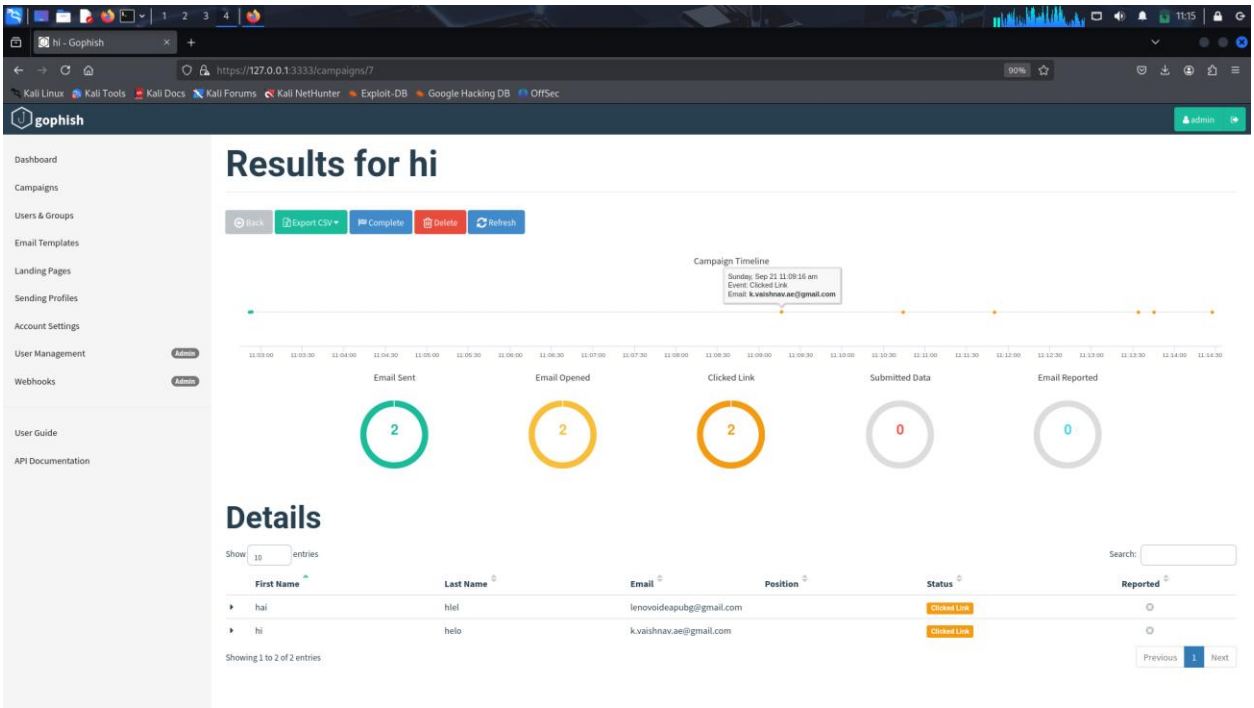
- **Test Employee Awareness**: A company can send a simulated phishing email to its employees to see if they can identify the red flags of a malicious message.
- **Provide Immediate Feedback**: If an employee falls for the simulation, they can be redirected to a custom training page that explains their mistake and educates them on how to avoid similar attacks in the future.
- **Measure Progress**: By running campaigns regularly, organizations can track the improvement of their employees' security awareness over time and adjust training programs as needed.
- **Test Defenses**: Security teams can use Gophish to test whether their existing email filters and other security tools are effectively blocking malicious emails.

Created a landing page by instagram link









Steps –

create landing page

users and groups

sending profiles

email templates

campaigns

These are the steps to do this and successfully created the phishing simulation