

Phishing Simulation Platform

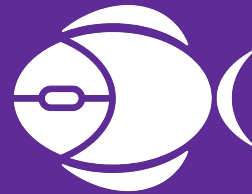
Presented by

Data Analysts

David Anselot
Patrycja Schaefer
Nicole Pretorius
Thérèse De Backer

Data Engineers

Edoardo Lai
Tumi Modiba
Miro Fronhoffs

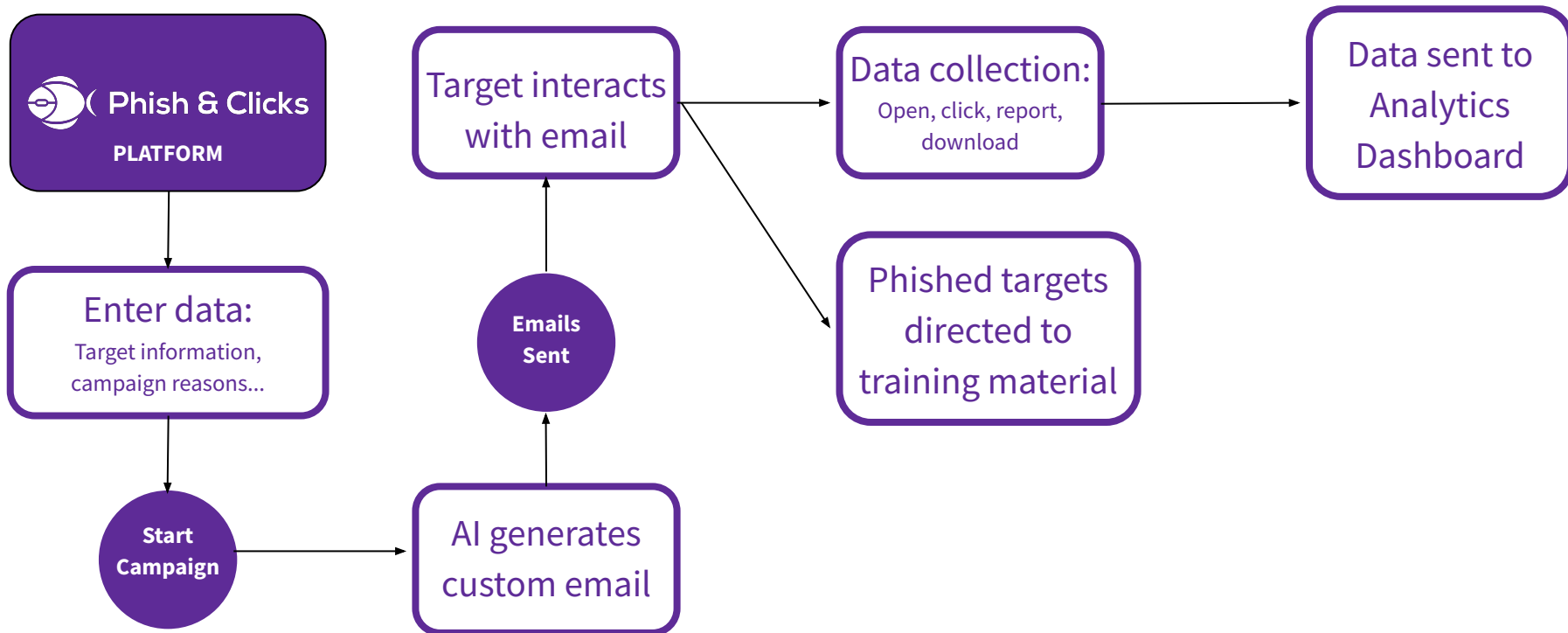


Phish & Clicks

Our Solution

PATRYCJA

User Flow



Challenges & Limitations

- ✦ GoPhish
 - Attaching tracker events to emails
- ✦ “Open” tracking event blocked when running database locally
 - Attachment download tracking limitations
 - Render deployment and database limitations

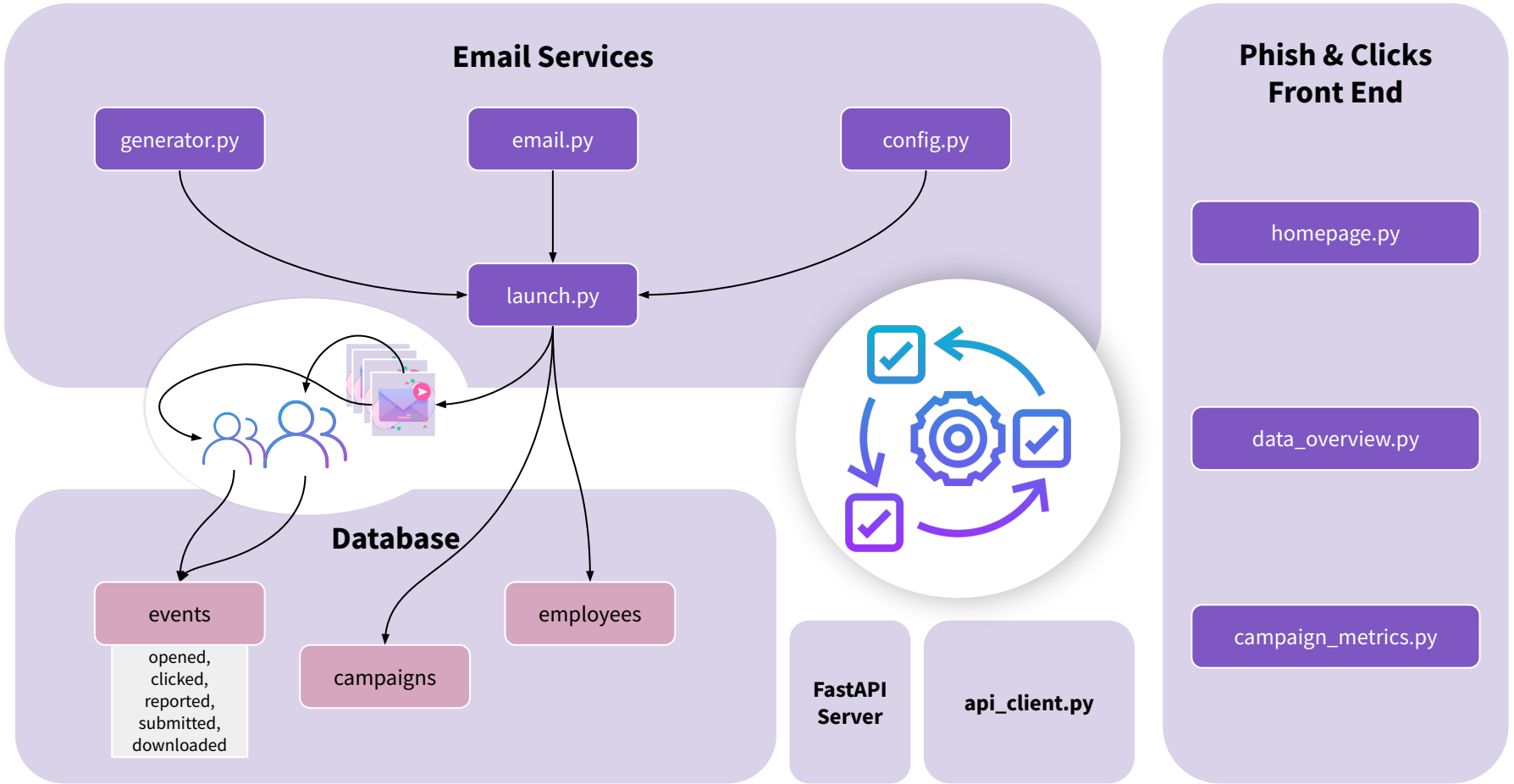
Our Solution

Architecture

- ✦ Back-end (API and Postgres.db)
- Front-end (Streamlit-UI layer)
- Email Services

Tools

- Fast API
 - ✦ Pydantic (Request/Response validation)
 - SQLAlchemy(ORM)
 - Google Gemini API
 - Matplotlib
 - ✦ Streamlit
 - Render (Postgres & FastAPI hosting)
-



Email Services

generator.py

email.py

config.py

launch.py

Deployment

Database

events

employees

campaigns

FastAPI
Server

api_client.py

Phish & Clicks Front End

homepage.py

data_overview.py

campaign_metrics.py



Personalization

NICOLE

- Names
- Business Unit
- Language
- Reasoning
- Links

Prompt Engineering

Compose a professional email in **{language}** from **{sender name}** to **{receiver name}** from the **{Team Name}** team. The email should address the following topic: **{reason}**.

The email should include the following elements:

1. A clear explanation of why **{reason}** is critical, with specific consequences if no action is taken.
2. A specific call to action requiring the recipient to click this link: “{pretty link}”
3. Include a deadline with a **{future date}** and **{random time}** in the near-future, excluding weekends.
- ✦ 4. Ensure the tone is professional and not overly alarming to avoid suspicion.

Remember to:

- Use realistic and natural-sounding language throughout, avoiding repetitive or template-like phrases.
- ✦ - Keep the tone professional and approachable, like a helpful colleague.
- Make the email appear tailored specifically for the recipient **{name} {surname}**.
- ✦ - Format the result as an HTML body text with only <p> tags to subdivide in paragraphs.
- Format the date and time between tags to highlight it.
- Only write the body of the email. Do not include headers or signatures.

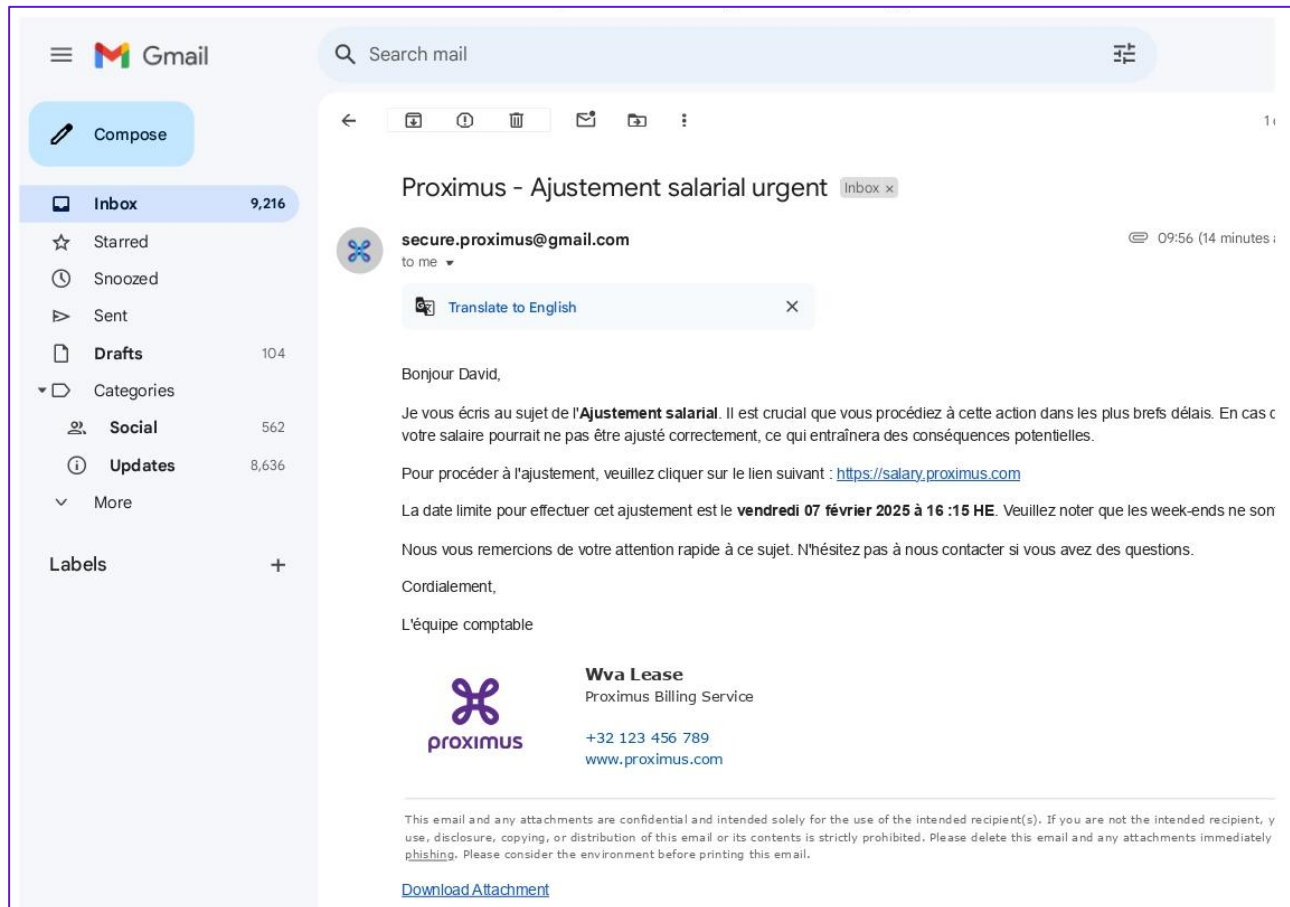
Result

Brand spoofing

No over the top styling

Employee to employee

In real-life context -
would be modeled after
internal emails.



Training

Materials:

11-page Guide

Email content

Quiz

Follow-up:

Immediate feedback

Scoring system (future)

12 → Can you identify the red flags in this phishing email?

Choose all that apply.

Choose as many as you like

- ☐ A Generic greeting
- ☐ B Sender's email does not match the organization
- ☐ C Suspicious Link(s)
- ☐ D Suspicious attachment(s)
- ☐ E Threatening tone / Sense of urgency
- ☐ F Request for immediate payment

LastPass Security Notice Inbox x

LastPass <LastPass@secure-monitor.com>
to me ▾

LastPass ****

Dear LastPass User,

We wanted to alert you that, recently, our team discovered and immediately blocked : on our network. Some user vault data was taken including email addresses and pass

To be sure that your information was NOT compromised, we have built [this secure w](#) can enter your last pass login information and we can tell you if your account was on compromised.

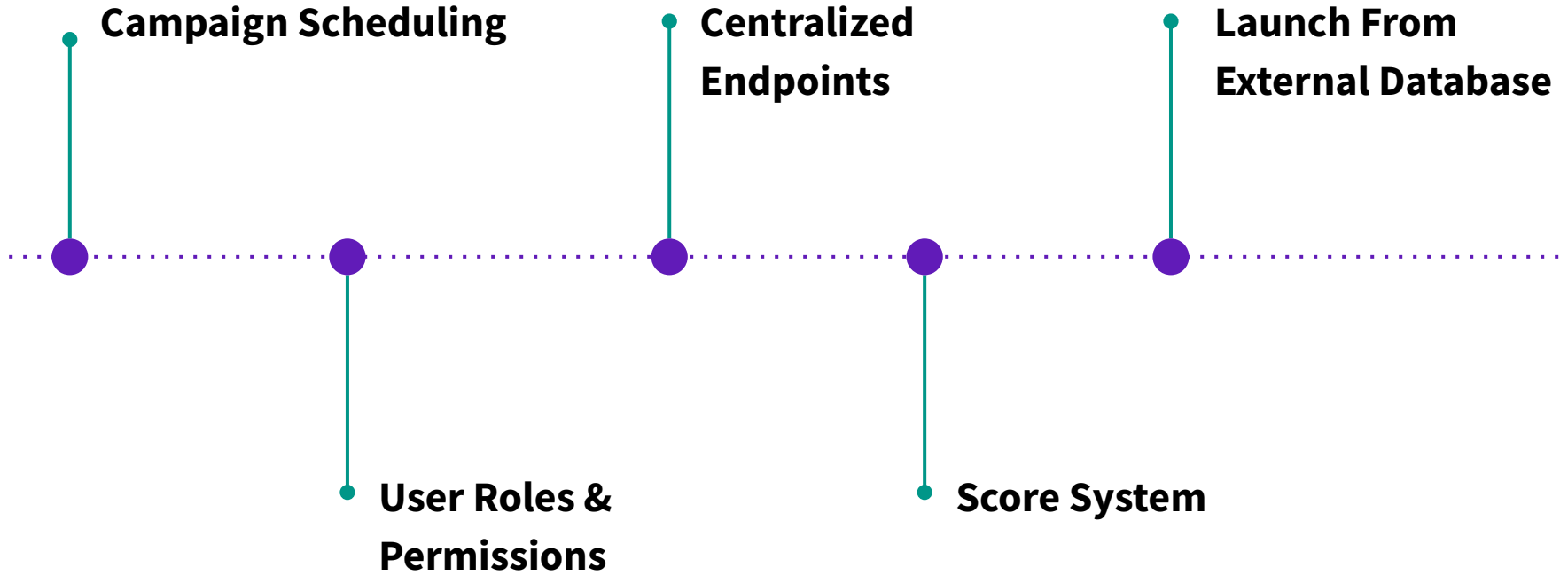
We apologize for the inconvenience, but ultimately we believe this will better protect I Thank you for your understanding, and for using LastPass.

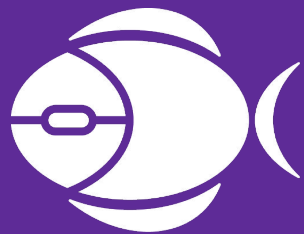
Regards,
The LastPass Team

[Learn More](#)

^ ▾  Powered by Typeform

Future Improvements





Phish & Clicks

DEMO