Phishing Simulation Assessment for Tech Crush

Organization: Tech Crush

Project Type: Security Awareness Phishing Simulation

Date: Jan 15th, 2026

Prepared by: Group 4

TABLE OF CONTENTS

1. Project Overview & Scope

Objective

The objective of this project is to design and execute a controlled **phishing simulation** for the organization **Tech Crush**. The simulation is intended to assess employee awareness of phishing threats by measuring how many users interact with a simulated phishing email, including clicking a malicious-looking link and submitting credentials on a **simulated phishing landing** page.

No real credentials, malware, or harmful payloads are used during this exercise. All data collected is **for security awareness and risk assessment purposes only**.

Scope

This project includes the following activities:

- Designing a phishing policy aligned with ethical and security best practices
- Researching and selecting an open-source phishing simulation tool
- Configuring and executing a phishing campaign against a defined group of Tech Crush staff
- Tracking user interactions such as:
    - Email opens
    - Link clicks
    - Credential submissions (simulated only)
- Analyzing results to identify organizational risk
- Producing two formal reports:
  an Executive Report for management
  a Technical Report documenting the full process

Out of scope:

- Real credential harvesting
- Malware delivery
- Exploitation of systems
- Any unauthorized testing

Deliverables

At the conclusion of this project, the following deliverables will be produced:

1. Executive Report

A non-technical summary intended for leadership that explains:

- What was tested
- Why phishing poses a risk to Tech Crush
- Key results of the simulation
- Risk implications
- Recommendations for improvement

2. Technical Report

A detailed, technical document that includes:

- Tool selection and justification
- Environment setup and configuration
- Campaign design and execution steps
- Screenshots of Gophish configuration and results
- Metrics and analysis
- Challenges encountered and mitigations

Success Criteria

The project will be considered successful if:

- The phishing simulation runs without technical errors
- User interactions are accurately tracked
- Results clearly demonstrate phishing awareness levels
- All deliverables meet academic and ethical requirements

2. Tool Selection: Pick and Justify an Open-Source Tool

Selection Criteria

To select an appropriate phishing simulation tool for this project, the following criteria were used:

- **Ease of Setup and Use** — Suitable for beginners and academic environments
- **Phishing-Specific Features** — Ability to design phishing emails, landing pages, and track user interaction
- **Reporting Capabilities** — Clear metrics such as email opens, clicks, and form submissions
- **Open-Source Availability** — Free to use and inspectable code
- **Community Support & Documentation** — Availability of tutorials, documentation, and active user community

Tool Comparison

1. Gophish

Gophish is an open-source phishing simulation framework specifically designed for security awareness training and ethical phishing campaigns. It provides a web-based user interface that allows administrators to easily configure phishing campaigns without extensive technical knowledge.

Key features include:

- Email template creation
- Landing page creation
- Target group management
- Campaign tracking (emails sent, opened, links clicked, and credentials submitted)
- Real-time dashboard and reporting

Gophish is widely used by security professionals and is well-documented, making it ideal for academic and beginner-level projects.

2. Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is a powerful penetration testing framework that includes phishing among many other social engineering attack vectors.

While SET offers advanced capabilities, it has several limitations for this project:

- Designed primarily for penetration testers, not awareness simulations
- More complex setup and command-line driven
- Limited built-in reporting for phishing awareness metrics
- Higher risk of misuse if not carefully controlled

Due to its complexity and broader attack scope, SET is less suitable for a controlled, educational phishing simulation.

3. Other Tools (KingPhisher, uPhish, etc.)

Other open-source tools such as KingPhisher and uPhish were considered. However:

- Some require more manual configuration
- Some have steeper learning curves
- Others lack a polished user interface or comprehensive tracking features

These tools were therefore not selected for this project.

Tool Selection Justification

After evaluating the available options, Gophish was selected as the phishing simulation tool for this project.

Gophish best meets the project requirements because:

- It is purpose-built for phishing simulations
- It provides a simple and intuitive web interface
- It offers detailed tracking and reporting features
- It is open-source and widely supported
- It minimizes ethical and technical risk in an academic environment

Final Decision

Gophish is the most appropriate tool for conducting an ethical phishing simulation for Tech Crush due to its usability, focused feature set, and strong documentation.

3. Basic Technical Explanation of How Gophish Works

Gophish is an open-source phishing simulation platform designed to help organizations test and improve employee awareness of phishing attacks. It operates as a server application with a web-based management interface that allows administrators to create, launch, and monitor phishing campaigns.

This section explains the main components of Gophish in plain language.

Installation & Setup

Gophish runs as a standalone server application that is installed on a local machine, virtual machine, or cloud server. Once started, it launches a secure web interface that is typically accessed through a web browser at:

https://localhost:3333

This web interface is used to configure all phishing campaigns, templates, targets, and reports. Gophish does not require a complex installation process and runs from a single executable file.

Campaign Components

Sending Profile

The sending profile defines how Gophish sends phishing emails. It contains:

- The SMTP server address
- Port number
- Authentication credentials
- Email sender address

This allows Gophish to send emails that appear to come from a legitimate source during the simulation.

Email Template

The email template is the phishing email content sent to users. It can be written in plain text or HTML and is designed to resemble a legitimate business email. The template typically includes a link that directs the user to a phishing landing page.

Landing Page

The landing page is a simulated web page that users see after clicking the phishing link. It often resembles a login page and is used to track whether users attempt to enter credentials. Any submitted data is simulated only and not used for real authentication.

Targets

Targets are the individual email addresses that will receive the phishing email. Targets are usually imported from a CSV file and represent the staff being tested in the simulation.

Groups

Groups are used to organize targets into logical sets, such as departments or test batches. This allows campaigns to be launched against specific groups rather than all users at once.

Campaign Execution

Once all components are configured, a campaign is created by linking:

- A sending profile
- An email template
- A landing page
- A target group

After launching the campaign, Gophish automatically sends phishing emails and begins tracking user interaction.

Tracking & Reporting

Gophish provides real-time reporting through its dashboard. The platform tracks:

- Emails sent
- Emails opened
- Links clicked
- Credentials submitted (simulated)

These metrics are displayed visually and can be exported for analysis. The collected data is used to measure phishing awareness and identify areas where additional training may be required.

Summary

In summary, Gophish simplifies phishing simulations by providing an easy-to-use interface for campaign creation, execution, and reporting. Its modular design allows each component to be configured independently, making it suitable for educational and organizational security awareness testing.

4. Security and Ethical Considerations

Phishing simulations involve deliberate deception and therefore must be conducted with strict ethical and security controls. This project was designed and executed in accordance with ethical hacking principles and organizational security policies to ensure that no harm was caused to individuals or systems.

Authorization and Consent

Prior to conducting the phishing simulation, explicit authorization must be obtained from Tech Crush management. This authorization confirms:

- Approval to conduct a phishing awareness simulation
- Identification of the scope of testing
- Agreement on which employees or groups will be included
- Confirmation of the campaign duration

No phishing activity is conducted without documented permission.

Use of Non-Malicious Simulation

The phishing campaign is strictly simulated and does not include:

- Real malware or malicious payloads
- Exploitation of vulnerabilities

- Real credential harvesting

Any credentials entered on the landing page are treated as simulated input only and are not used for authentication or stored in usable form.

Scope Definition and Transparency

Leadership at Tech Crush is informed of:

- The objectives of the simulation
- What metrics will be measured (opens, clicks, submissions)
- What will not be tested (e.g., system compromise)

This ensures transparency and prevents misunderstandings regarding the purpose of the campaign.

Data Handling and Privacy

All collected data is handled securely and used solely for analysis and reporting. Controls include:

- Limiting access to simulation data to authorized personnel
- Storing data on secured systems
- Avoiding the collection of unnecessary personal information

Results are reported in aggregate form to avoid singling out individual employees.

Legal and Ethical Compliance

This project adheres to ethical hacking standards, including:

- Acting only within approved scope
- Avoiding unnecessary disruption to business operations
- Respecting employee privacy
- Using results for improvement rather than punishment

Summary

By enforcing authorization, limiting scope, protecting data, and ensuring transparency, this phishing simulation aligns with accepted ethical and legal standards. These controls ensure that the project provides value to Tech Crush without introducing risk.

5. Installation & Configuration

This section documents the environment setup, installation, and configuration of the Gophish phishing simulation framework used in this project.

5.1 Environment Setup

Chosen Environment

Gophish was deployed in a :
Local Virtual Machine (VirtualBox / VMware)

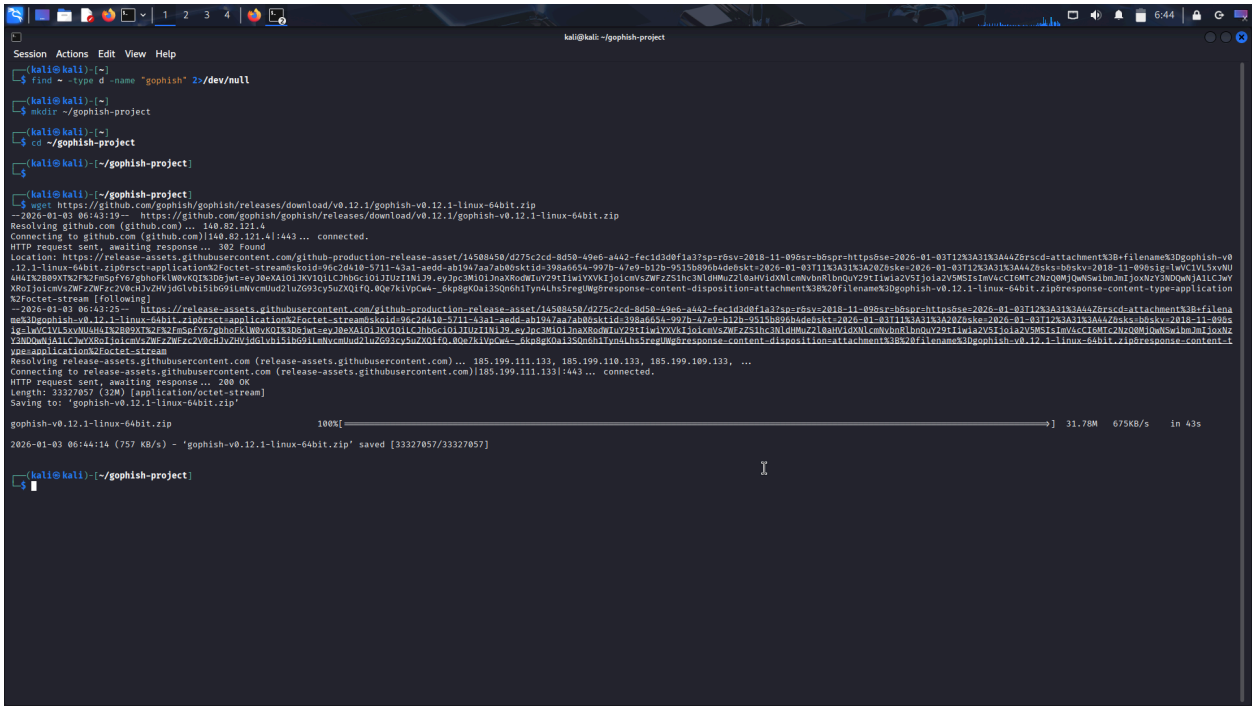
Environment Details

- Operating System: Ubuntu Linux 22.04 LTS
- CPU: 2 vCPUs
- RAM: 4 GB
- Network: NAT / Bridged (as required)

5.2 Gophish Installation

Downloading Gophish

1. Navigate to the official Gophish GitHub repository.
2. Download the correct binary for the operating system in use.
3. Extract the downloaded archive to a working directory.



1.1 Installing Gophish

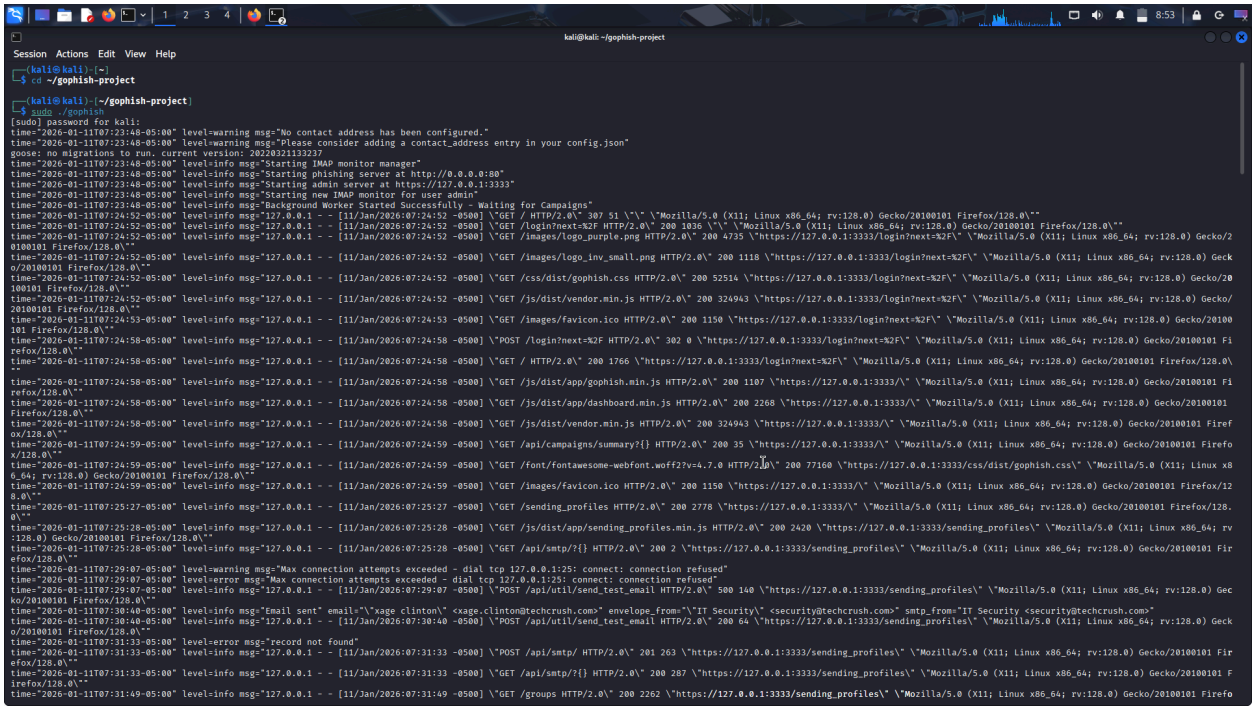
Running Gophish

1. Open a terminal or command prompt.
2. Navigate to the extracted Gophish directory.
3. Run the Gophish executable.

   Example: ./gophish

Once started, Gophish displays startup logs and launches:

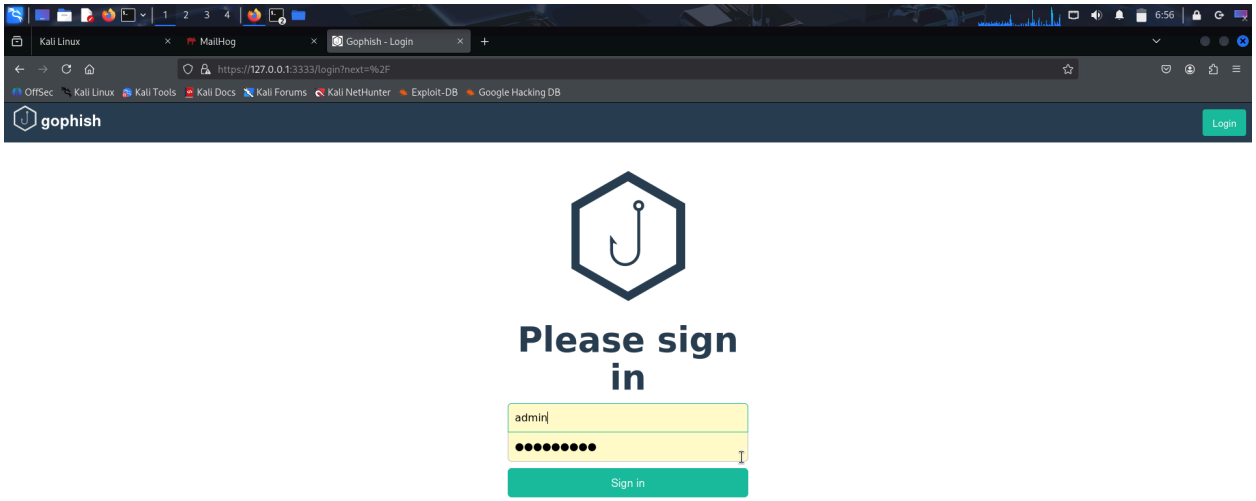
- Admin interface: https://localhost:3333
- Phishing server: http://localhost:80 (default)



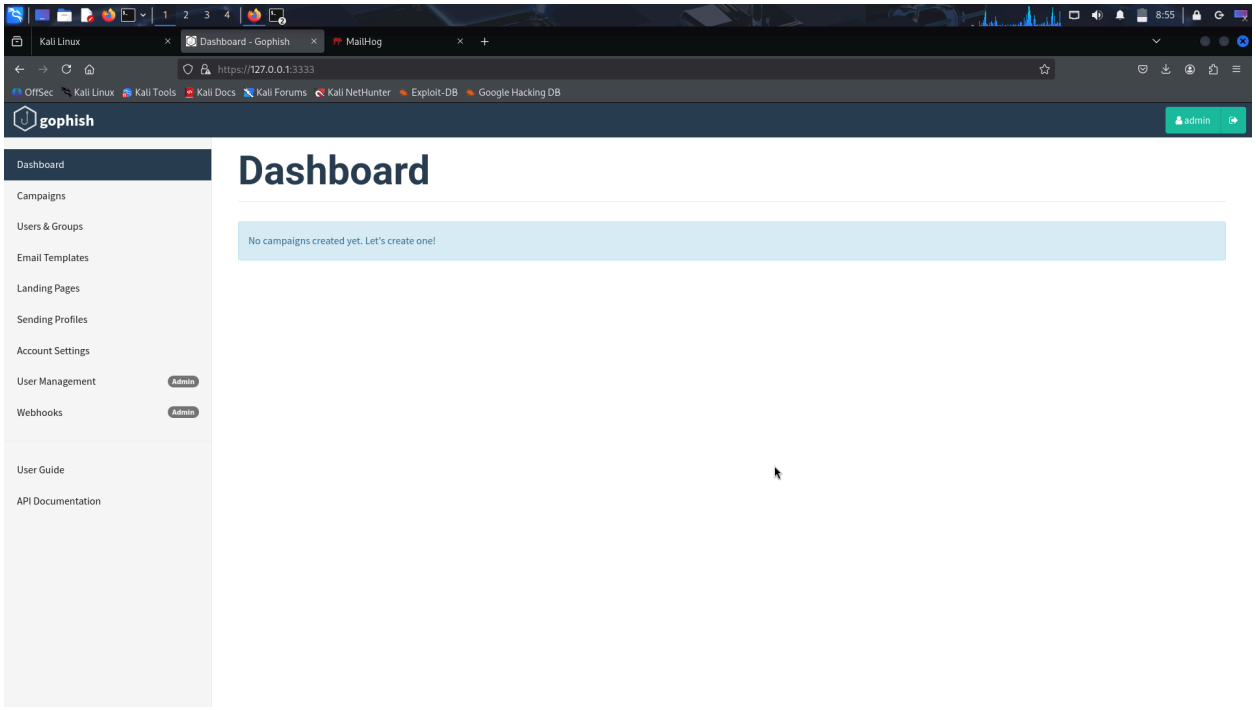
1.2 Gophish Running

Initial Login

- Open a web browser and navigate to https://localhost:3333
- Log in using the default credentials
- Change the default password immediately after login



1.3 Gophish login page



1.4 Gophish dashboard after successful login

5.3 SMTP Configuration

To send phishing emails, Gophish requires an SMTP sending profile.

SMTP Options

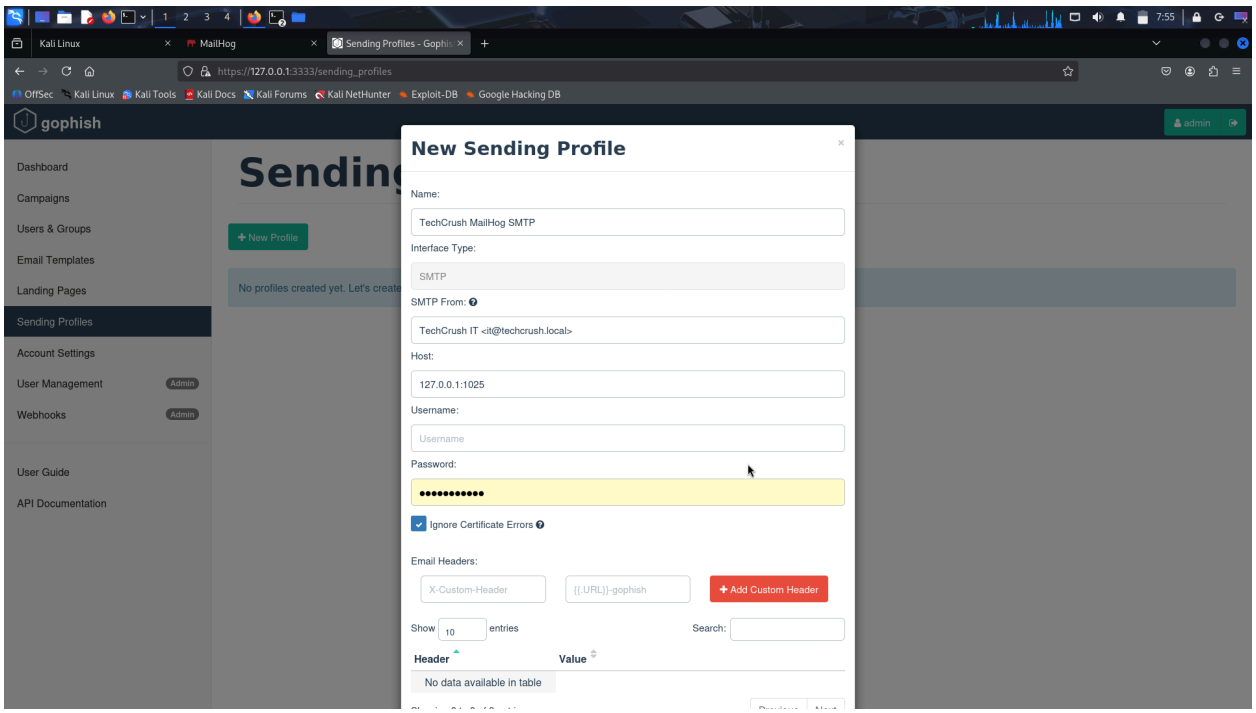
If a corporate mail server is unavailable, one of the following can be used:

- Sandbox SMTP service
- Test mail server
- Email testing platform

SMTP Configuration Details

The following parameters were configured:

- SMTP Server Address: http://127.0.0.1
- Port: 1025
- Authentication Enabled: Yes
- Sender Email Address: it@techcrush.local



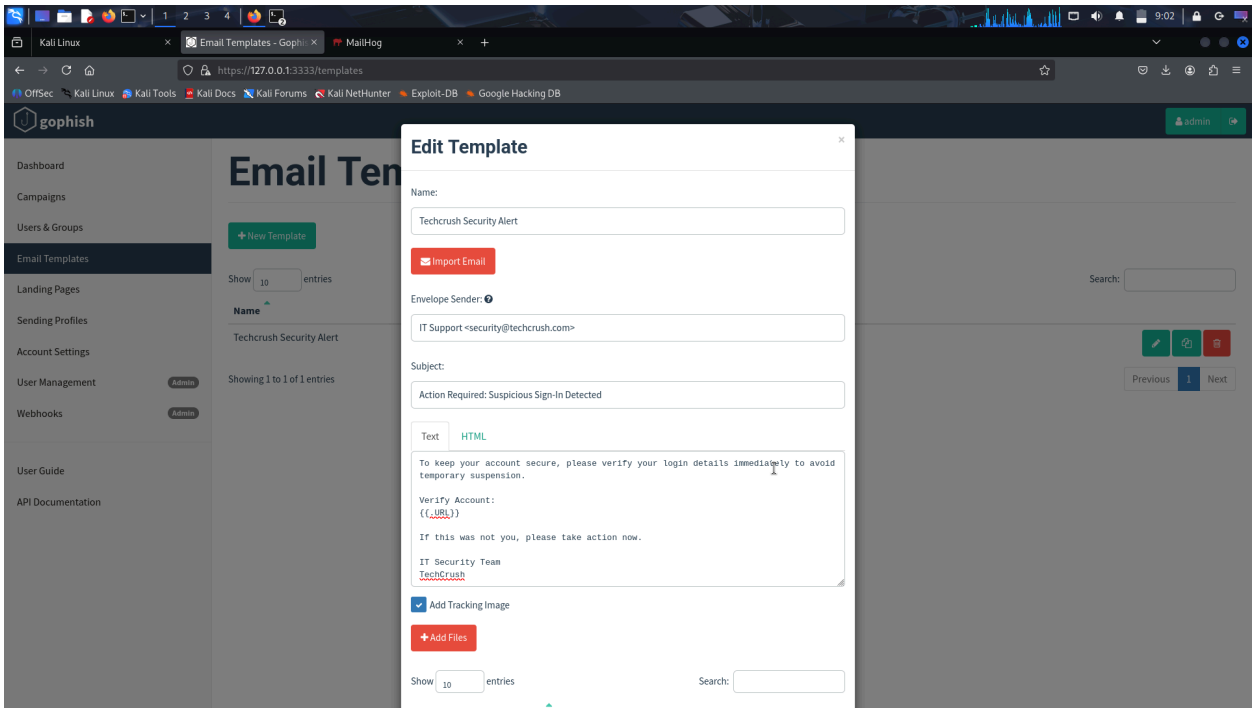
1.5 Sending Profile configuration screen

5.4 Template Creation

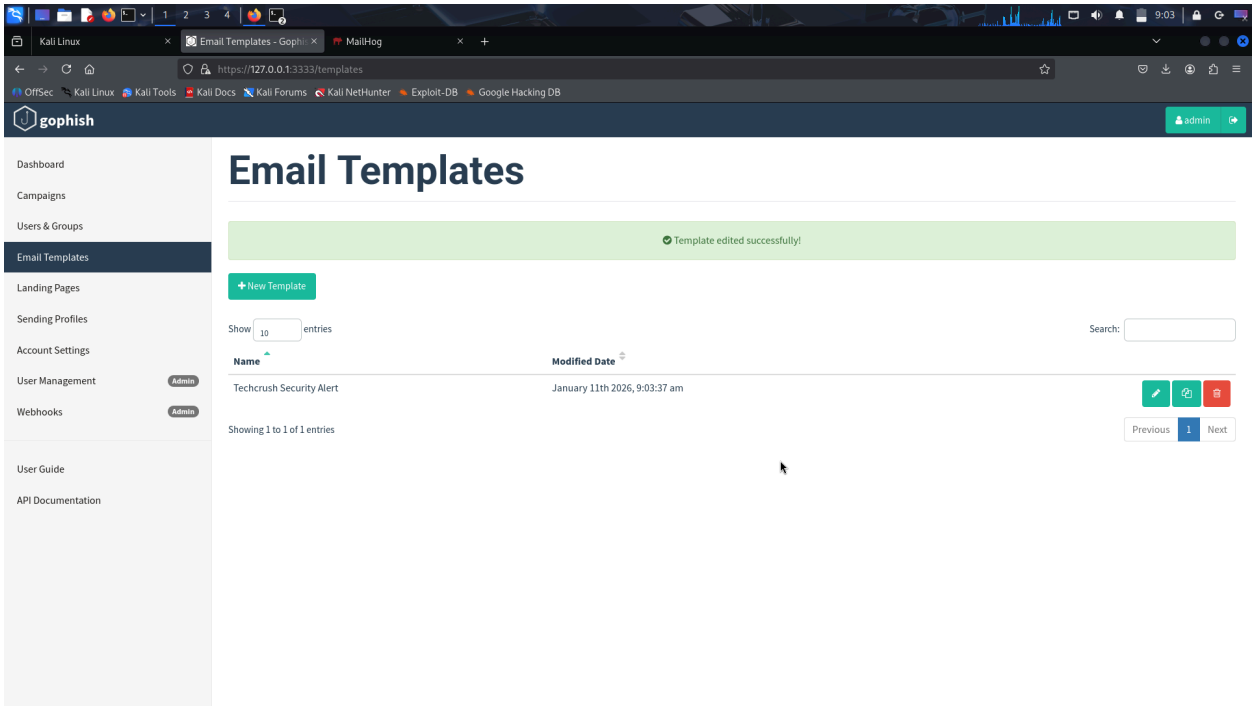
Email Template

A phishing email template was created to simulate a legitimate internal security message. The message was designed to appear realistic while remaining non-malicious.

Example theme:
“Security Update Required – Please Verify Your Account”



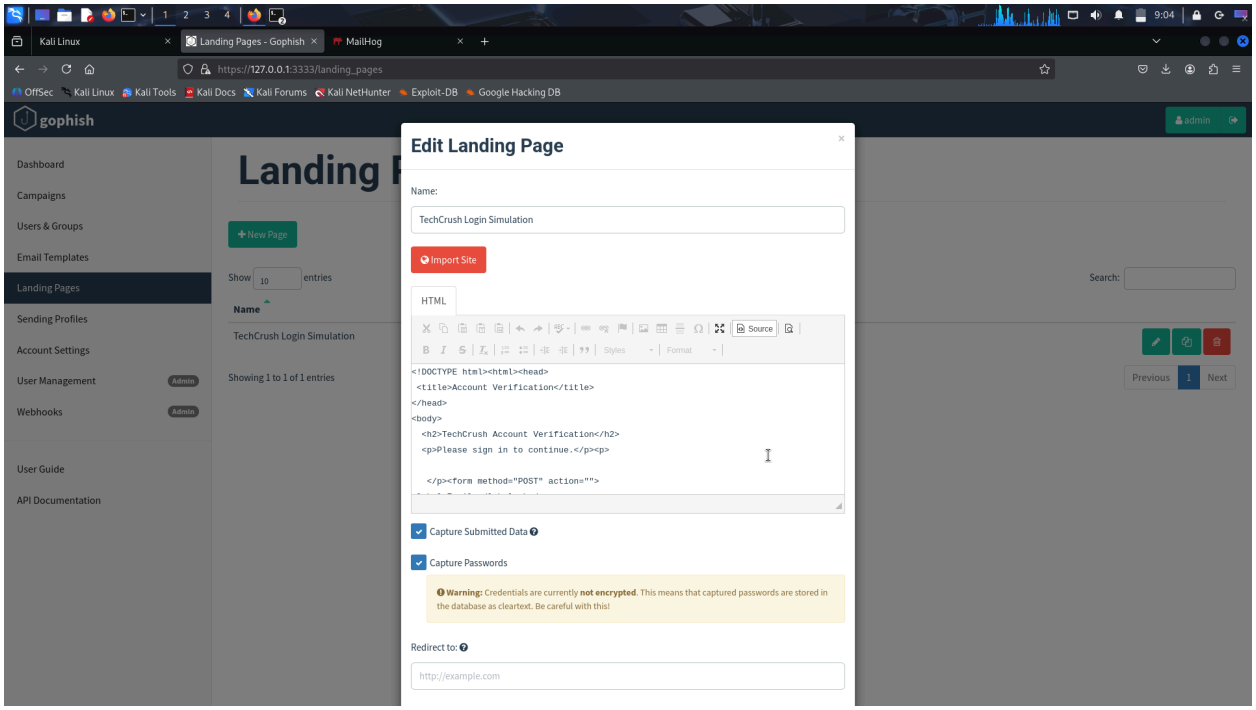
1.6 Email template editor



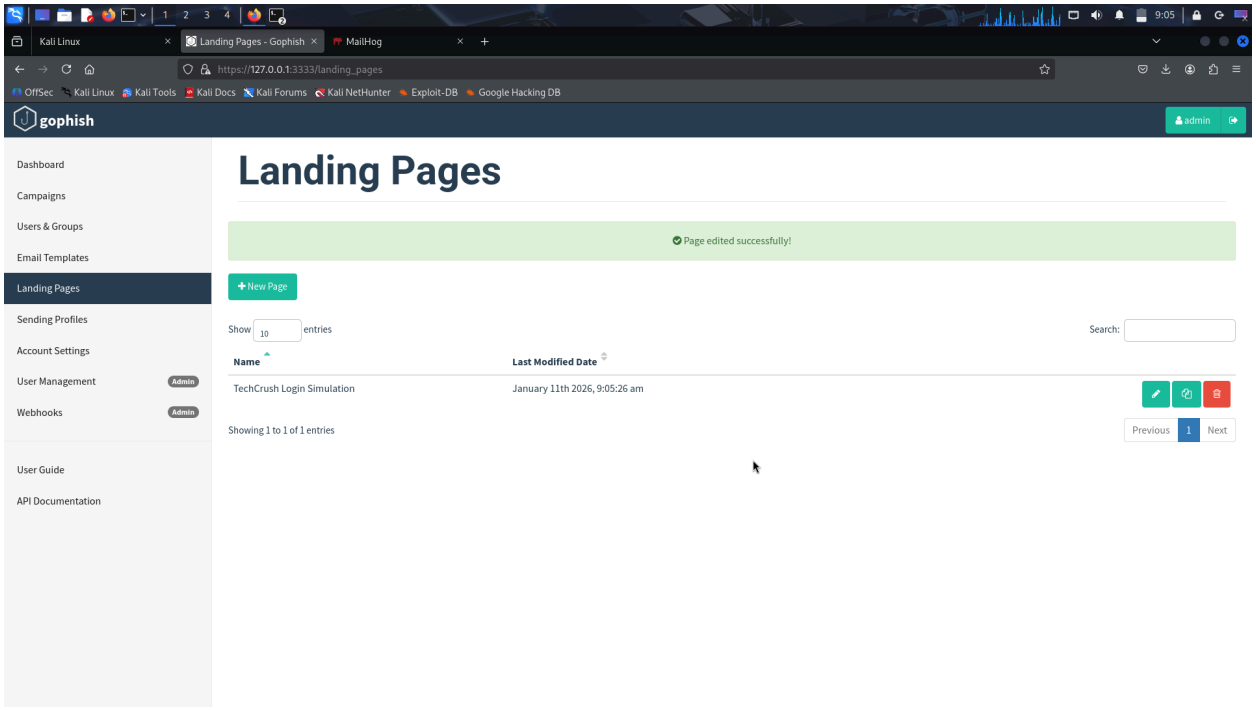
1.7 Saved email template

Landing Page

A simulated login page was created to capture user interaction. The page mimics a login form but does not validate or store real credentials.



1.8 Landing page editor



1.9 Saved landing page

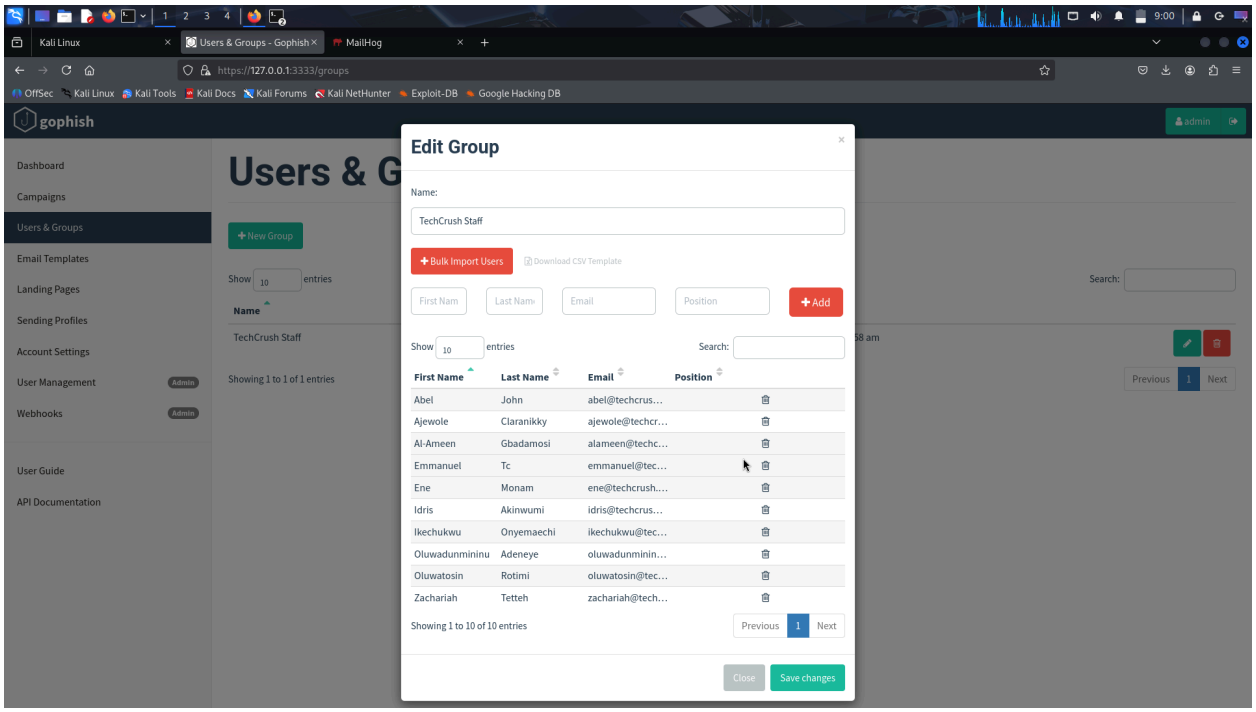
5.5 Importing Target List

Target CSV File

Targets were imported using a CSV file with the following format:

email,first_name,last_name
user1@techcrush.com,John,Doe
user2@techcrush.com,Jane,Smith

The file represents Tech Crush staff participating in the simulation.



2.0 Target group created and populated

5.6 Summary

At the completion of this step, Gophish was fully installed and configured with:

- A functioning admin dashboard
- A configured SMTP sending profile
- Phishing email and landing page templates
- An imported target list ready for campaign launch

6. Launch the Simulation

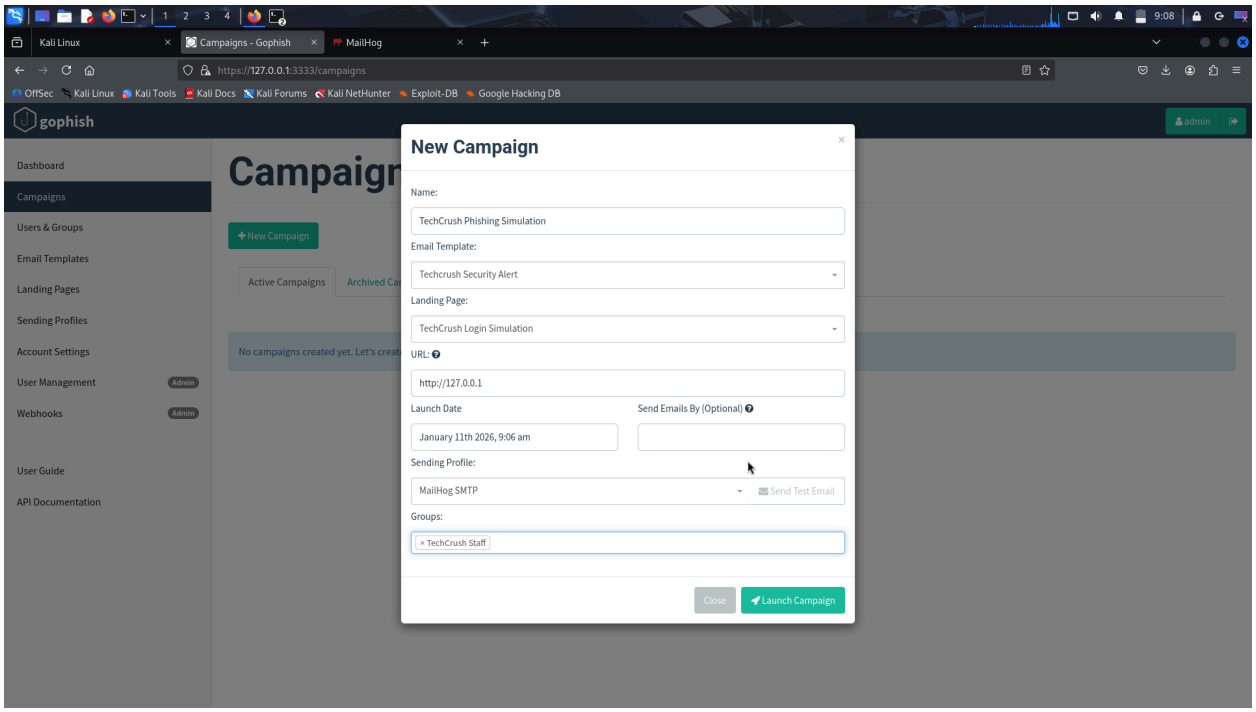
After completing the installation and configuration of Gophish, a phishing simulation campaign was created and launched to assess user awareness within Tech Crush.

Campaign Creation

A new campaign was created in the Gophish dashboard by linking the following components:

- **Email Template**: Simulated security notification email
- **Sending Profile**: Configured SMTP profile
- **Landing Page**: Simulated login page
- **Target Group**: Imported Tech Crush staff email list

Each component was verified to ensure proper configuration prior to launch.

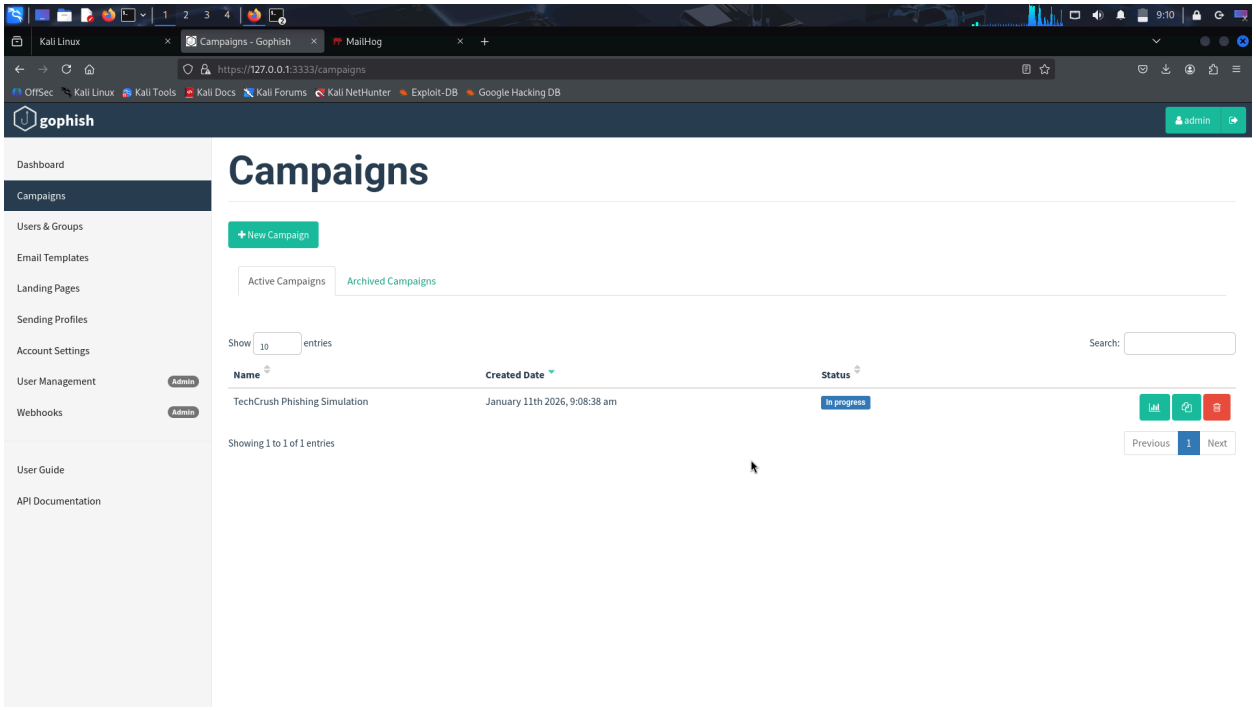


2.1 Campaign creation screen showing all selected components

Campaign Launch

Once all settings were confirmed, the campaign was launched from the Gophish dashboard.

- Campaign start time was recorded
- The campaign was configured to run for 24–48 hours
- Emails were sent automatically to all targets



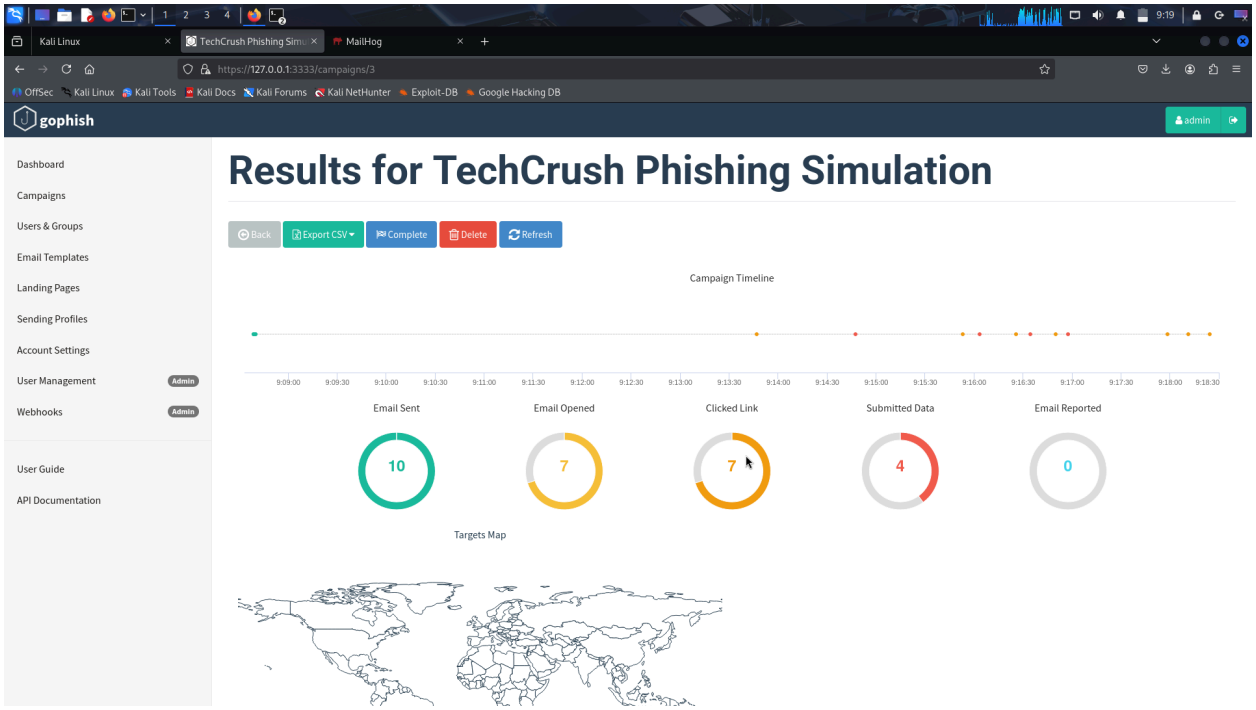
2.2 Campaign dashboard immediately after launch

Monitoring the Campaign

During the active campaign period, the Gophish dashboard was used to monitor user interaction in real time. The following metrics were observed:

- Number of emails sent
- Number of emails opened
- Number of links clicked
- Number of credential submissions (simulated)

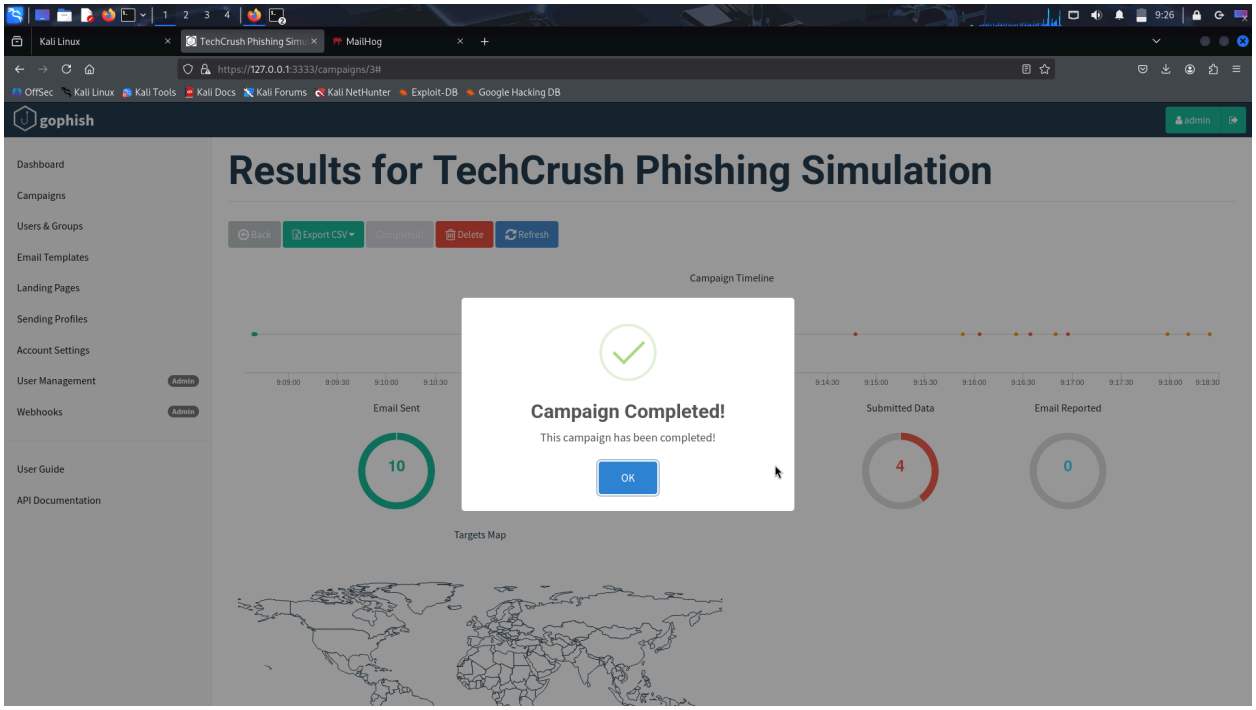
Monitoring was performed without intervening or modifying campaign settings.



2.3 Real-time campaign statistics

Campaign Completion

After the campaign period ended, final results were reviewed and recorded. These results form the basis for the analysis presented in later sections of this report.



2.4 Final campaign results dashboard

Summary

The phishing simulation campaign was successfully launched and monitored using Gophish. User interaction data was collected in a controlled and ethical manner, enabling accurate assessment of phishing awareness within Tech Crush.

7. Tracking Results & Analytics

After the phishing simulation campaign concluded, the results were reviewed and analyzed using Gophish's built-in reporting and export features. The collected data provides insight into user behavior and phishing awareness within Tech Crush.

Metrics Collected

Gophish automatically tracked the following key metrics during the campaign:

- **Total Emails Sent** — Number of phishing emails successfully delivered

- **Emails Opened** — Number of recipients who opened the phishing email
- **Links Clicked** — Number of recipients who clicked the phishing link
- **Credentials Submitted (Simulated)** — Number of recipients who attempted to enter login details on the landing page

These metrics were used to evaluate employee susceptibility to phishing attacks.

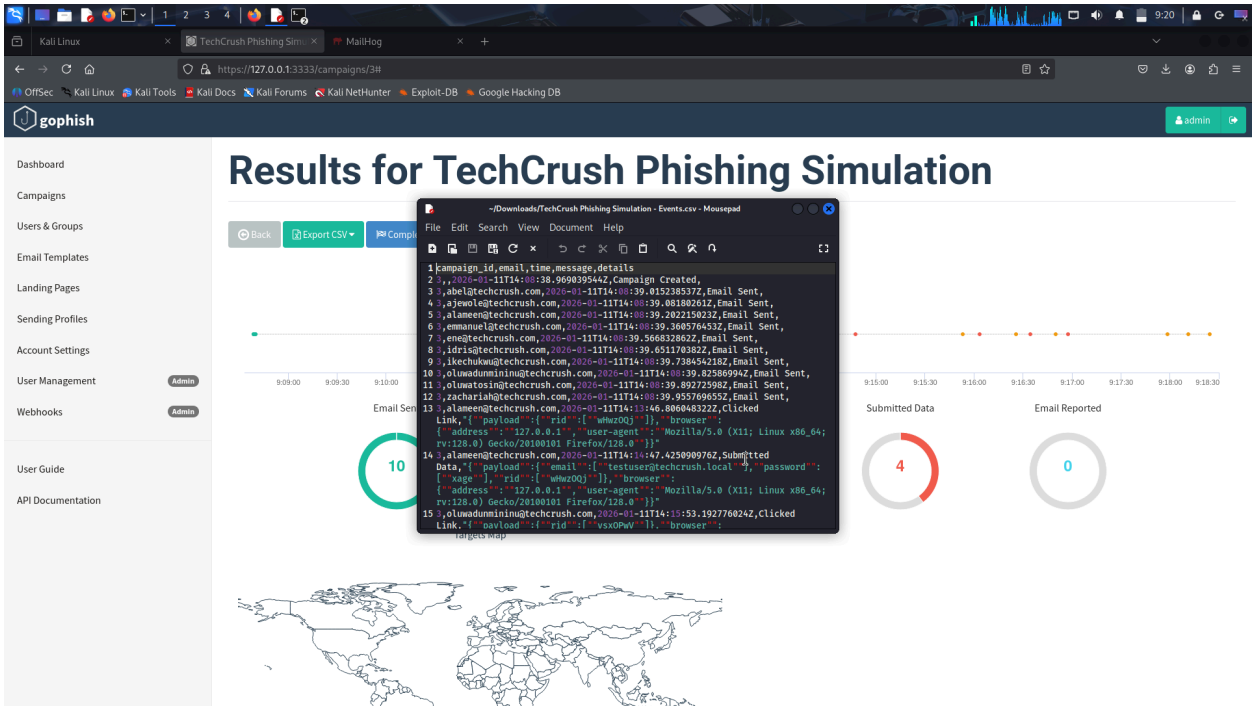
Results Collection

Results were reviewed directly from the Gophish campaign dashboard after the campaign ended. The platform provides both visual charts and numerical summaries. Campaign results dashboard showing final metrics

Data Export

To support reporting and analysis, the campaign results were exported from Gophish in CSV format. This allowed the data to be reviewed in spreadsheet software and used to generate tables and charts.
Exported data included:

- Individual target status
- Timestamped interactions
- Campaign-wide summary metrics



2.5 Export results option or downloaded CSV file

Results Summary

The following table format was used to summarize campaign results:

Metric	Count
Email Sent	10
Emails Opened	7
Links Clicked	7
Credentials Submitted(Simulated)	4

Observations

Initial analysis of the results indicated:

- A percentage of users interacted with the phishing email
- Some users proceeded beyond email interaction to click the embedded link
- A smaller subset attempted to submit credentials, indicating higher risk behavior

These observations highlight areas where additional security awareness training may be beneficial.

Summary

The tracking and analytics provided by Gophish enabled accurate measurement of user interaction throughout the phishing simulation. The exported data serves as the foundation for both technical analysis and executive-level reporting.