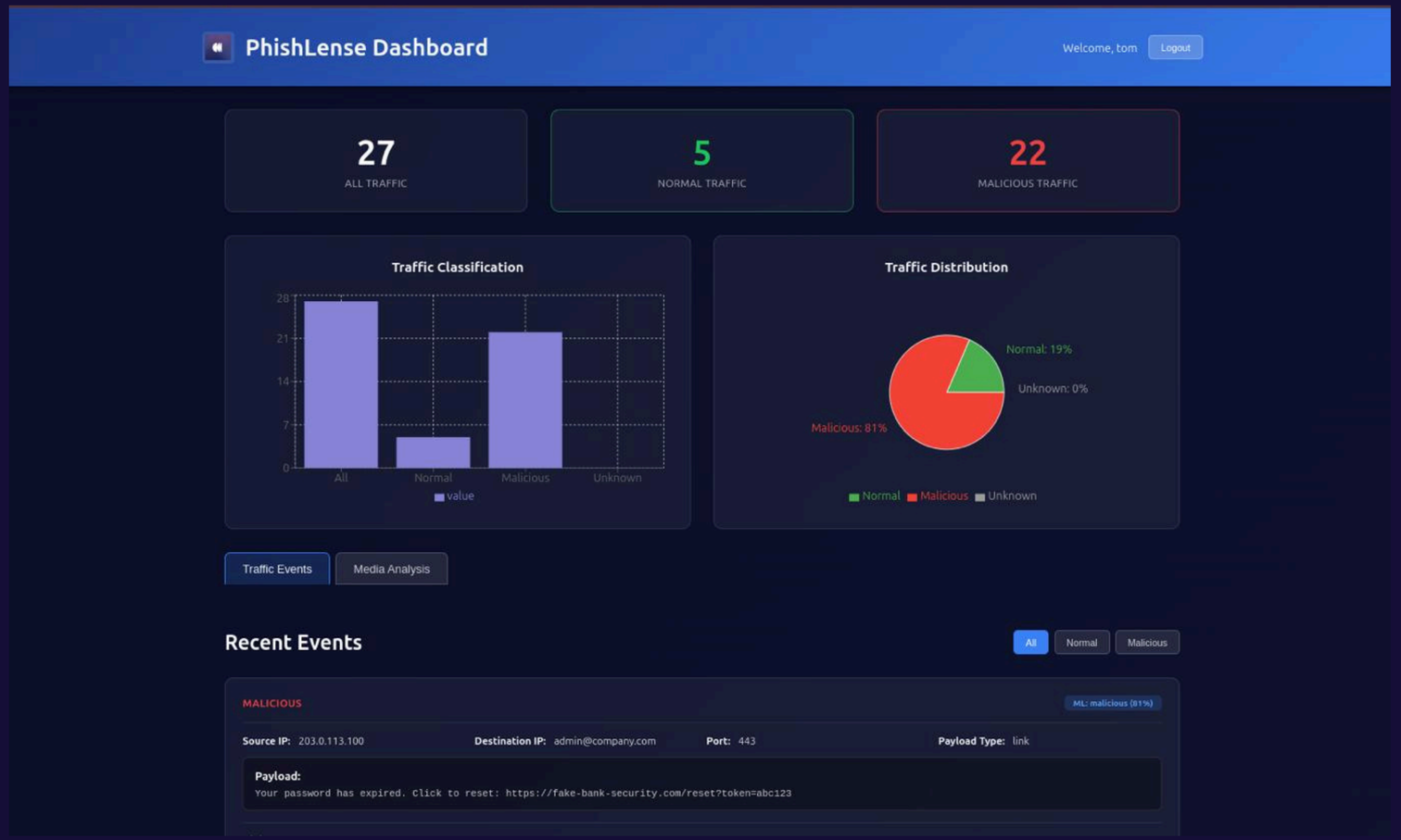
PhishLense



The AI That Executes Dangerous stuff, So You Don't Have To

BBC

NEWS

Menu

Business | Economy | Technology of Business | AI Business

M&S profits almost wiped out after cyber hack hit sales

The food and fashion retailer had some empty shelves after a cyber attack hit its website and disrupted supply chains

Faarea Masud

Business reporter

M&S's profits were almost wiped out after it was hit by a cyber-attack which left shoppers unable to buy online from the company for months.

The hack was "an extraordinary moment in time," it said, as it revealed statutory profit before tax - a figure that reflects all costs for a period - slumped 99% from £391.9m to £3.4m for the first half of the year, compared with the year prior.

As well as disrupting its online business, the hack affected M&S in-store too, leaving some shelves bare in the weeks after it was targeted.

M&S's boss said profits should recover in the key Christmas period, but warned a later Budget and chancellor's speech on Tuesday had not inspired confidence in UK shoppers.

"The presentation may have calmed the bonds markets, but it hasn't really calmed our customers," chief executive Stuart Machin said.

"They [customers] might be planning for a good Christmas, but they're also planning for the worst when it comes to the Budget," he added.

Expectations have grown that taxes will be hiked in the Budget on 26 November after Reeves **refused to rule out a U-turn on Labour's general election manifesto pledge not to hike income tax, VAT or National Insurance.**

Mr Machin questioned why the government was holding a Budget so late in the year. "We're all sitting here," he said.

M&S

£300M lost

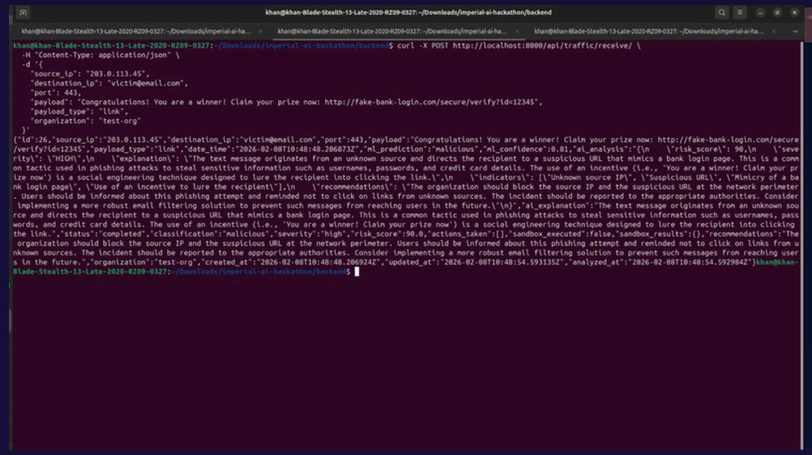
The Problem:

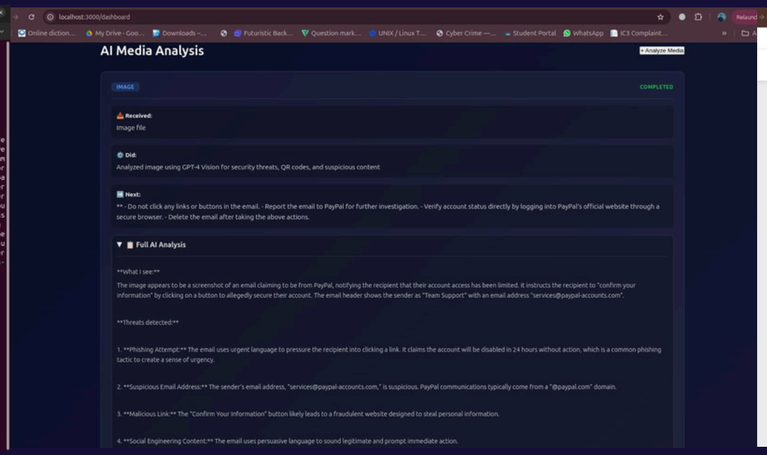
82%

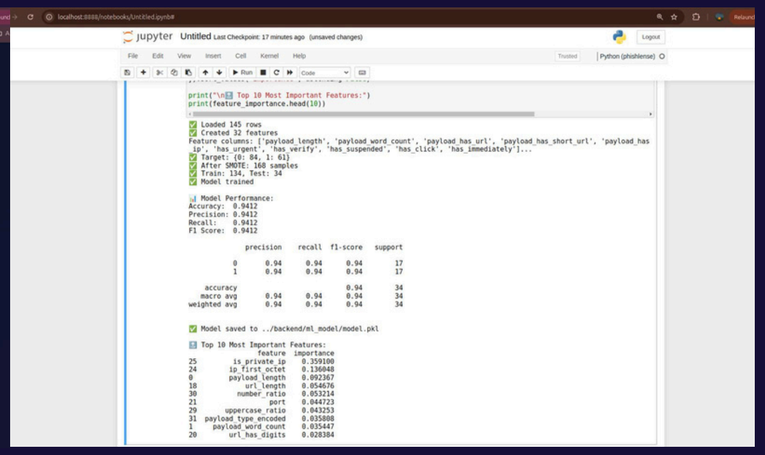
of phishing emails now use AI. They have perfect grammar, personalized content, and zero red flags. Small businesses don't have security teams to protect them.

The Solution:

PhishLense is an AI frontier agent. Instead of your employees clicking suspicious links, our AI does. It opens emails, clicks links, fills forms with fake data, and reports exactly what the attacker tried to steal — before any damage happens.







1: Real Attack

2: ChatGPT integration for analysis & recommended action

3: ML model training

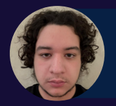
Why PhishLense Wins?

TAM：Global Email Security Market $5.5 BILLION

Feature	legacy gateway proofpoint.	Heavy sandbox ANY.RUN	PhishLense
Detection tech	Static Rules	VM Simulation	**Hybrid Ai + Docker**
Analysis Time	seconds	3-5 minutes	**seconds**
Context Aware?	✖	✖	✔
Infrastructure	Database	Heavy VM	**Lightweight Container**
Explainability	"Blocked"	Screenshots	**Human Summary**

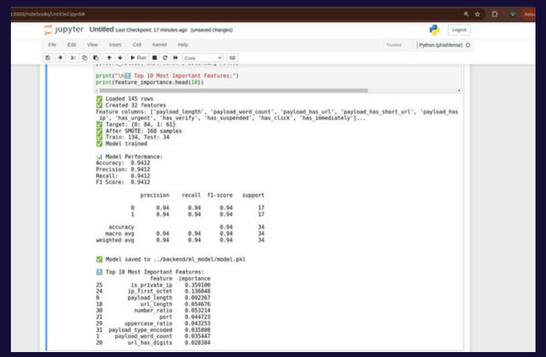
What Built This Weekend


Sheriff Danish
Computer Science


Riad Tarverdiyev
Business + Tech

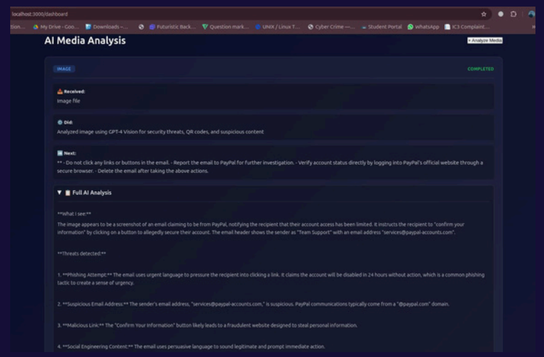

Kara Wong
MBA

Working ML Model



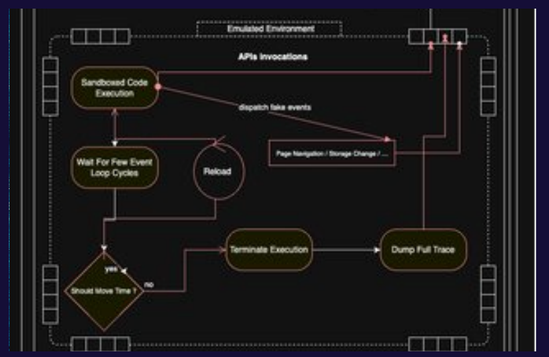
- Random Forest classifier
- 94% accuracy
- 145 URLs trained

GPT-4o Integration



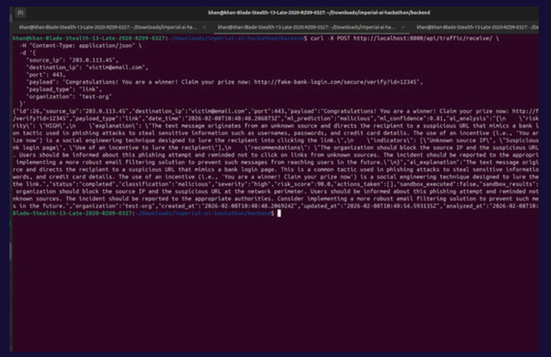
- Intent analysis
- Plain-English explanations

Sandbox Execution (Future work/ in progress)



- Playwright headless browser
- Form detection
- Auto-fill

Tested on Real Attacks



- Synthetic dataset
- Validated with actual phishing samples

Next 90 days:

Pilot Desktop App → Run with 3 SME design partners → **Chrome Extension Launch** → Gmail & Outlook support → **First 10 Paying Customers**