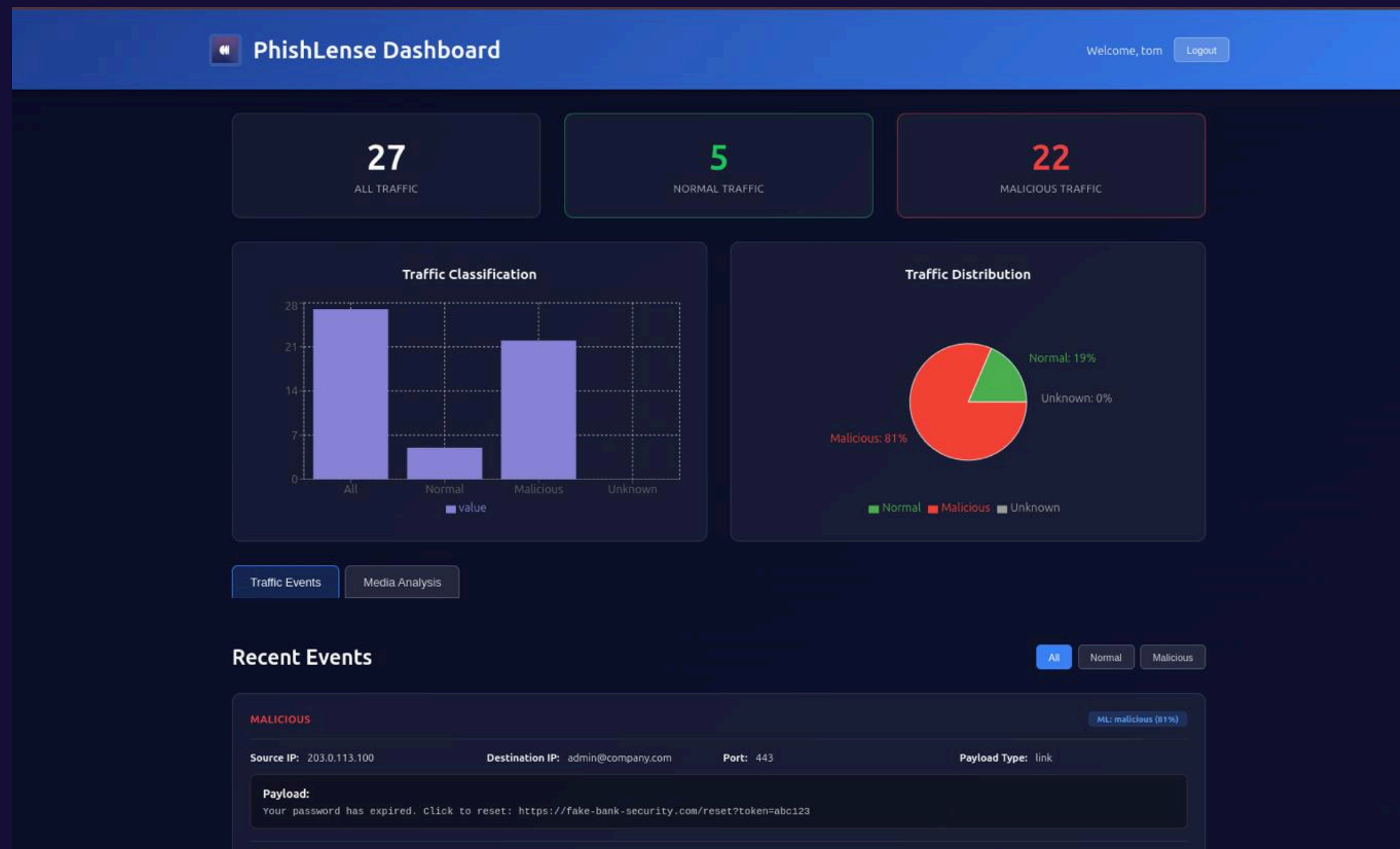


# PhishLense



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



£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.

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.

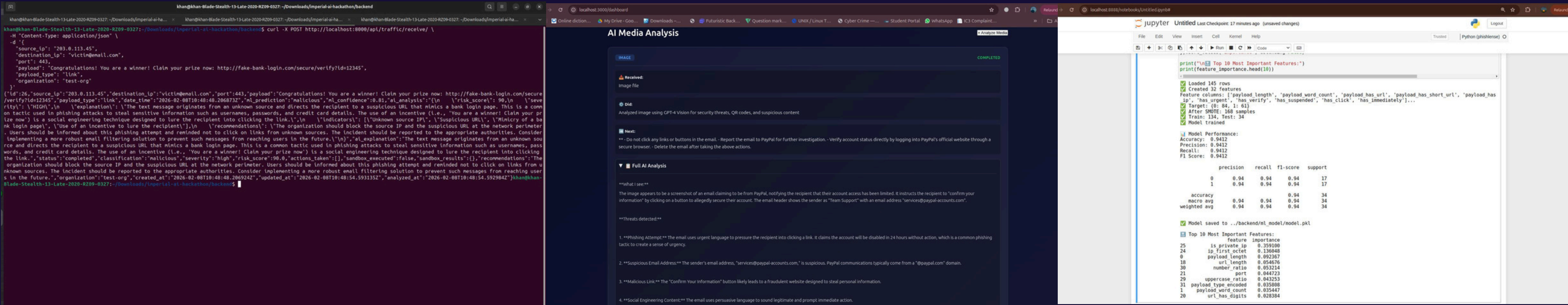
"They [customers] might be planning for a good Christmas, but they're also planning for the worst when it comes to the Budget," he added.

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.

# 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 ANYRUN	
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



**Sheriff Danish**  
Computer Science



**Riad Tarverdiyev**  
Business + Tech



**Kara Wong**  
MBA

# Built This Weekend

## Working ML Model

```
print("\n\nTop 10 Most Important Features:")
print(feature_importance.head(10))

# Loaded 345 rows
# Created 32 features
# Feature columns: ['payload_length', 'payload_word_count', 'payload_has_url', 'payload_has_short_url', 'payload_has_ip', 'has_urgent', 'has_verify', 'has_suspicious', 'has_click', 'has_immediately']...
# Target: (0: 84, 1: 62)
# After 50000: 100 samples
# Train: 134, Test: 34
# Model Trained

# Model Performance:
# Accuracy: 0.9422
# Precision: 0.9422
# Recall: 0.9422
# F1 Score: 0.9422

# Confusion Matrix:
#          actual \ predicted   0      1
# predicted 0       84      62
#           1       62      84

# Feature Importance:
# feature      importance
# payload_length  0.250180
# payload_word_count  0.136880
# url_length  0.092367
# number_ratio  0.054676
# port  0.053214
# uppercase_ratio  0.043253
# payload_type_encoded  0.032080
# payload_word_count  0.031447
# url_has_digits  0.020384
```

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

## GPT-4o Integration

**AI Media Analysis**

**Received**

Image file

**0:04**

Analyzed image using GPT-4 Vision for security threats, QR codes, and suspicious content.

**News:**

- Do not click any links or buttons in the email. Report the email to PayPal for further investigation. Verify account status directly by logging into PayPal's official website through a secure browser. Delete the email after taking the above actions.

**Full AI Analysis**

**What I see...**

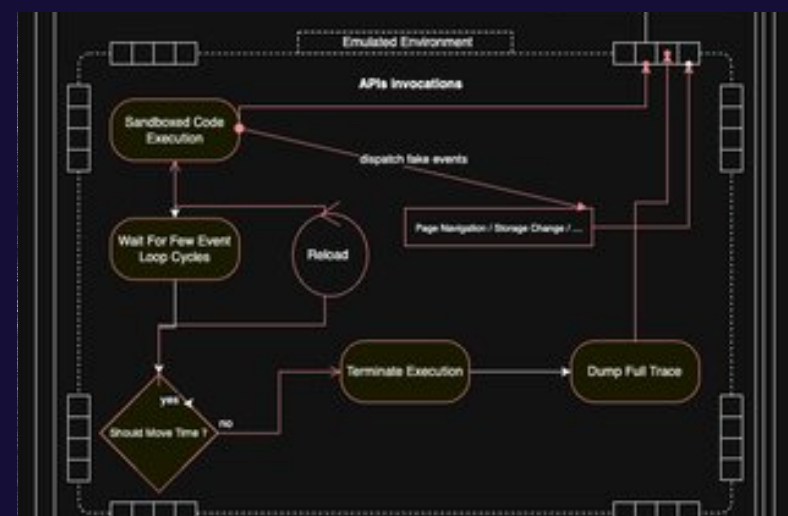
The image appears to be a screenshot of an email claiming to be from PayPal, notifying the recipient that their account access has been limited. It instructs the recipient to "confirm your information" by clicking on a button to allegedly secure their account. The email header shows the sender as "Team Support" with an email address "team@paypal.com".

**Threats detected...**

- Phishing Attempt:** The email uses urgent language to pressure the recipient into clicking a link. It claims the account will be disabled in 24 hours without action, which is a common phishing tactic to create a sense of urgency.
- Suspicious Email Address:** The sender's email address, "team@paypal.com", is suspicious. PayPal communications typically come from a "@paypal.com" domain.
- Malicious Link:** The "Confirm your information" button likely leads to a fraudulent website designed to steal personal information.
- Social Engineering Content:** The email uses persuasive language to sound legitimate and prompt immediate action.

- Intent analysis
- Plain-English explanations

## Sandbox Execution (Future work/ in progress)



- Playwright headless browser
- Form detection
- Auto-fill

## Tested on Real Attacks

```
curl -X POST http://localhost:8080/api/traffic/receive/ \
-d '{
  "Content-Type": "application/json",
  "source_ip": "203.0.113.45",
  "destination_ip": "victim@mail.com",
  "port": 443,
  "payload": "Congratulations! You are a winner! Claim your prize now: http://fake-bank-login.com/secure/verify?id=12345",
  "payload_type": "link",
  "organization": "Test-org"
}'

{"id": "ph", "source_ip": "203.0.113.45", "destination_ip": "victim@mail.com", "port": 443, "payload": "Congratulations! You are a winner! Claim your prize now: http://fake-bank-login.com/secure/verify?id=12345", "payload_type": "link", "date_time": "2024-02-08T10:48:48.260972Z", "ml_prediction": "malicious", "ml_confidence": 0.81, "al_analysis": [{"risk": "high", "reason": "The text message originates from an unknown source and directs the recipient to a suspicious URL that mimics a bank login page. The use of an incentive (i.e., 'You are a winner!') is a social engineering technique designed to lure the recipient into clicking the link."}], "indicators": [{"type": "suspicious_ip", "value": "203.0.113.45"}, {"type": "suspicious_payload", "value": "Congratulations! You are a winner! Claim your prize now: http://fake-bank-login.com/secure/verify?id=12345"}], "status": "completed", "classification": "malicious", "severity": "high", "risk_score": 98.0, "actions_taken": [{"action": "block", "target": "203.0.113.45"}, {"action": "block", "target": "http://fake-bank-login.com/secure/verify?id=12345"}], "sandbox_results": {"executed": true, "analysis": "The text message is a phishing attempt designed to steal personal information. The link 'http://fake-bank-login.com/secure/verify?id=12345' is a malicious URL. The organization should block the source IP and the suspicious URL at the network perimeter. Users should be informed about this phishing attempt and reminded not to click on links from unknown sources. The incident should be reported to the appropriate authorities. Consider implementing a more robust email filtering solution to prevent such messages from reaching users in the future."}, "organization": "Test-org", "created_at": "2024-02-08T10:48:48.260972Z", "updated_at": "2024-02-08T10:48:48.260972Z", "analyzed_at": "2024-02-08T10:48:48.260972Z"}
```

- Synthetic dataset
- Validated with actual phishing samples

## Next 90 days:

