APP DESIGN WITH LOVEABLE -SHOWASING-AI

My prompts

Project Name

CyberGuard Pro – Email Phishing Detection

Overview

CyberGuard Pro is a modern React-based cybersecurity application that scans emails for phishing threats and social engineering attacks. It provides **real-time threat scoring**, **authority impersonation detection**, and **comprehensive security reporting** in a sleek, cyber-themed UI.

Key Features

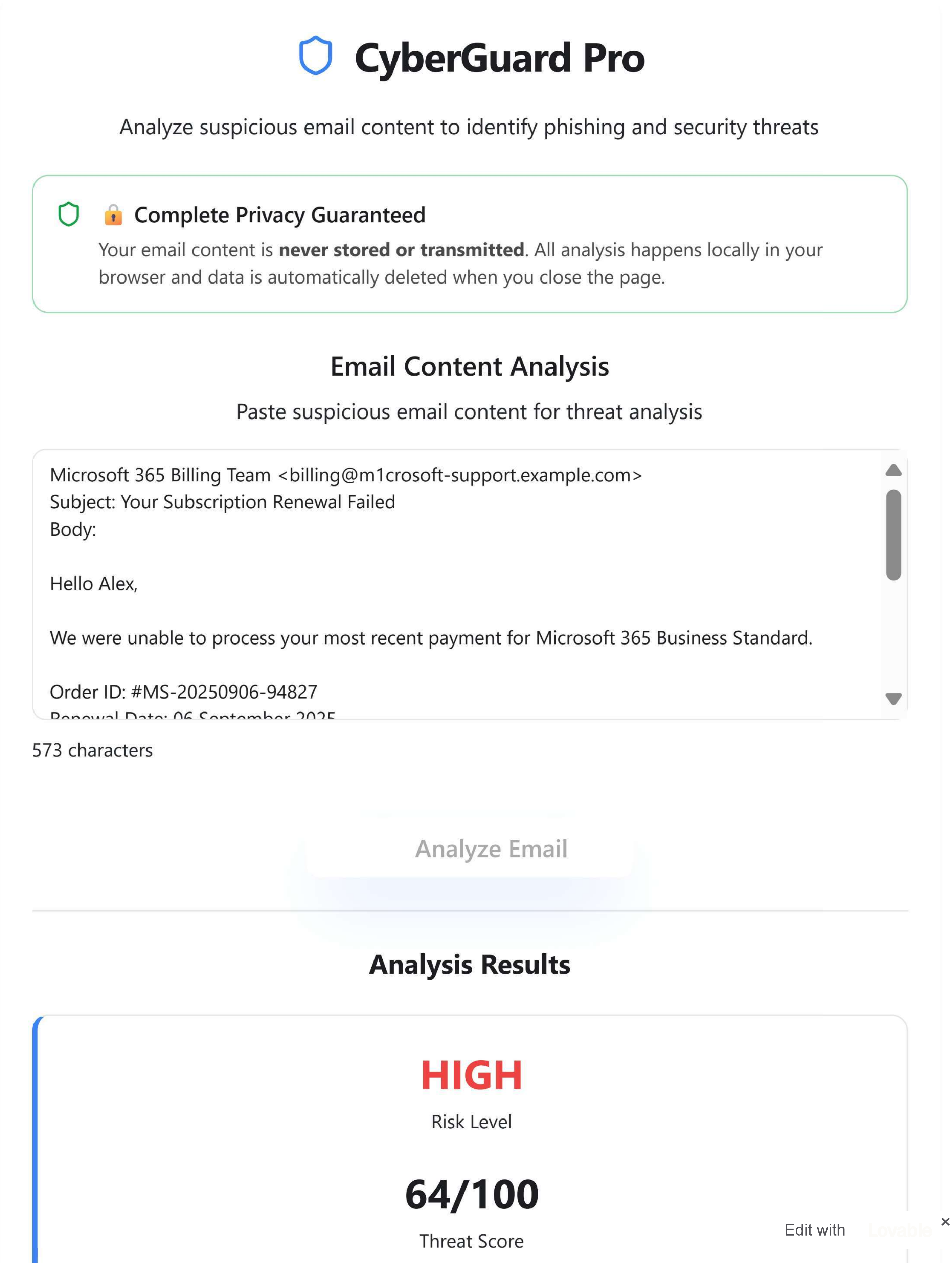
- **Email Analysis & Threat Detection:** Highlights suspicious indicators like urgent tone, credential requests, or link mismatches.
- **Authority Impersonation Detection:** Flags emails pretending to be executives, banks, or government agencies.
- **Real-Time Threat Scoring:** Provides a 0–100 threat score with severity labels.
- **Professional Security Reports:** Generate clear, sharable reports for analysis.
- **Responsive & Accessible UI:** Cyber-themed design, keyboard navigable, and ARIA compliant.

What I Learned

- **Cybersecurity Awareness:** Deepened understanding of phishing patterns and social engineering tactics.
- **Interactivity & UX:** Implemented real-time scoring and dynamic indicator feedback.
- **Problem Solving:** Designed heuristics for threat detection and authority impersonation identification.

Skills Demonstrated

- **Cybersecurity Knowledge:** Email threat detection, phishing awareness, authority impersonation.
- **Problem Solving & Logic:** Threat scoring algorithms and detection heuristics.
- **Portfolio & Professional Presentation:** Clear documentation, GitHub-ready project, professional UI.



CyberGuard Pro

Analyze suspicious email content to identify phishing and security threats

🔒 **Complete Privacy Guaranteed**

Your email content is **never stored or transmitted**. All analysis happens locally in your browser and data is automatically deleted when you close the page.

Email Content Analysis

Paste suspicious email content for threat analysis

```
Microsoft 365 Billing Team <billing@m1crosoft-support.example.com>
Subject: Your Subscription Renewal Failed
Body:

Hello Alex,

We were unable to process your most recent payment for Microsoft 365 Business Standard.

Order ID: #MS-20250906-94827
Renewal Date: 06 September 2025
```

573 characters

Analysis Results

HIGH

Risk Level

64/100

Threat Score

40%

Confidence

Summary:

⚠️ HIGH RISK: This email shows 5 suspicious patterns with a risk score of 64/100. Exercise extreme caution and verify authenticity.

Detected Threats:

HIGH **Credential Harvesting**

Attempts to steal login credentials

Action: Never enter credentials through email links. Access services directly.

HIGH **Urgency Manipulation**

Psychological pressure tactics to force hasty decisions

Action: Take time to verify. Legitimate urgent matters have alternative contact methods.

HIGH **Authority Impersonation**

Impersonates trusted authorities or companies

Action: Verify through official channels. Government agencies do not initiate contact via email.

MEDIUM **Invoice/Billing Scams**

Fake invoices or billing notifications to steal payment information

Action: Check your actual accounts directly. Do not click payment links in emails.

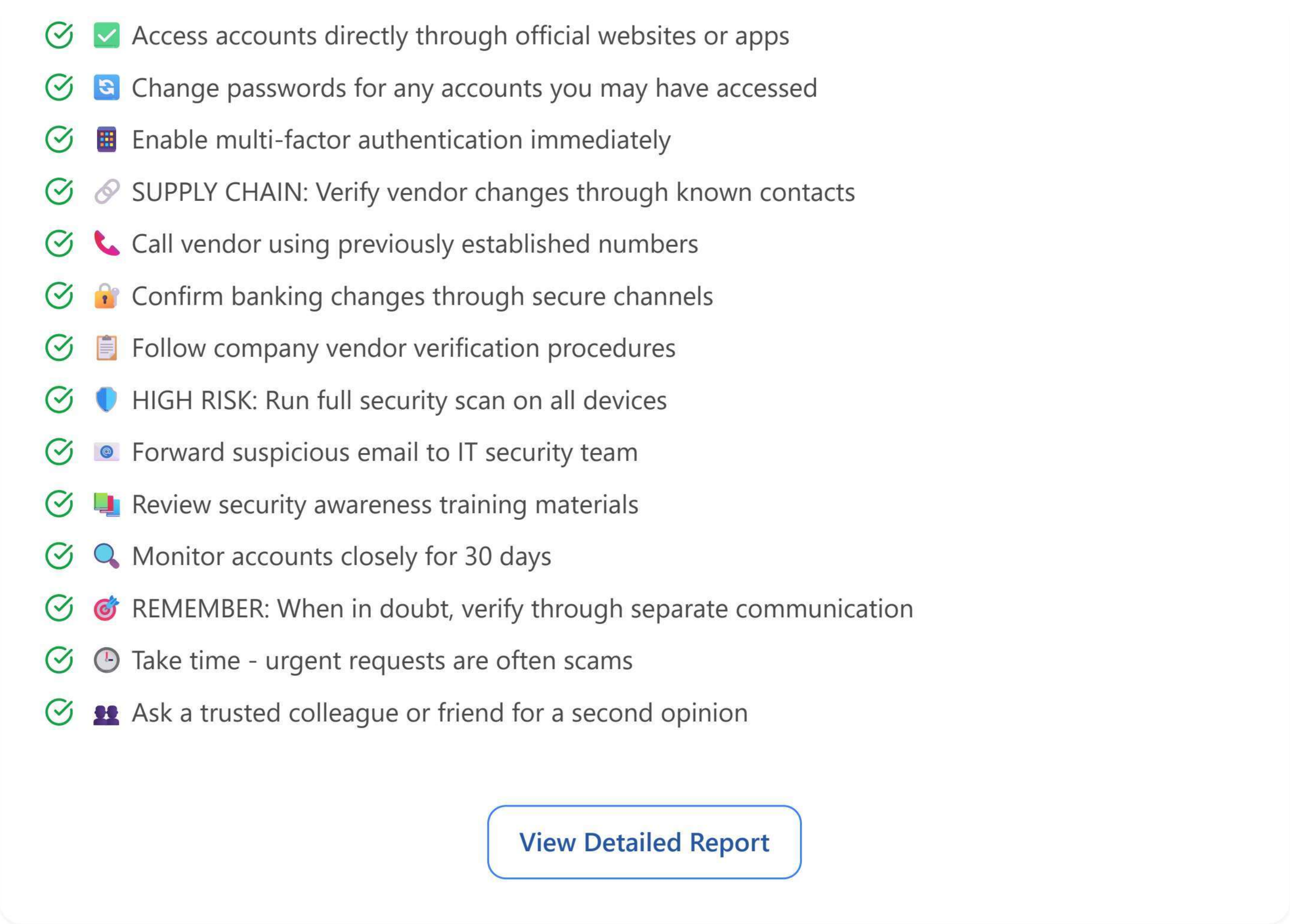
HIGH **Supply Chain Attacks**

Attacks targeting business relationships and vendor communications

Action: Verify vendor communications through established channels. Confirm account changes.

Recommendations:

✓ 🔐 CREDENTIALS: Do not enter login information through email links



- ✓ ✅ Access accounts directly through official websites or apps
- ✓ 🔄 Change passwords for any accounts you may have accessed
- ✓ 📱 Enable multi-factor authentication immediately
- ✓ 🔗 SUPPLY CHAIN: Verify vendor changes through known contacts
- ✓ 📞 Call vendor using previously established numbers
- ✓ 🔐 Confirm banking changes through secure channels
- ✓ 📋 Follow company vendor verification procedures
- ✓ 🛡️ HIGH RISK: Run full security scan on all devices
- ✓ 📧 Forward suspicious email to IT security team
- ✓ 📚 Review security awareness training materials
- ✓ 🔍 Monitor accounts closely for 30 days
- ✓ 🎯 REMEMBER: When in doubt, verify through separate communication
- ✓ 🕐 Take time - urgent requests are often scams
- ✓ 👥 Ask a trusted colleague or friend for a second opinion

Microsoft 365 Billing Team <billing@m1crosoft-support.example.com>
Subject: Your Subscription Renewal Failed
Body:

Hello Alex,

We were unable to process your most recent payment for Microsoft 365 Business Standard.

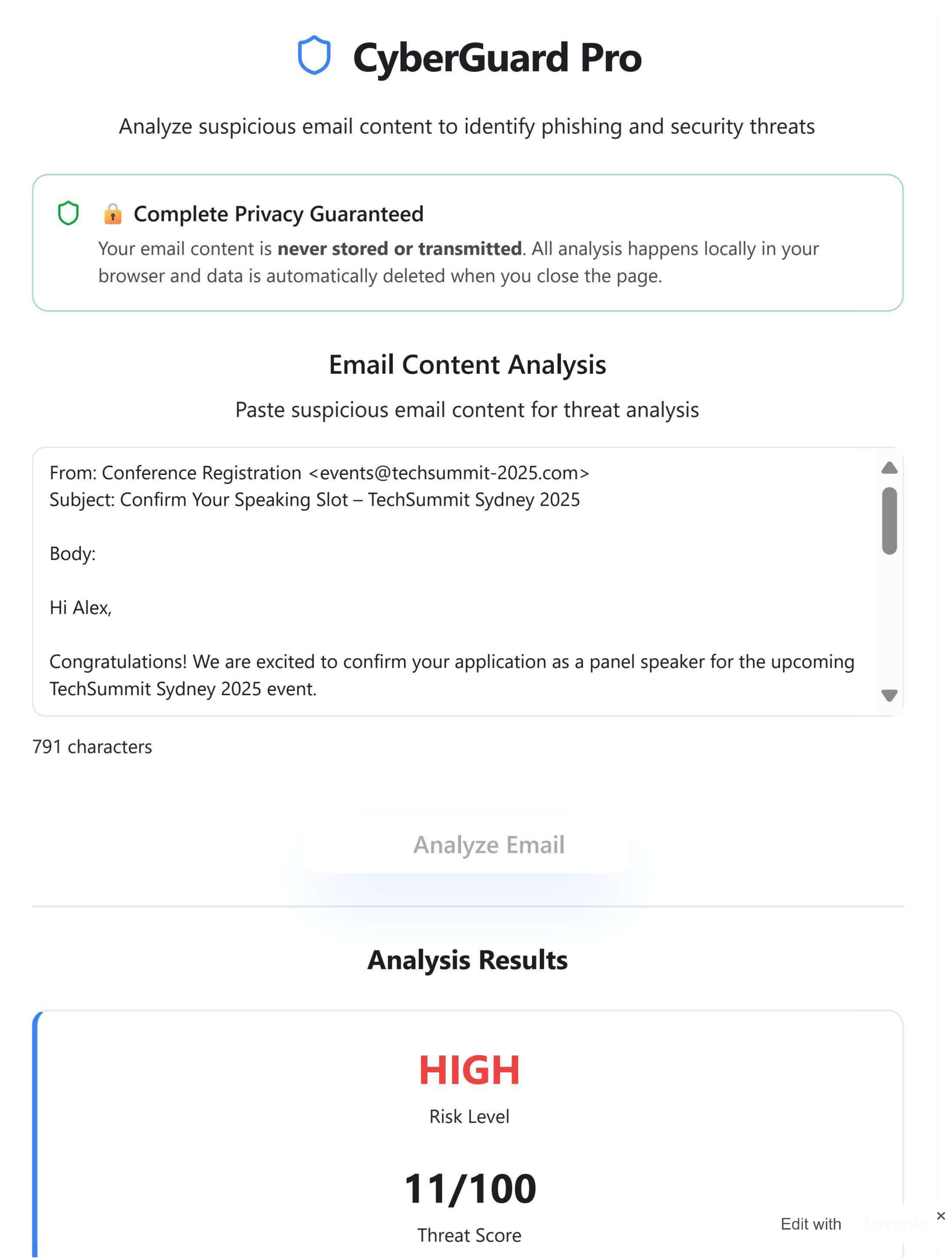
Order ID: #MS-20250906-94827
Renewal Date: 06 September 2025
Amount: $129.99 AUD

To avoid interruption to your services, please update your payment details immediately:

https://account.microsoft365-billing.example.com/renew?id=94827

Thank you,
Microsoft Billing Support

Note: If you recently updated your payment method, please disregard this message.



CyberGuard Pro

Analyze suspicious email content to identify phishing and security threats

🔒 **Complete Privacy Guaranteed**

Your email content is **never stored or transmitted**. All analysis happens locally in your browser and data is automatically deleted when you close the page.

Email Content Analysis

Paste suspicious email content for threat analysis

From: Conference Registration <events@techsummit-2025.com>
Subject: Confirm Your Speaking Slot – TechSummit Sydney 2025

Body:

Hi Alex,

Congratulations! We are excited to confirm your application as a panel speaker for the upcoming TechSummit Sydney 2025 event.

791 characters

Analysis Results

HIGH

Risk Level

11/100

Threat Score

36%

Confidence

Summary:

⚠️ HIGH RISK: This email shows 2 suspicious patterns with a risk score of 11/100. Exercise extreme caution and verify authenticity.

Detected Threats:

HIGH **Urgency Manipulation**

Psychological pressure tactics to force hasty decisions

Action: Take time to verify. Legitimate urgent matters have alternative contact methods.

MEDIUM **Prize Scams**

Fake lottery or prize notifications

Action: Legitimate prizes do not require payment or personal information to claim.

Recommendations:

- ✓ 🛡️ HIGH RISK: Run full security scan on all devices
- ✓ 📧 Forward suspicious email to IT security team
- ✓ 📚 Review security awareness training materials
- ✓ 🔍 Monitor accounts closely for 30 days
- ✓ 🎯 REMEMBER: When in doubt, verify through separate communication
- ✓ 🕒 Take time - urgent requests are often scams
- ✓ 👥 Ask a trusted colleague or friend for a second opinion

View Detailed Report

From: Conference Registration <events@techsummit-2025.com>
Subject: Confirm Your Speaking Slot – TechSummit Sydney 2025

Body:

Hi Alex,

Congratulations! We are excited to confirm your application as a panel speaker for the upcoming TechSummit Sydney 2025 event.

Your provisional session details are as follows:
Topic: Emerging Threats in Cloud Security
Date: Thursday, 23 October 2025
Time: 2:00 – 3:30 PM AEST

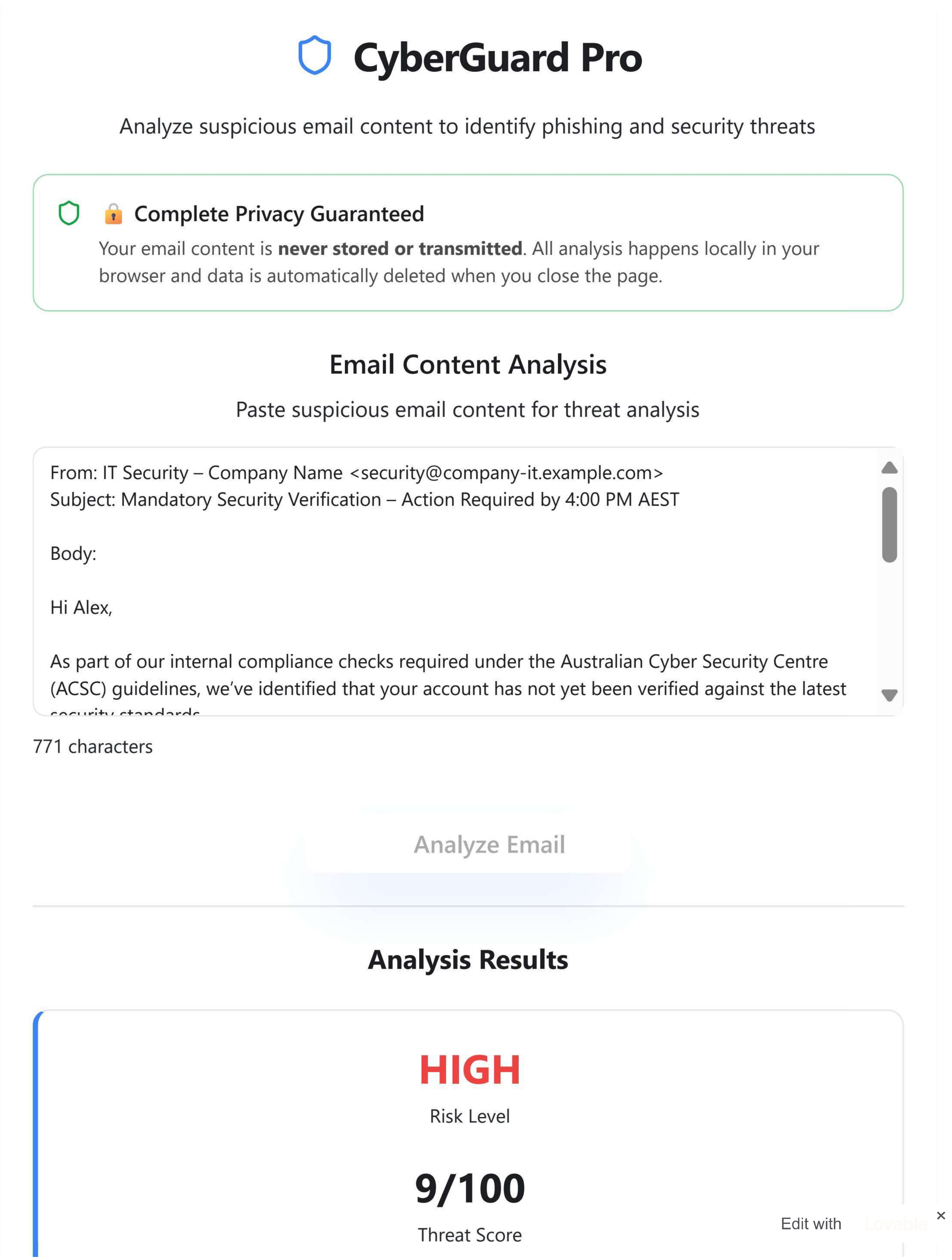
To finalize your slot and upload your headshot for marketing material, please confirm your participation by visiting the secure portal:

https://speakers.techsummit-2025.example.com/confirm?id=947182

Deadline for confirmation: Monday, 15 September 2025.

We look forward to showcasing your expertise at the event.

Warm regards,
Event Coordination Team
TechSummit Sydney 2025



CyberGuard Pro

Analyze suspicious email content to identify phishing and security threats

🔒 **Complete Privacy Guaranteed**

Your email content is **never stored or transmitted**. All analysis happens locally in your browser and data is automatically deleted when you close the page.

Email Content Analysis

Paste suspicious email content for threat analysis

From: IT Security – Company Name <security@company-it.example.com>
Subject: Mandatory Security Verification – Action Required by 4:00 PM AEST

Body:

Hi Alex,

As part of our internal compliance checks required under the Australian Cyber Security Centre (ACSC) guidelines, we've identified that your account has not yet been verified against the latest security standards

771 characters

Analysis Results

HIGH

Risk Level

9/100

Threat Score

35%

Confidence

Summary:

⚠️ HIGH RISK: This email shows 1 suspicious patterns with a risk score of 9/100. Exercise extreme caution and verify authenticity.

Detected Threats:

HIGH **Authority Impersonation**

Impersonates trusted authorities or companies

Action: Verify through official channels. Government agencies do not initiate contact via email.

Recommendations:

- ✓ 🛡️ HIGH RISK: Run full security scan on all devices
- ✓ 📧 Forward suspicious email to IT security team
- ✓ 📚 Review security awareness training materials
- ✓ 🔍 Monitor accounts closely for 30 days
- ✓ 🎯 REMEMBER: When in doubt, verify through separate communication
- ✓ 🕒 Take time - urgent requests are often scams
- ✓ 👥 Ask a trusted colleague or friend for a second opinion

View Detailed Report

From: IT Security – Company Name <security@company-it.example.com>
Subject: Mandatory Security Verification – Action Required by 4:00 PM AEST

Body:

Hi Alex,

As part of our internal compliance checks required under the Australian Cyber Security Centre (ACSC) guidelines, we’ve identified that your account has not yet been verified against the latest security standards.

To remain compliant, all staff must complete this verification process before 4:00 PM AEST today. Failure to do so will result in temporary suspension of your Microsoft 365 access, and your manager will be notified.

Please complete the check here:

https://secureverify.company-it.example.com/au?id=672194

Thank you for your immediate cooperation.

Regards,
IT Security Team
Company Name Pty Ltd