

TEAM 14 PRESENTS

HARTNELL PHISHING

By Kafui, Reign, Samer, Teddy & Ed



**\$3M LOST IN CALIFORNIA STATE
FUNDING (2024)**

\$10M LOST IN FEDERAL FUNDING (2024)

**\$350M+ LOST TO GHOST STUDENT
SCAMS (PAST 5 YEARS)**

ABC News, 2026

HARTNELL'S PHISHING PROBLEM

- Students receive phishing emails posing as:
 - Internship offers
 - Financial aid notices
 - College communications
- Every reported email required manual IT review



HARTNELL'S PHISHING PROBLEM

- Client expressed need for:
 - Identify phishing trends each month
 - Generate executive threat summaries
 - Create student & staff security alerts
 - Produce a monthly "Threat of the Month" newsletter

An Effective Solution

**SES/Comprehend: limited to benign vs. phishing
classification**

**A simpler Amazon S3 text-file workflow was more
effective.**

An Effective Solution

- **Interactive UI**
- **Direct connection to S3 buckets**
- **Easily print newsletters**
- **View top threats and most common**

The Data Pipeline

- **Browser upload triggers the Source S3 bucket**
- **S3 ObjectCreated event invokes the Python Lambda**
- **Lambda validates, parses, and classifies each row**
- **Deterministic insights and HTML drafts are rendered**
- **Immutable run artifacts land in the Drafts S3 bucket**
- **Results page and dashboard serve straight from S3**

HARTNELL COLLEGE · INFORMATION TECHNOLOGY

Security 411

Monthly phishing threat analysis & awareness drafts

UPLOAD REPORTED EMAILS

Drop a CSV file of reported phishing emails. The file should have two columns: **label** (PHISHING or BENIGN) and **text** (email body). Headers are optional. The pipeline will classify, analyse, and generate four audience-specific drafts automatically.



Drag & drop your CSV here
or click to browse

Selected: training_set.csv (69563.4 KB)

Generate Drafts

Takes ~30-60 seconds after upload.

This upload is complete and all four custom drafts are ready. 22,415 phishing messages were categorized.

GENERATED DRAFTS

Review each draft below. Open in a new tab, copy the HTML, or save to send manually.



Executive Summary

Ranked threat table for cabinet. Every category this period, volume & target audience.

Open



Student Email

Awareness bulletin for students. Top threats with student-specific guidance.

Open

Additional Features

Resource Considerations for a Complete Build

With a conventional development timeline, we would aim to deliver:

- **LLM integration**
- **Increased automation and transparency**
- **AWS domain automation (Amazon SES & Amazon Route 53)**
- **Improved customer convenience**

Next Steps

Considering the Importance of AI Governance & Explainability

We value clear AI explanations for reliability and safety. Future applications will consider:

- **Cybersecurity**
- **Privacy**
- **Citability**

Conclusion

Team 14's AI Utility will:

- **Automate email review, summarization, and threat reporting**
- **Save staff time each month**
- **Demonstrate Customer Obsession by reducing manual effort**



THANK YOU!

QUESTIONS?

By Kafui, Reign, Samer, Teddy & Ed