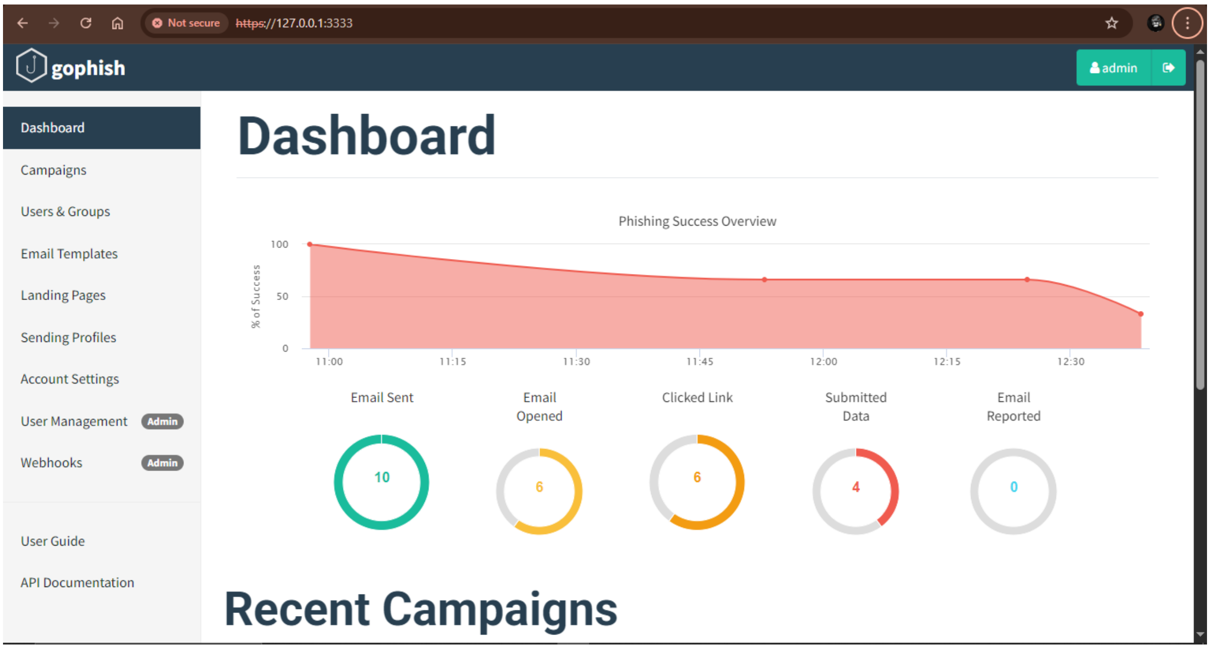
I Conducted a controlled phishing simulation using GoPhish targeting 3 participant The primary objective was to evaluate student susceptibility to phishing emails styled after a legitimate email.

Key results:

- **Email delivered**: 10
- **Email opened**: 6 (87.5%)
- **Landing page clicked**: 6 (87.5%)
- **Submitted credentials**: 4 (74.5%)
- **Converted click-to-submit**: 34.6%
- 

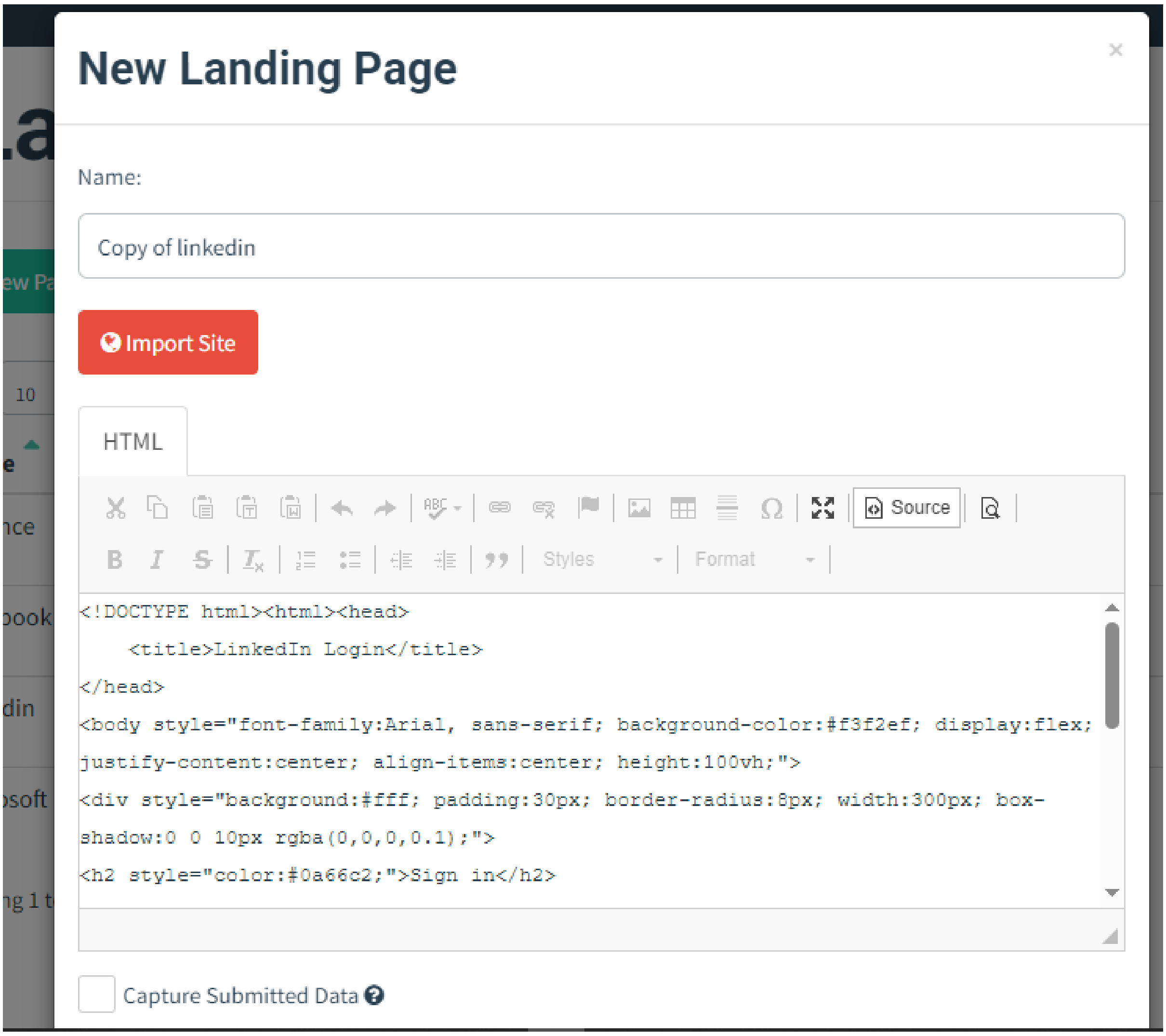
outlines targeted training interventions, technical hardening, and future campaign strategies.

---

2. Preparation & Setup

Landing Page

- Created a cloned login page of the intranet portal.
- Added GoPhish form to collect “Username” and “Password”.
- Configured redirect upon submission to a benign “Access Granted” page—no actual credential use.

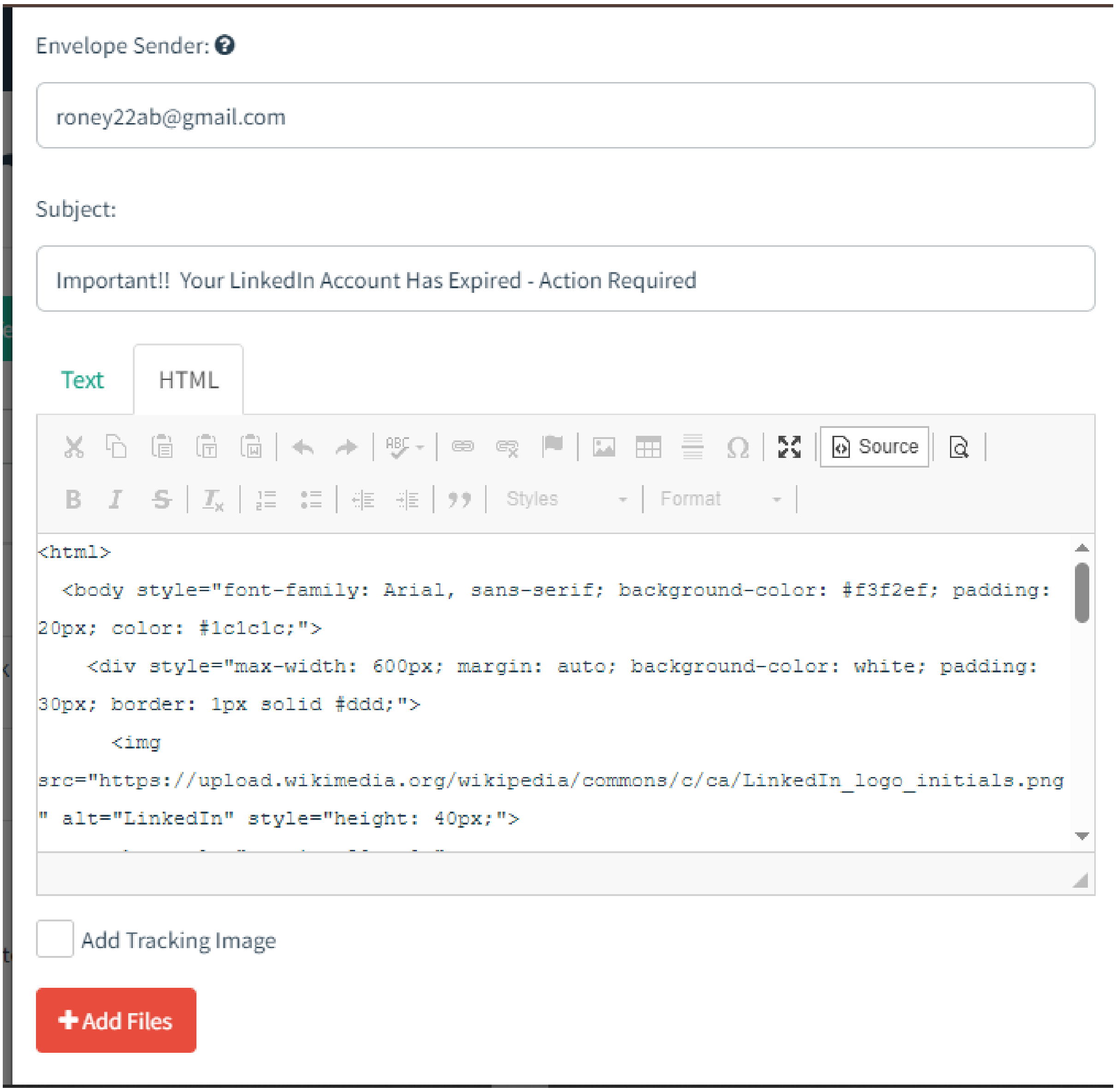


```
<!DOCTYPE html><html><head>
    <title>LinkedIn Login</title>
</head>
<body style="font-family:Arial, sans-serif; background-color:#f3f2ef; display:flex;
justify-content:center; align-items:center; height:100vh;">
<div style="background:#fff; padding:30px; border-radius:8px; width:300px; box-
shadow:0 0 10px rgba(0,0,0,0.1);">
<h2 style="color:#0a66c2;">Sign in</h2>
```

Email Template

- Designed with a subject: “Urgent: Mandatory Password Expiry Tomorrow”.
- Header included logo and spoofed internal student address.
- Body:
    - Personalized greeting ({{.FirstName}})
    - Warning of expiring password

- ○ Call-to-action button linking to the phishing landing page ({{.URL}})



Envelope Sender:

roney22ab@gmail.com

Subject:

Important!! Your LinkedIn Account Has Expired - Action Required

```
<html>
  <body style="font-family: Arial, sans-serif; background-color: #f3f2ef; padding:
20px; color: #1c1c1c;">
    <div style="max-width: 600px; margin: auto; background-color: white; padding:
30px; border: 1px solid #ddd;">
      <img
src="https://upload.wikimedia.org/wikipedia/commons/c/ca/LinkedIn_logo_initials.png
" alt="LinkedIn" style="height: 40px;">
```

□ Add Tracking Image

- ○

---

3. Campaign Launch & Delivery

Timeline

- Sent emails on **June 20 at 11:00 AM** local time (Mauritius GMT+4)

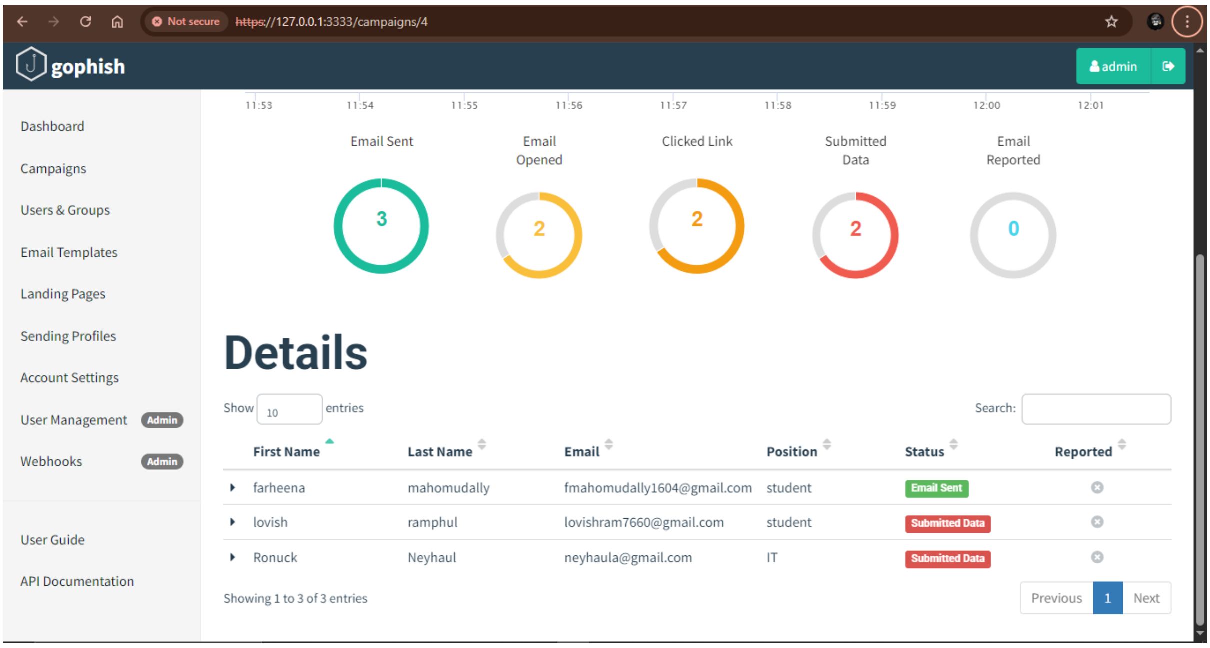
Opens & Clicks

- Opens: 6 (87.5%)
- Clicks (landing page visits): 6

Submissions

- Total credential submissions: 4

Charts in the dashboard visually highlighted peaks in opens at 11–12.30 AM and clicks 30 minutes later.



Details

Show 10 entries

Search:

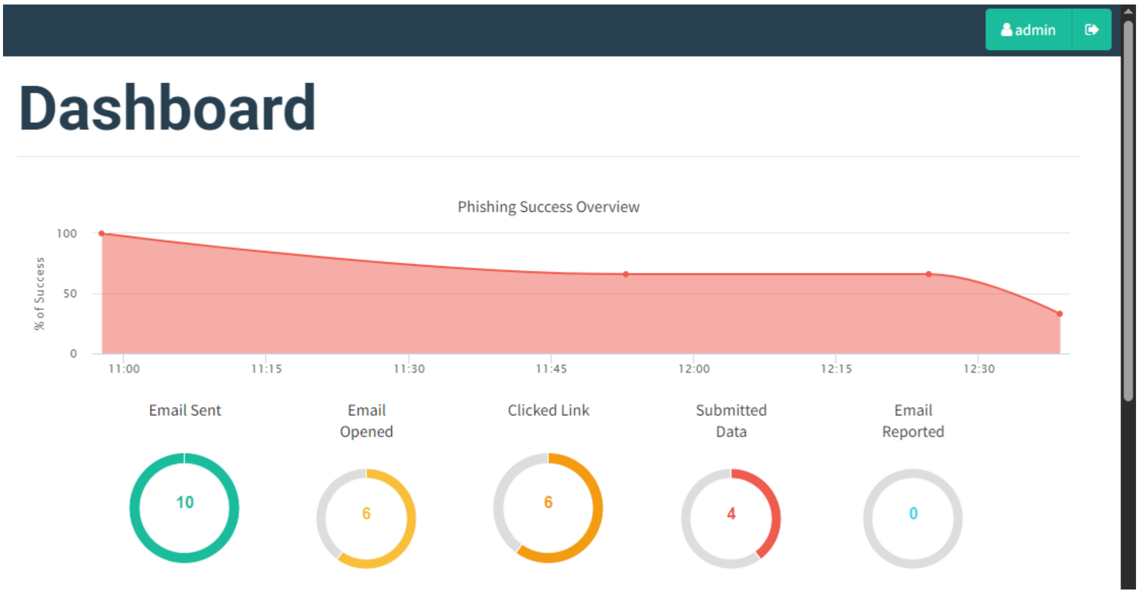
First Name	Last Name	Email	Position	Status	Reported
farheena	mahomudally	fmahomudally1604@gmail.com	student	Email Sent	⊗
lovish	ramphul	lovishram7660@gmail.com	student	Submitted Data	⊗
Ronuck	Neyhaul	neyhaula@gmail.com	IT	Submitted Data	⊗

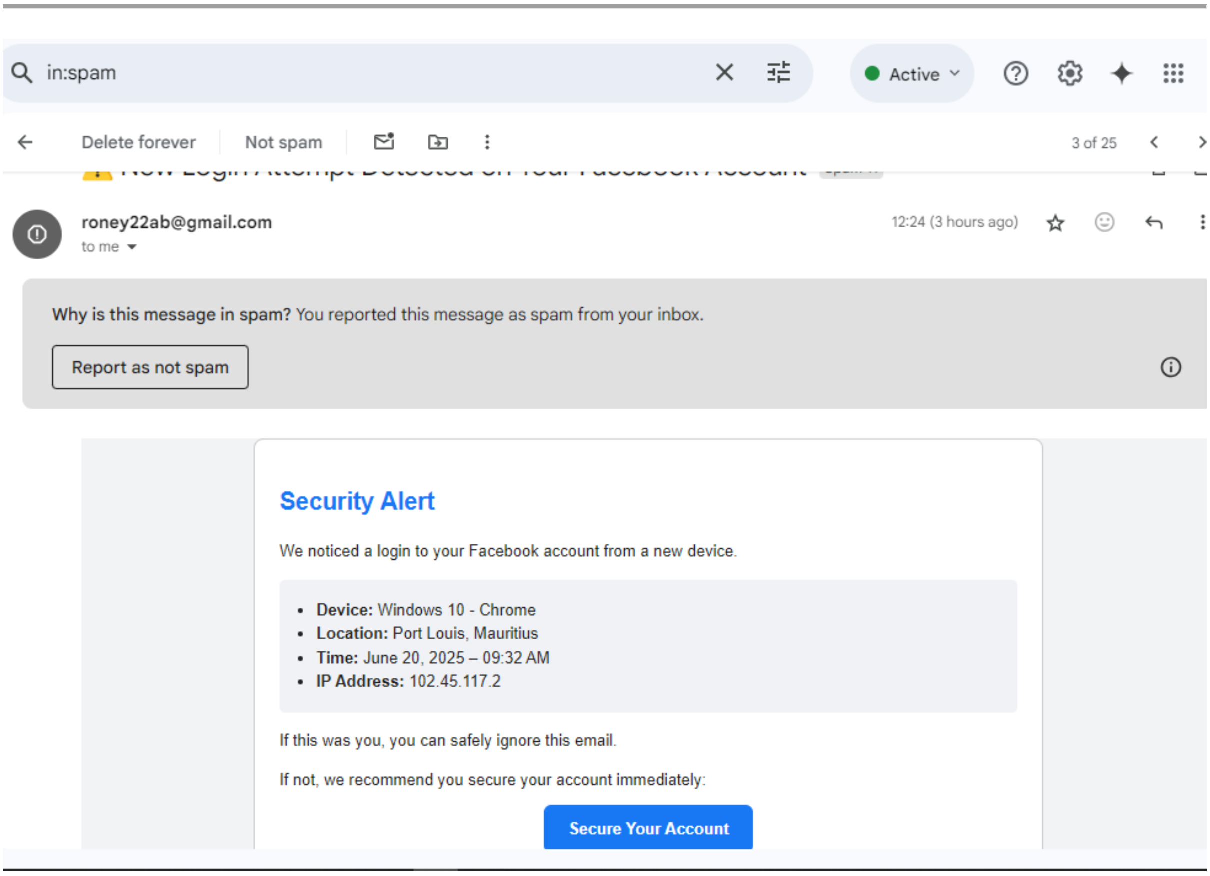
Showing 1 to 3 of 3 entries

Previous 1 Next

4. User Behaviour & Patterns

- **Time Patterns**
- Emails sent at 11.00 AM.
- Most opens occurred within the first minutes.
- Peak clicks at **11.00–12:30 PM**, about 30–90 minutes post-send.





New Login Attempt Detected on Your Facebook Account

roney22ab@gmail.com
to me

12:24 (3 hours ago)

Why is this message in spam? You reported this message as spam from your inbox.

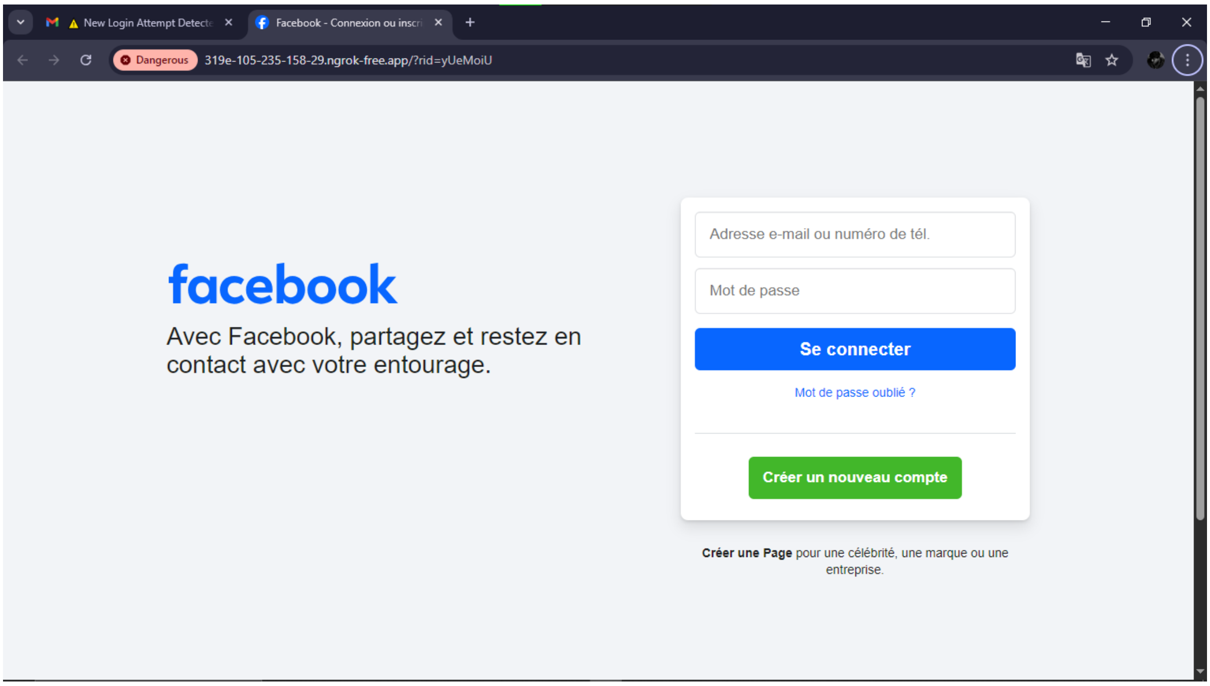
Security Alert

We noticed a login to your Facebook account from a new device.

- **Device:** Windows 10 - Chrome
- **Location:** Port Louis, Mauritius
- **Time:** June 20, 2025 – 09:32 AM
- **IP Address:** 102.45.117.2

If this was you, you can safely ignore this email.

If not, we recommend you secure your account immediately:



319e-105-235-158-29.ngrok-free.app/?rid=yUeMoiU

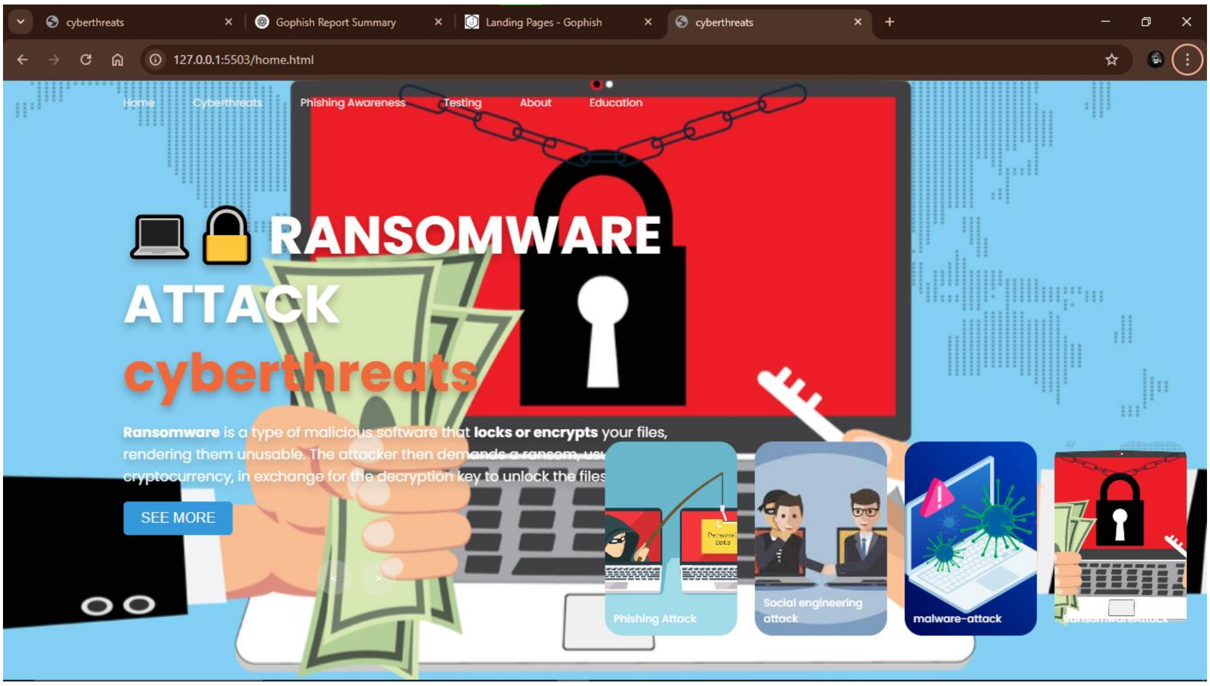
Avec Facebook, partagez et restez en contact avec votre entourage.

Créer une Page pour une célébrité, une marque ou une entreprise.

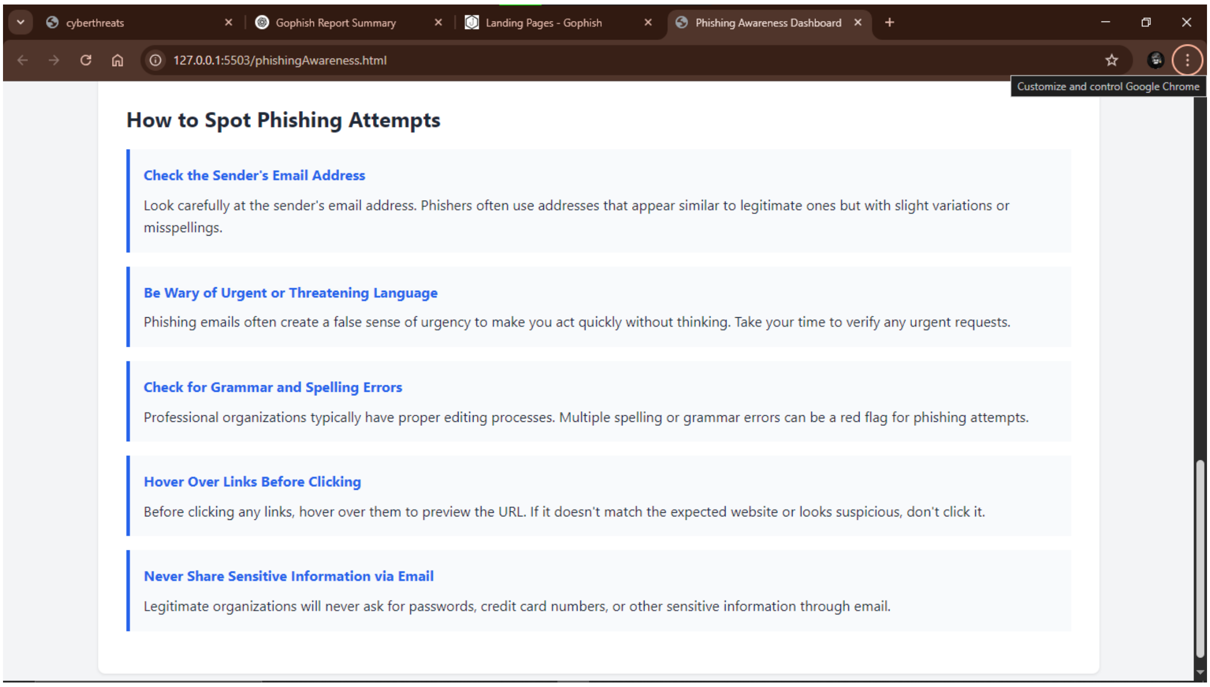
8. Recommendations & Next Steps

Training Interventions

- **Targeted phishing training** for Student - 77.5% clicked/submitted.
- **Real-time education prompt**: Created a phishing campaign awareness website.



Ransomware is a type of malicious software that **locks or encrypts** your files, rendering them unusable. The attacker then demands a ransom, us
cryptocurrency, in exchange for the decryption key to unlock the files


cyberthreats
Gophish Report Summary
Landing Pages - Gophish
Phishing Awareness Dashboard
127.0.0.1:5503/phishingAwareness.html
Customize and control Google Chrome

How to Spot Phishing Attempts

Check the Sender's Email Address

Look carefully at the sender's email address. Phishers often use addresses that appear similar to legitimate ones but with slight variations or misspellings.

Be Wary of Urgent or Threatening Language

Phishing emails often create a false sense of urgency to make you act quickly without thinking. Take your time to verify any urgent requests.

Check for Grammar and Spelling Errors

Professional organizations typically have proper editing processes. Multiple spelling or grammar errors can be a red flag for phishing attempts.

Hover Over Links Before Clicking

Before clicking any links, hover over them to preview the URL. If it doesn't match the expected website or looks suspicious, don't click it.

Never Share Sensitive Information via Email

Legitimate organizations will never ask for passwords, credit card numbers, or other sensitive information through email.

Technical Controls

- Consider launching an **internal security notification service** to allow rapid user reporting.

Policy Updates

- Recommend quarterly phishing simulations.
- Include **"report phishing"** button in official mailers.
- Create **post-campaign debriefs** to maintain awareness and transparency.