EMAIL PHISHING ANALYSIS AND DETECTION

Team Members :

Mahmoud Ahmed

Youssef Ahmed Fouad

Gamal Abd Elnaser Sayed

Supervisorer :

Eng/ Noureldin Essam

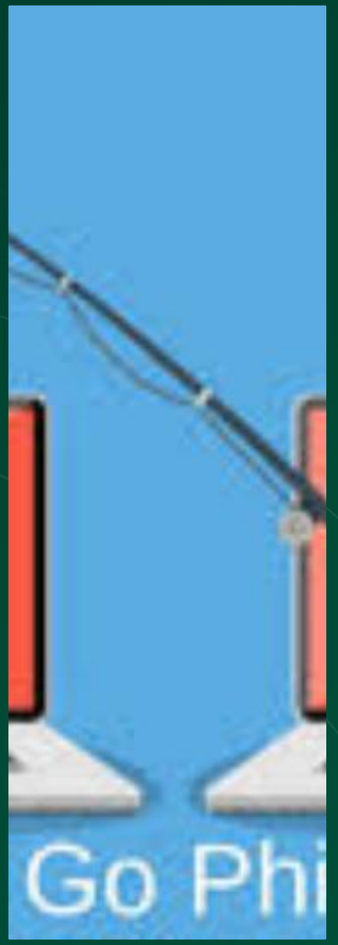
INTRODUCTION

- Email phishing is one of the most common cyber attacks today.
- Attackers trick users into revealing sensitive information using fake emails.
- This project demonstrates how to detect phishing emails using basic analysis techniques.

PROJECT OBJECTIVE

The goal of the project is to:

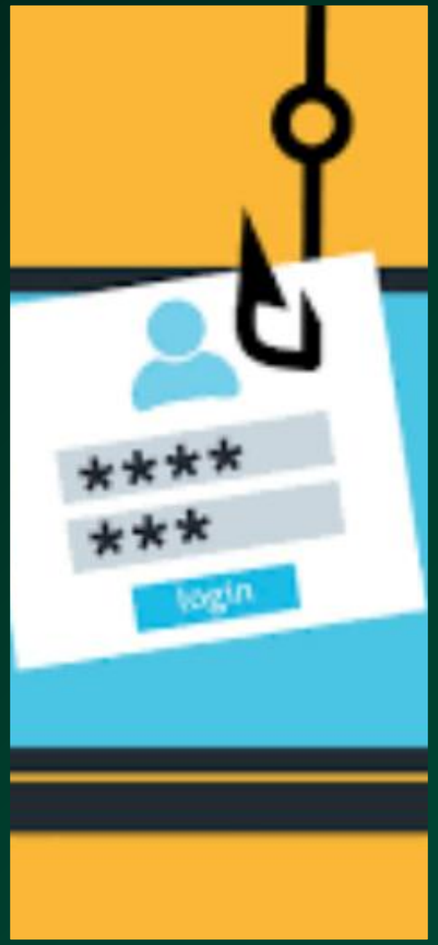
- Identify suspicious email characteristics
- Detect fake or spoofed sender addresses
- Analyze URLs and unusual language patterns
- Create a simple script/tool that flags potential phishing emails and generates a report



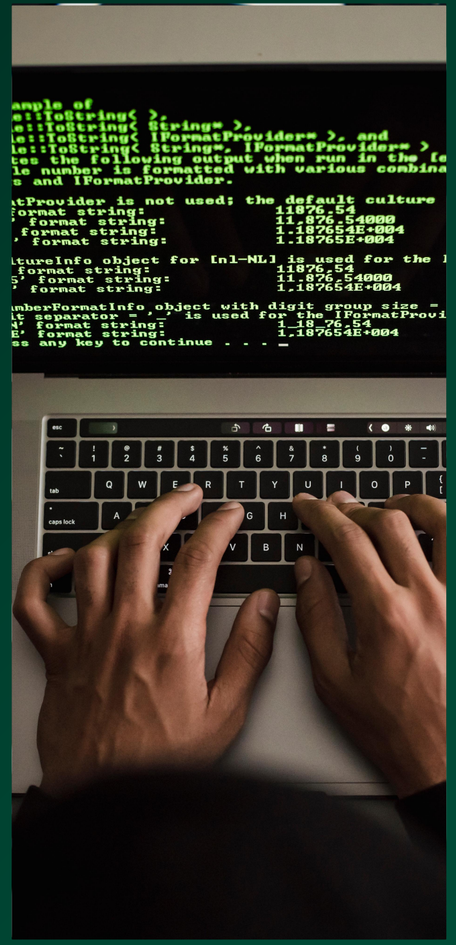
HOW PHISHING WORKS

Social engineering

Urgent emotional triggers

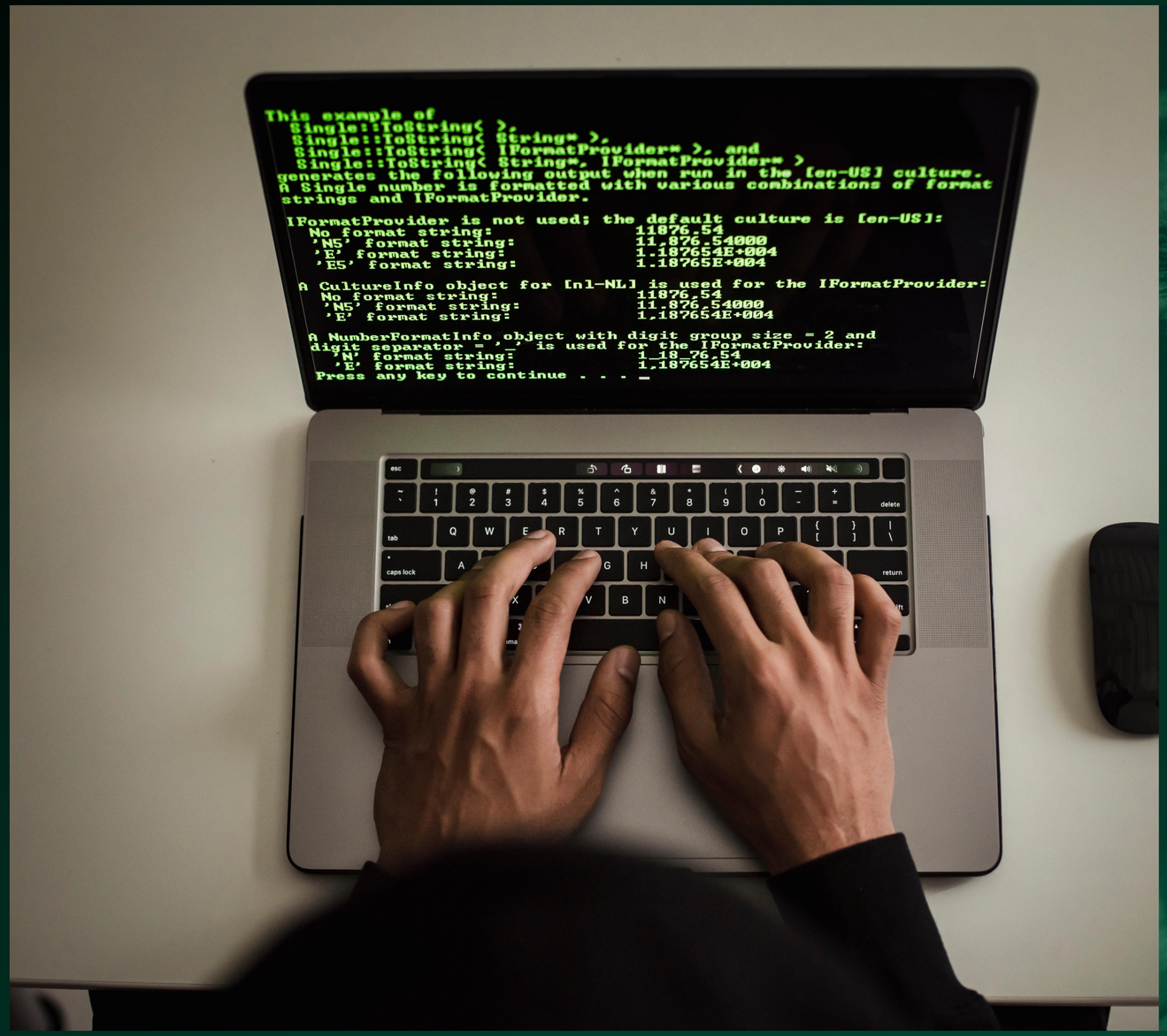


Fake login pages



Spoofed email addresses

Malicious links or attachments



SPOTTING A PHISHING EMAIL

- Misspelled domain name
- Suspicious links
- Urgent tone: “Act Now!”
- Unknown attachments
- Always verify sender identity

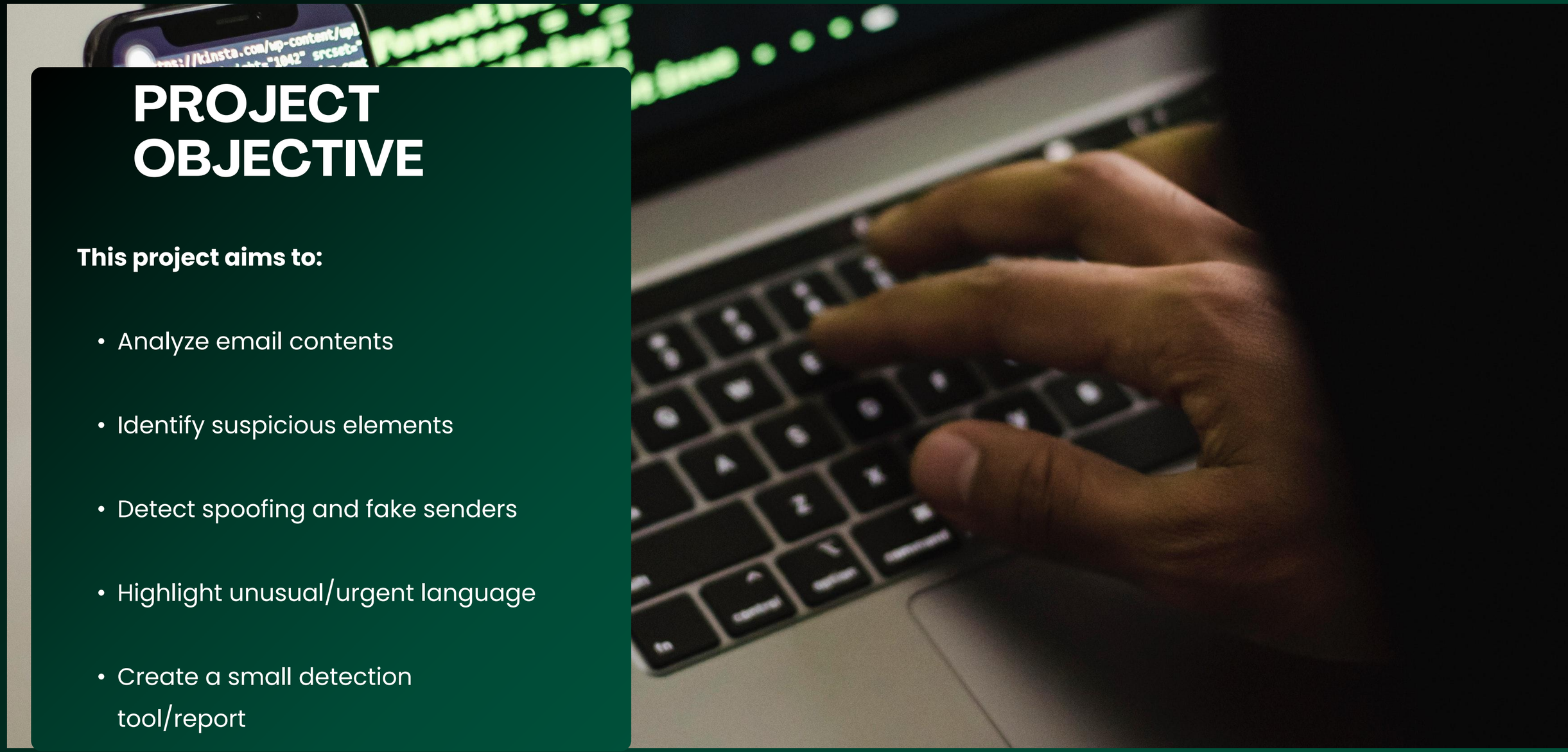
WHY THIS PROJECT MATTERS

- Phishing is the #1 cause of data breaches.
- 90% of cyber attacks start with a phishing email.
- Simple user mistakes cause massive losses.
- Detecting phishing early protects individuals & companies.

PROJECT OBJECTIVE

This project aims to:

- Analyze email contents
- Identify suspicious elements
- Detect spoofing and fake senders
- Highlight unusual/urgent language
- Create a small detection tool/report



COMMON PHISHING INDICATORS

Suspicious or shortened links

Urgent requests (e.g., Your account will be closed!)

Unknown sender names

Spoofed domains (e.g., support@paypall.com)

EMAIL ANATOMY
WE ANALYZE THREE MAIN PARTS:

Email Header — sender info

Body Content — text & language

URLs & Attachments — danger sources

HEADER ANALYSIS

CHECK:

- From address
- Reply-to address
- Domain authenticity
- IP reputation
- Sender name mismatch

URL ANALYSIS

WE CHECK:

- Real vs displayed link
- Shortened URLs
- Redirect chains
- Domain similarity (paypal.com vs paypal.com)
- HTTPS or unsecured links

In conclusion, this presentation highlights the growing threat of phishing and the importance of building effective detection techniques. By understanding common phishing indicators, analyzing email structures, and applying basic automation, we can significantly reduce the risk of successful attacks.
This project demonstrates how technical skills, critical thinking, and cybersecurity awareness work together to protect users and organizations.

THANK YOU FOR YOUR ATTENTION