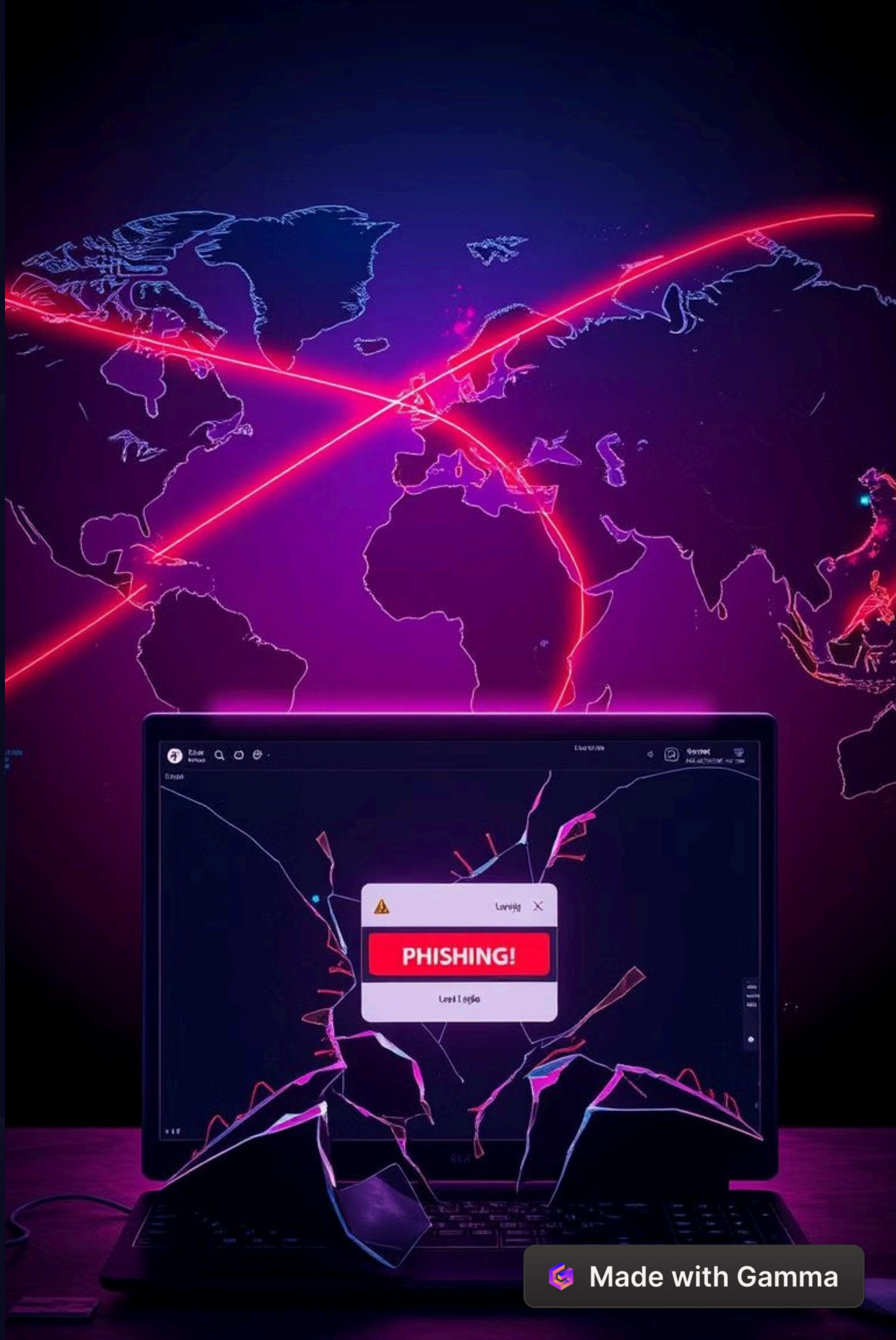
# Phishing Link Detector: A C++ Project for Cybersecurity Awareness

This presentation will explore a C++ project designed to raise awareness about phishing attacks and equip users with the tools to identify suspicious URLs. This project aims to empower individuals with knowledge and technology to navigate the online landscape with greater safety.

Group Members:

| | |
|---|---|
| Imtiaz Hussain (CY-24F-111) | Sanaullah Lakho (CY-24F-131) |
| M. Irtaza (CY-24F-149) | Taha Akbar (CY-24F-121) |



# Understanding the Phishing Threat

## What is Phishing?

Phishing attacks are malicious attempts by hackers to trick users into clicking fake links or providing sensitive information. They often impersonate legitimate entities, such as banks, social media platforms, or government agencies.

## The Dangers of Phishing

Phishing attacks can lead to significant consequences, including data theft, financial loss, identity fraud, and even malware infections. Hackers can gain access to personal information like passwords, credit card details, and bank account credentials.

# Introducing our Phishing Link Detector

### Input

Our detector takes a URL as input from the user, allowing them to check the safety of any link they encounter.

### Analysis

The program analyzes the URL for various phishing indicators using a series of predefined rules and checks.

### Output

The detector provides a risk score ranging from 0 to 10, indicating the likelihood of the URL being a phishing attempt. It also displays a warning message if the URL is deemed dangerous.

# Key Features of Our Detector

### Phishing Domains

Our detector identifies suspicious domain extensions like .xyz, .tk, and other less commonly used domains, which are often associated with phishing attempts.

### Suspicious Words

The program checks for misspelled brand names or unusual characters in the URL, such as g00gle or pay-pal, to indicate a potential phishing attempt.

### Excessive Symbols

An abundance of dashes (-) or underscores (_) in the URL can be a red flag, as phishing URLs sometimes use these symbols excessively to disguise the real domain.

### IP-Based URLs

If the URL uses an IP address instead of a domain name, it could be a sign of a phishing attack, as legitimate websites generally use domain names.

### @ Symbol

Phishing URLs may use the @ symbol in the URL to hide the true domain name, making it appear legitimate.

# Code Walkthrough: Function Breakdown

### hasPhishingDomain()

This function checks the domain extension of the URL and flags it as suspicious if it matches a list of predefined phishing domain extensions.

### hasSuspiciousWords()

This function scans the URL for misspellings or unusual characters in brand names, comparing them to a database of known brands and flagging any discrepancies.

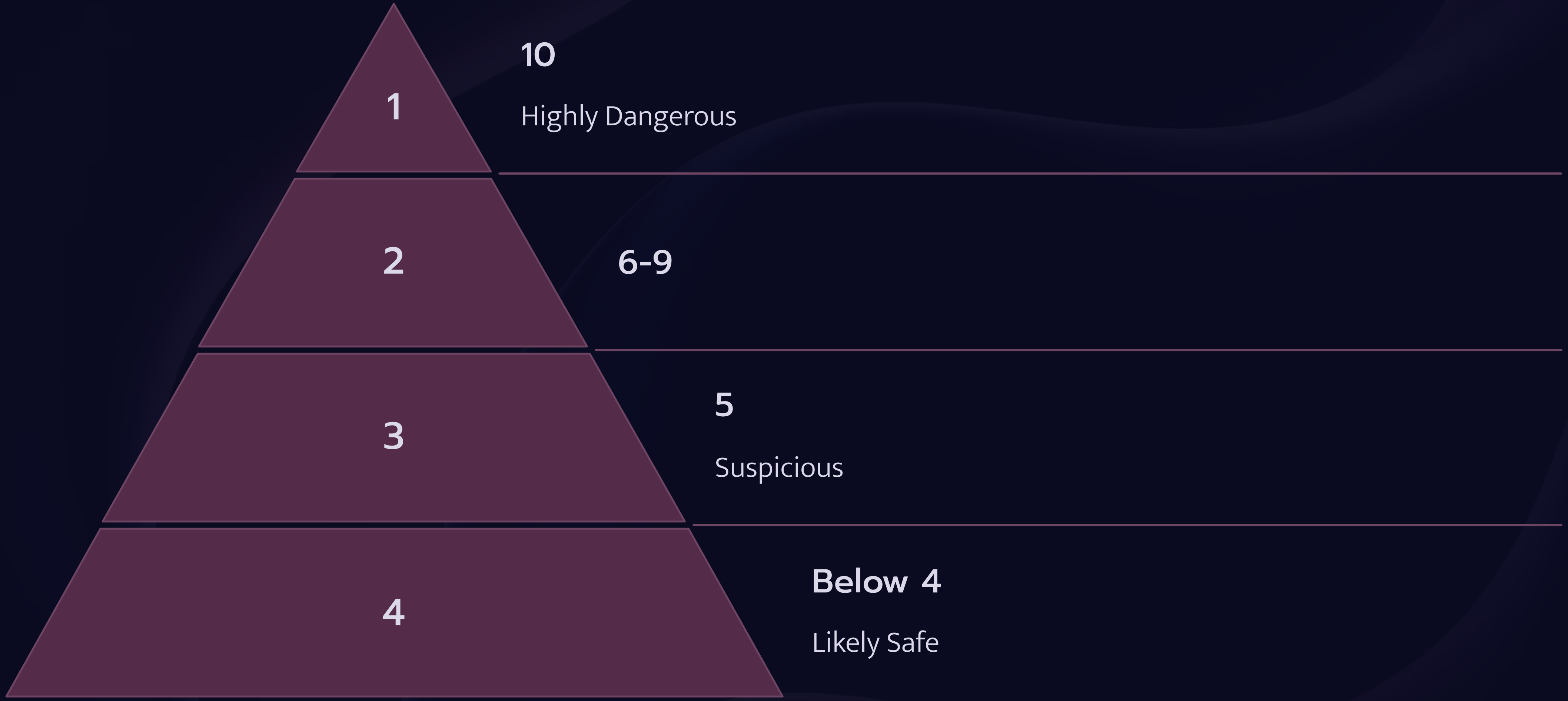
### hasTooManyDashes() and hasAtSymbol()

These functions check for an excessive number of dashes (-) or the presence of the @ symbol in the URL, which are common characteristics of phishing links.

### isIPAddress() and calculateRiskScore()

The isIPAddress() function determines if the URL is based on an IP address, while the calculateRiskScore() function assigns a risk score based on the results of the various checks.

# Risk Score System: Evaluating the Threat



1

**10**

Highly Dangerous

2

**6-9**

3

**5**

Suspicious

4

**Below 4**

Likely Safe

The risk score system assigns points based on the number of phishing indicators detected. A higher score indicates a higher risk of the URL being a phishing attempt.

# Live Demo: Putting Our Detector to the Test

1

URL Input

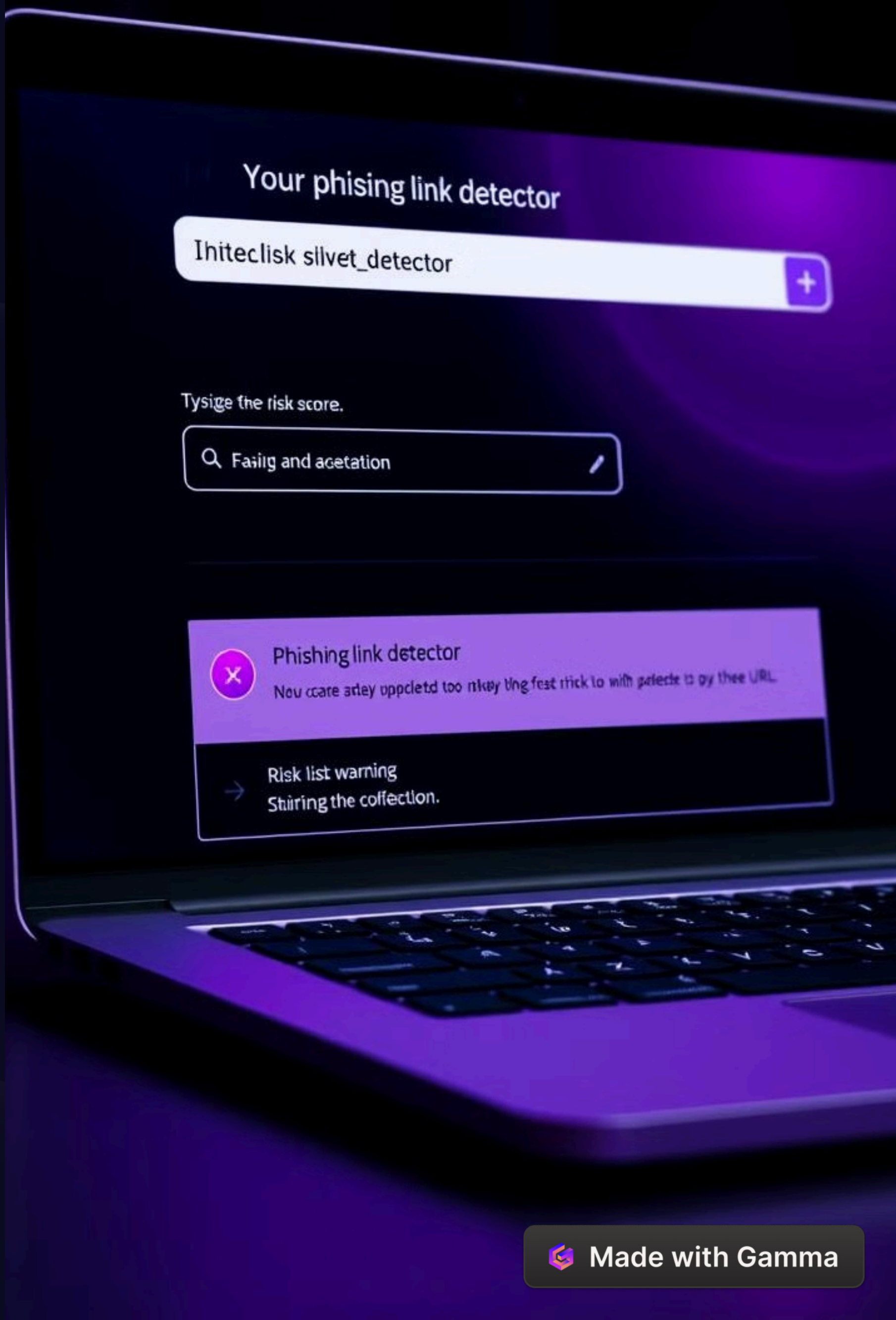
2

Analysis

3

Results

This live demo will showcase how our detector operates in real-time. We will demonstrate the input process, the analysis performed by the program, and the final output, including the risk score and warning message.


Your phising link detector
Ihiteclisk silvet_detector
Tysige the risk score.
Faiig and acetation
Phishing link detector
Nou ccate atey uppcletd too nkuy ung fest rtick to with gelecte is oy thee URL
Risk list warning
Stiiring the coffection.

# The Importance of Cybersecurity Awareness

### Protection

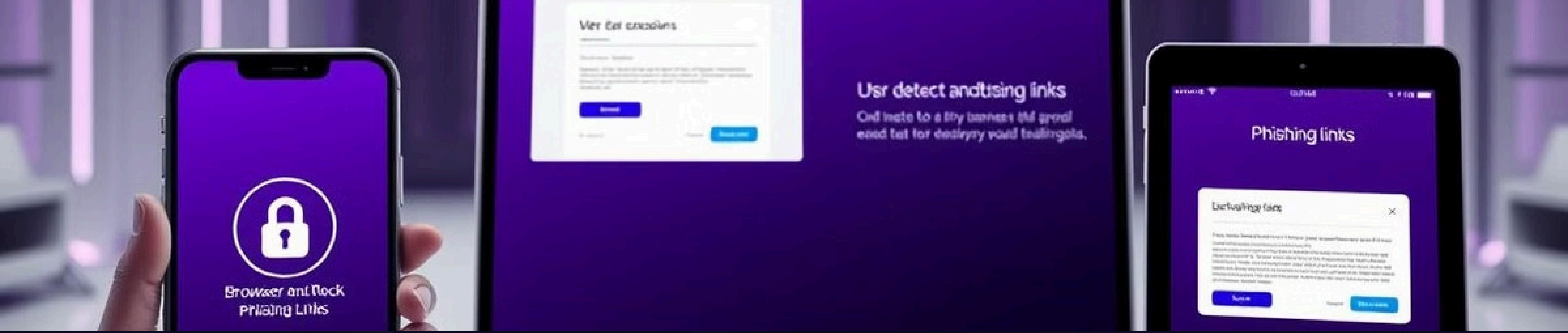
Our project empowers users to identify and avoid phishing scams, protecting their personal information and financial security.

### Education

This initiative helps raise awareness about cybersecurity risks, equipping individuals with the knowledge to make informed decisions online.

### Future Development

The foundation of this project can be expanded to include AI-powered detection systems and integrated databases to enhance its capabilities.



# Future Improvements: Expanding our Reach

1

### Machine Learning Integration

Integrating machine learning algorithms will enable the detector to adapt to new phishing patterns and evolve with the ever-changing cyber landscape.

2

### Anti-Bypass mask-up links

The advance phishing attack can bypass the detectors , which is why it is improving time by time .

3

### Browser Extension

Integrating our detector as a browser extension will provide real-time protection against phishing attacks, allowing users to confidently navigate the web.

# Conclusion & Q&A

In conclusion, this project serves as a powerful tool in the fight against phishing attacks. By raising awareness and providing a practical solution, we aim to empower individuals with the knowledge and tools they need to stay safe online. We encourage you to ask any questions you may have about our detector or the broader topic of cybersecurity.