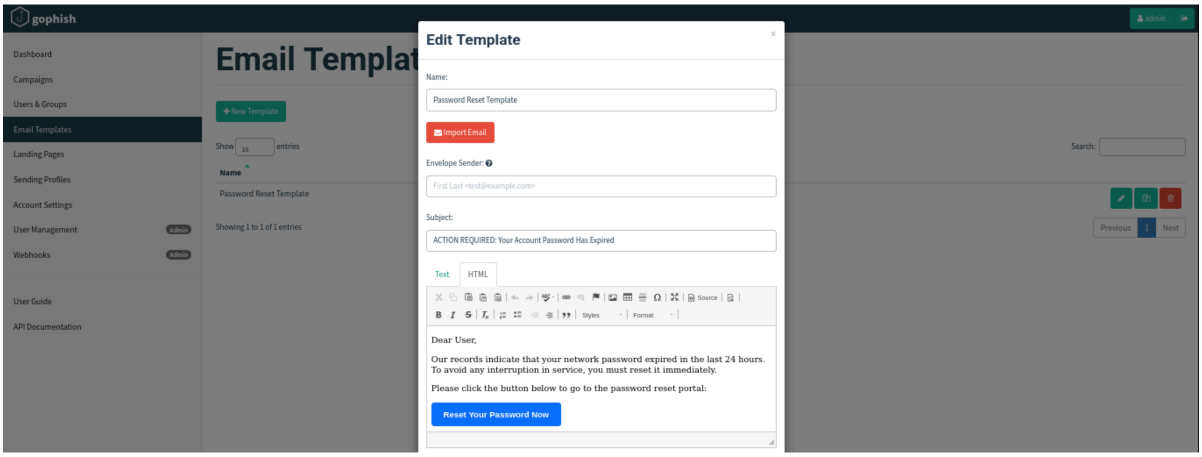
Report: Simulated Phishing Campaign Analysis

Executive Summary

- Objective: To simulate a basic password-harvesting phishing attack in a controlled educational environment to understand the mechanics and identify key defensive weaknesses.
- Methodology: A campaign was launched using the Gophish framework, targeting a single test user (myself).
- Key Finding: The simulation was 100% successful. The email was delivered, the link was clicked, and credentials were successfully captured. This demonstrates the high risk of credential-harvesting attacks, even simple ones.

Campaign Setup & Configuration



Edit Template

Name: Password Reset Template

Envelope Sender: First Last <test@example.com>

Subject: ACTION REQUIRED: Your Account Password Has Expired

Show 10 entries

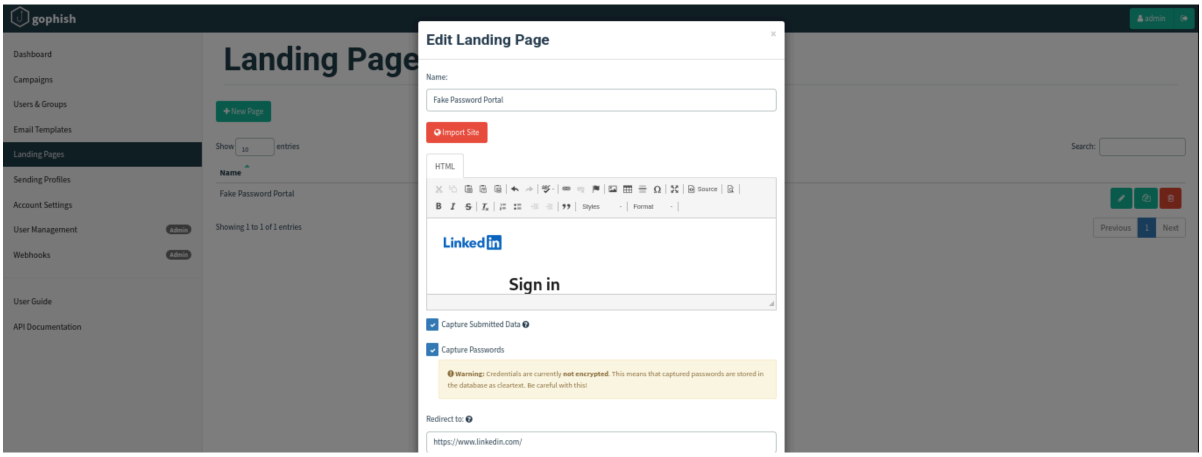
Name
Password Reset Template

Showing 1 to 1 of 1 entries

Dear User,

Our records indicate that your network password expired in the last 24 hours. To avoid any interruption in service, you must reset it immediately.

Please click the button below to go to the password reset portal:



Edit Landing Page

Name: Fake Password Portal

Show 10 entries

Name
Fake Password Portal

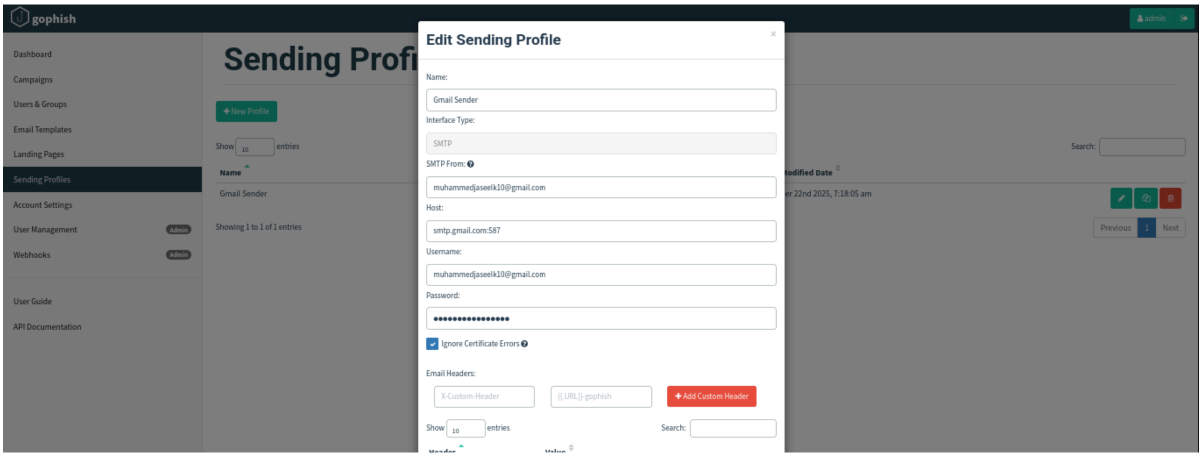
Showing 1 to 1 of 1 entries

☑ Capture Submitted Data

☑ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: https://www.linkedin.com/



Edit Sending Profile

Name: Gmail Sender

Interface Type: SMTP

SMTP From: muhammedjaseelk10@gmail.com

Host: smtp.gmail.com:587

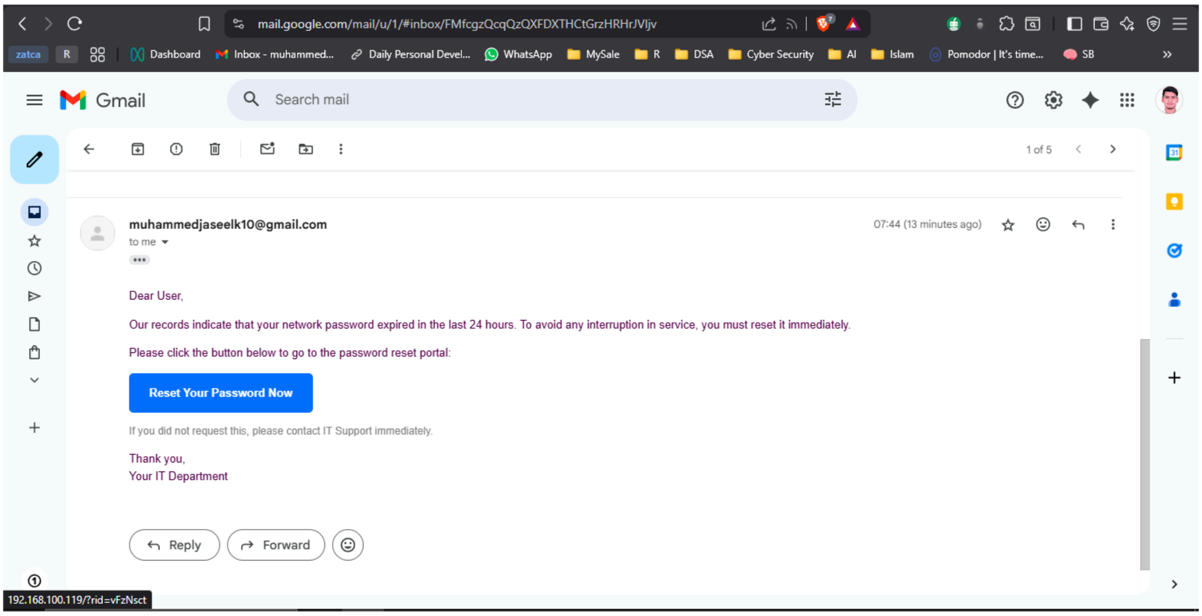
Username: muhammedjaseelk10@gmail.com

Password: ••••••••••••••••

☑ Ignore Certificate Errors

Email Headers: X-Custom-Header {{.URL}}-gophish

Execution & Results



muhammedjaseelk10@gmail.com
to me

07:44 (13 minutes ago)

Dear User,

Our records indicate that your network password expired in the last 24 hours. To avoid any interruption in service, you must reset it immediately.

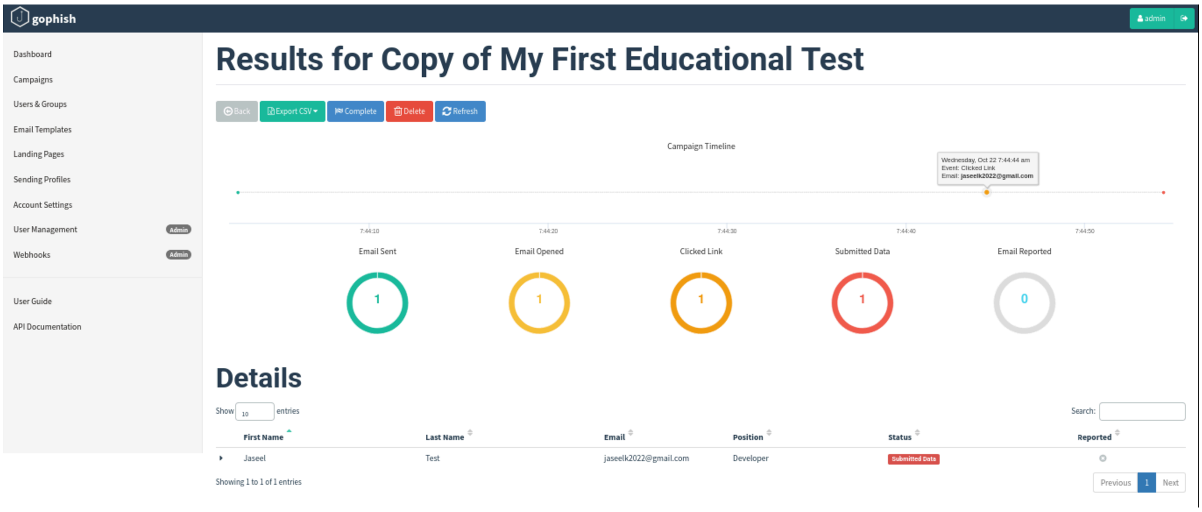
Please click the button below to go to the password reset portal:

Reset Your Password Now

If you did not request this, please contact IT Support immediately.

Thank you,
Your IT Department

192.168.100.119/?rid=vFzNsct



Results for Copy of My First Educational Test

Wednesday, Oct 22 7:44:44 am
Event: Clicked Link
Email: jaseelk2022@gmail.com

Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported
1	1	1	1	0

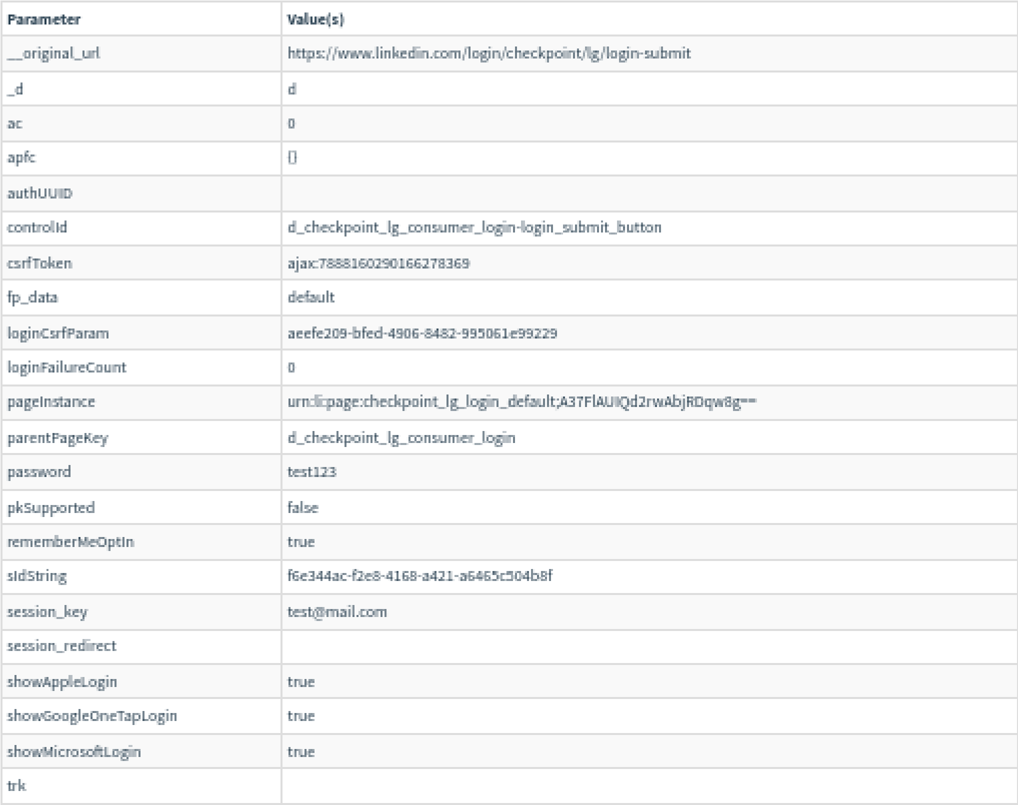
Details

Show 10 entries

Search:

First Name	Last Name	Email	Position	Status	Reported
Jaseel	Test	jaseelk2022@gmail.com	Developer	Submitted Data	⊗

Showing 1 to 1 of 1 entries



Parameter	Value(s)
__original_url	https://www.linkedin.com/login/checkpoint/lg/login-submit
_d	d
ac	0
apfc	{}
authUUID	
controlId	d_checkpoint_lg_consumer_login-login_submit_button
csrfToken	ajax:7888160290166278369
fp_data	default
loginCsrfParam	aeefe209-bfed-4906-8482-995061e99229
loginFailureCount	0
pageInstance	urn:li:page:checkpoint_lg_login_default;A37FlAUIQd2rwAbjRDqw8g==
parentPageKey	d_checkpoint_lg_consumer_login
password	test123
pkSupported	false
rememberMeOptIn	true
sIdString	f6e344ac-f2e8-4168-a421-a6465c504b8f
session_key	test@mail.com
session_redirect	
showAppleLogin	true
showGoogleOneTapLogin	true
showMicrosoftLogin	true
trk	

Analysis & Defensive Recommendations

Analysis: The attack was successful because it relied on social engineering (a sense of urgency) and a cloned website that looked legitimate. The "victim" (me) clicked the link and entered credentials without verifying the URL.

Defensive Recommendations:

1. User Training: This simulation proves that users should be trained to always hover over links to check the destination URL before clicking.
2. Email Filters: Better email security gateways could potentially block emails with links to raw IP addresses or newly registered domains.
3. Two-Factor/Multi-Factor Authentication (2FA/MFA): This is the single most effective defense. Even though the attacker (me) successfully stole the password, I would still be unable to log in to the real LinkedIn without the 2FA code from the user's phone.