

# **Gophish Tool Exploration**

## **Final Report**

### **Cyber Security**

**Name: BANAVATH ANUSHA**

**Program Name: Gophish CS Tool Exploration.**

**Date: 8/30/2025**

**Github Repository: <https://github.com/AnushaBanavath/Gophish-Exploration>**

# Gophish Tool Exploration– Final Report

## Project Overview

The goal of this project was to explore and implement the Gophish open-source phishing simulation toolkit. The objective was to simulate targeted phishing campaigns, analyze user susceptibility (email opens, link clicks, credential submissions, and reports), and gain hands-on experience in testing organizational security awareness.

## Technologies & Tools Used

**Gophish:** Application: Go-based phishing simulation framework

**MailHog:** For capturing and testing email delivery locally

**HTML:** For custom templates and landing pages

**Git & GitHub:** Version control for templates and scripts

## System Architecture

**Mail Server Setup:** Utilized MailHog for safe, local email delivery during testing

**Group Configuration:** Created target groups in Gophish for campaign segmentation

**Email Template Design:** Built custom phishing emails using the integrated HTML editor

**Landing Pages:** Deployed realistic landing pages to capture clicks and potential credentials

**Campaign Launch:** Sent simulated phishing emails to defined groups from the dashboard

**Result Analysis:** Tracked recipient actions (opened, clicked, submitted, reported) and exported findings for review

## Security Features

**Group Management:** Segregated users for targeted campaigns and analysis

**Local Mail Capture:** Prevented risk by using MailHog during development

**Live Campaign Tracking:** Monitored in real-time who opened emails, clicked links, or submitted data

**Reporting:** Encouraged users to report phishing emails; tracked responses

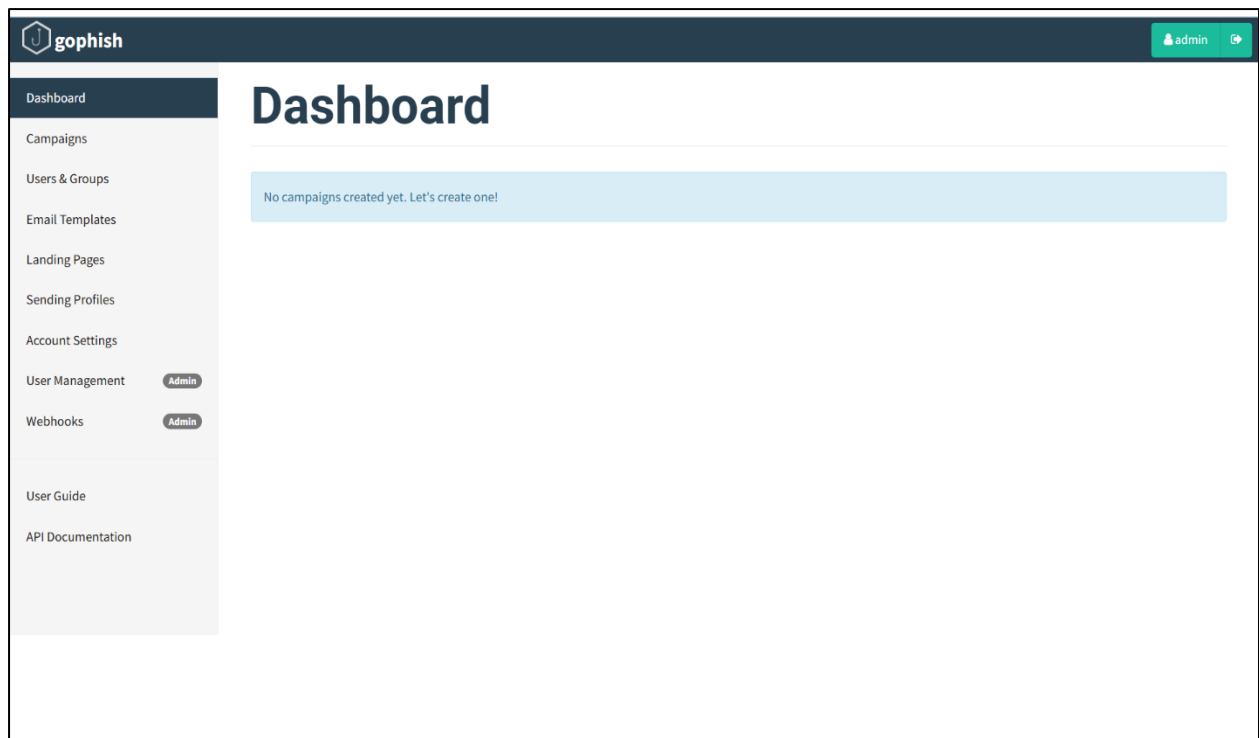
**Result Export:** CSV export for further processing and documentation

# Folder Structure


```
Gophish-exploration/
├── templates/
│   ├── sample_email.html    # Phishing email HTML template
│   └── targets.csv          # Recipient list for campaigns
├── screenshots/
│   ├── Group.png            # Group setup screenshot
│   ├── README.md            # Documentation for screenshots (optional)
│   ├── Result.png           # Campaign summary screenshot
│   ├── Result_Details.png   # Details/results screenshot
│   ├── dashboard.png        # Main dashboard screenshot
│   ├── email_template.png   # Email template creation screenshot
│   ├── landing_page.png     # Landing page setup screenshot
│   └── mailHog_inbox.png    # MailHog inbox screenshot
├── .gitignore               # Specifies files/folders for Git to ignore
├── ETHICS.md                # Ethical considerations and testing
├── disclaimers
│   ├── INSTALL.md           # Setup and installation instructions
│   └── README.md            # Project overview and usage documentation
```

# Screenshots

## 1. Dashboard Overview



## 2. Target Group Creation

gophish

admin

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User ManagementAdmin

WebhooksAdmin

User Guide

API Documentation

# Users & Groups

Group updated successfully!

New Group

Show 10 entries


Search:

Name	# of Members	Modified Date
Demo-Targets	3	August 30th 2025, 3:47:57 pm

Showing 1 to 1 of 1 entries

Previous1Next

## 3. Phishing Email Template

gophish

admin

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User ManagementAdmin

WebhooksAdmin

User Guide

API Documentation

# Email Templates

Template added successfully!

New Template

Show 10 entries

Search:

Name	Modified Date
Demo Template	August 30th 2025, 3:50:48 pm

Showing 1 to 1 of 1 entries

Previous1Next

## 4. Landing Page Setup

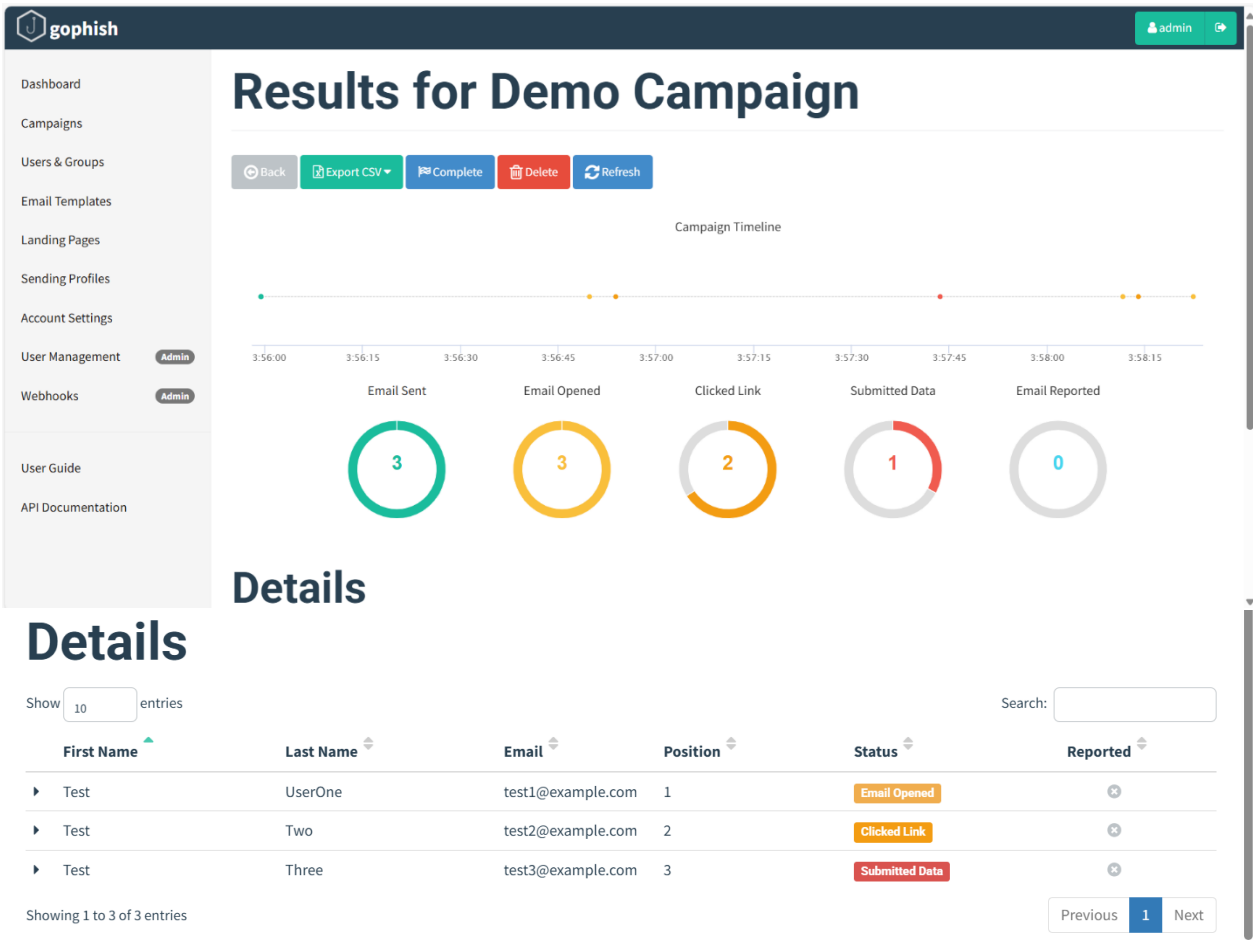
The screenshot shows the Gophish web interface for managing landing pages. The top navigation bar includes the Gophish logo and a user profile for 'admin'. The left sidebar contains a menu with options: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages (selected), Sending Profiles, Account Settings, User Management (Admin), Webhooks (Admin), User Guide, and API Documentation. The main content area is titled 'Landing Pages' and features a '+ New Page' button. Below this, there is a search bar and a table with columns 'Name' and 'Last Modified Date'. The table contains one entry: 'Demo Landing Page' with a last modified date of 'August 30th 2025, 3:52:52 pm'. To the right of the table entry are three icons: a pencil (edit), a document with a plus sign (clone), and a trash can (delete). At the bottom of the table, it says 'Showing 1 to 1 of 1 entries' and a pagination bar with 'Previous', '1', and 'Next' buttons.

Name	Last Modified Date
Demo Landing Page	August 30th 2025, 3:52:52 pm

## 5. Local Mail Server (MailHog)

The screenshot shows the MailHog web interface. The top navigation bar includes the MailHog logo, a search bar, and a GitHub logo. The left sidebar contains a menu with options: Connected (with a green status icon), Inbox (0), and Delete all messages. The main content area displays a message from 'Jim' with the text 'Jim is a chaos monkey. Find out more at GitHub.' and a button labeled 'Enable Jim'.

## 6. Campaign Results Summary & Details



## Testing & Results

- A demo campaign was created using a sample target group, email, and landing page.
- Campaign progress was tracked via Gophish dashboard; all recipients' actions were logged (opened, clicked, submitted data).
- No real emails were sent externally due to MailHog setup, ensuring a controlled test environment.
- Detailed recipient statistics helped analyze user behavior and security awareness.
- All data was exported and reviewed; no credentials were stored or misused.

## Deliverables

- GitHub repository containing all templates, configuration, and documentation
- Walkthrough screenshots demonstrating each workflow stage
- This final report summarizing the project and its findings

## **Learning Outcomes**

- Practical understanding of phishing simulation workflows using Gophish.
- Experience in configuring local mail servers for safe testing
- Analysis of security awareness metrics and reporting
- Familiarity with best practices for ethical phishing testing

## **Conclusion**

This project successfully demonstrates how Gophish can be used to launch and analyze simulated phishing attacks for educational and security testing purposes. With real-time tracking, local mail testing, and comprehensive reporting, the exercise provides valuable insights into organizational vulnerability and user awareness, laying a strong foundation for future security training initiatives.