# PhishIntel

## AI-powered URL and File Scam Detection Tool

TEAM MEMBERS:

Mayur Koreganokarr
Anjali Yadav

# Introduction

Phishing is a type of social engineering attack often used to steal user data,including login credential and credit card number.

# What is Phishing?

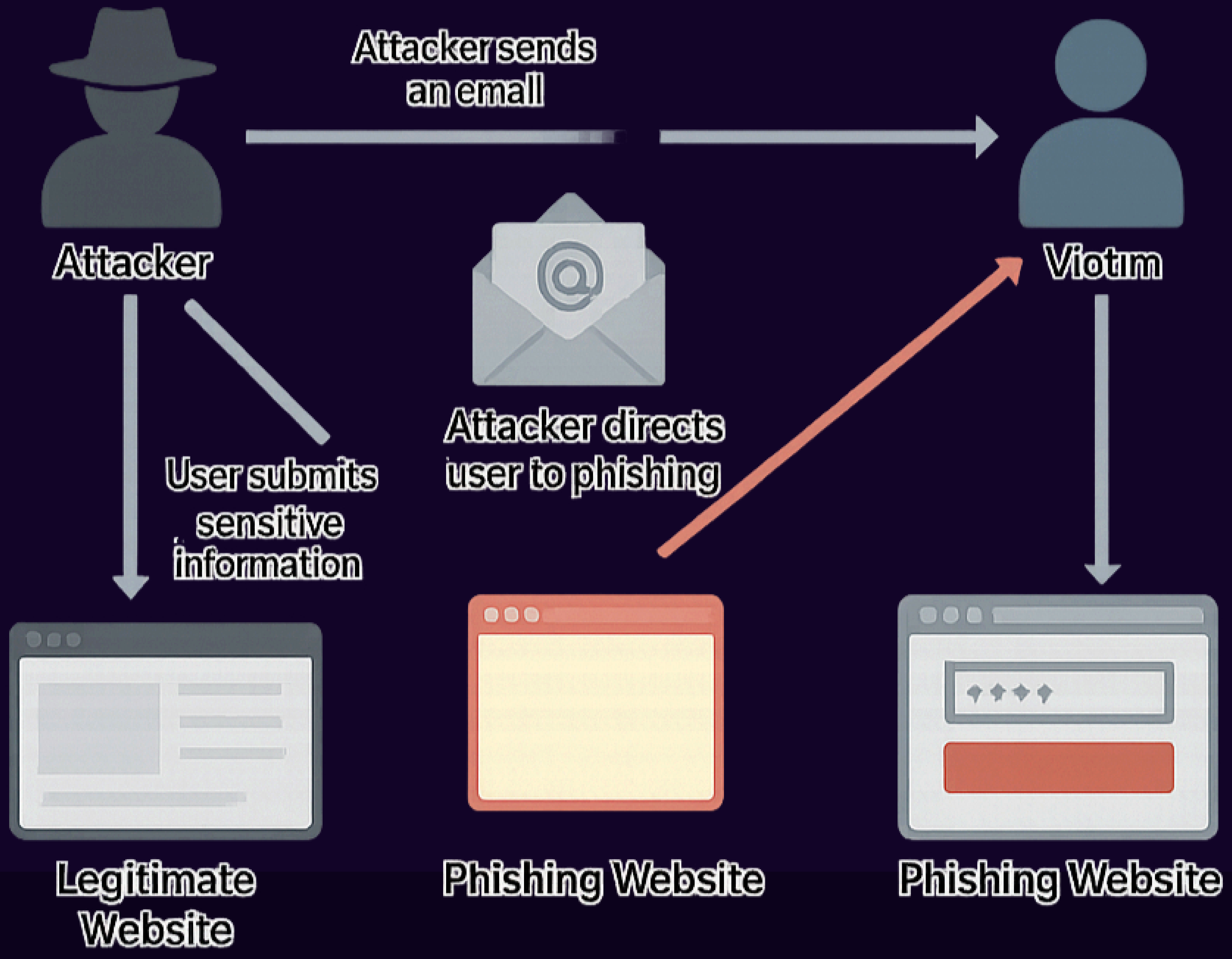
Phishing is a type of cyberattack where hackers trick people into sharing personal info by pretending to be trusted sources, like banks or websites.

They use fake emails, websites, or links to:

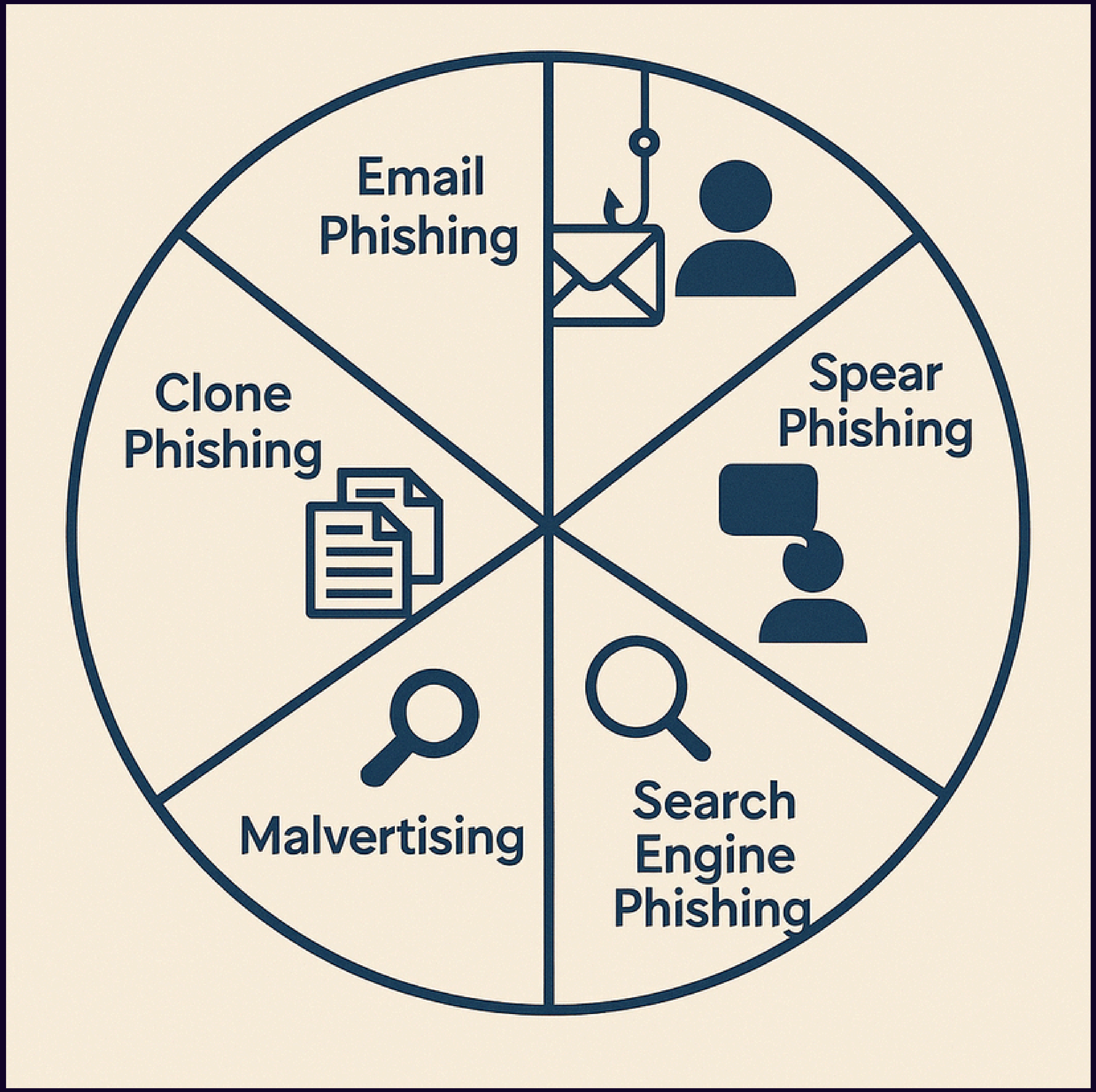
- Steal passwords
- Access bank accounts
- Install malware
- Commit identity theft
-

Phishing works by fooling people, not by hacking systems, which makes it a serious threat.

# How  Does Phishing Work?

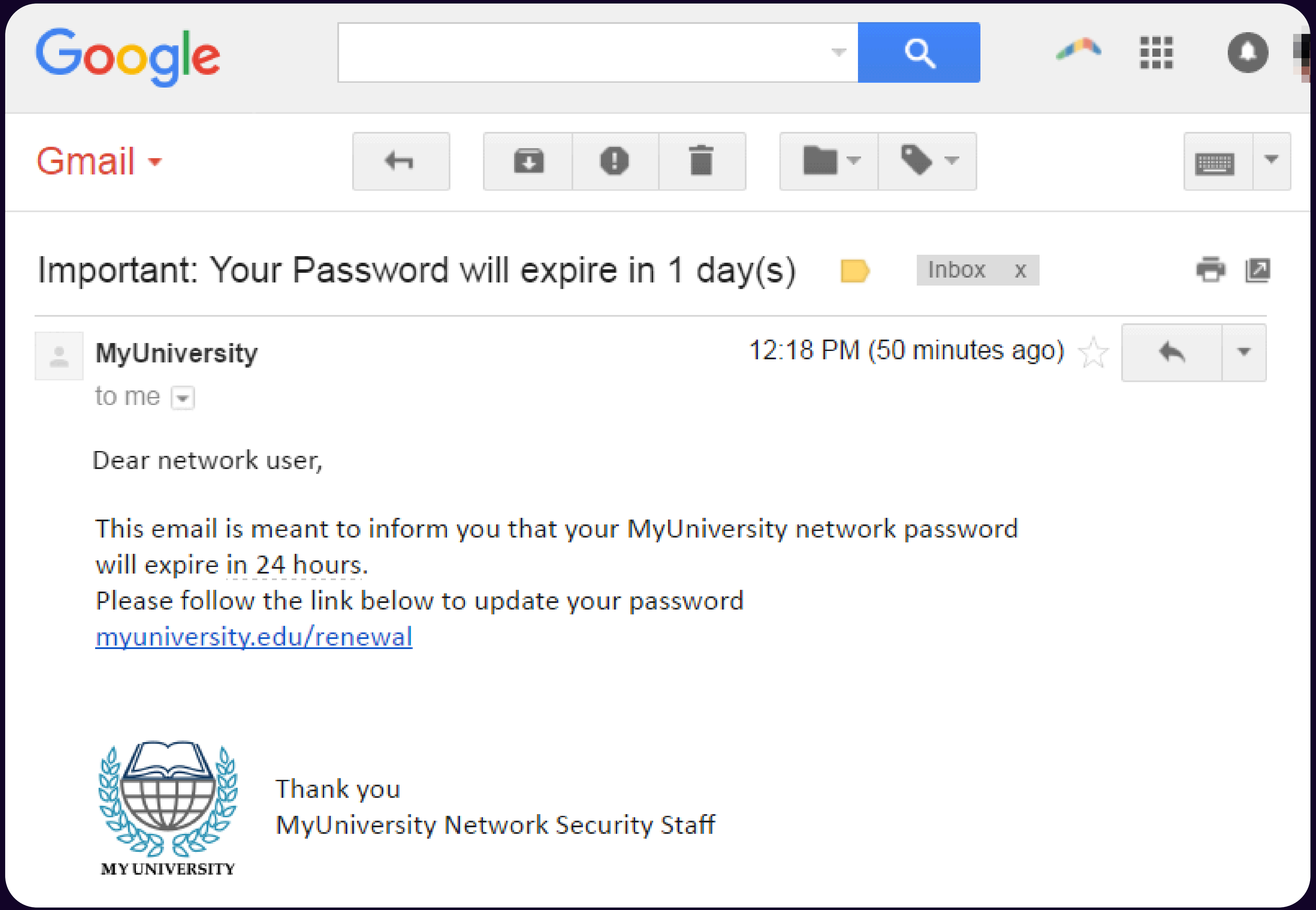


# Typs of Phishing Attacks



# Email Phishing

The most widely known form of phishing,this attack is an attempt to steal sensitive information via an email that appears to be from a legitimate organization.



Important: Your Password will expire in 1 day(s)

MyUniversity
to me

12:18 PM (50 minutes ago)

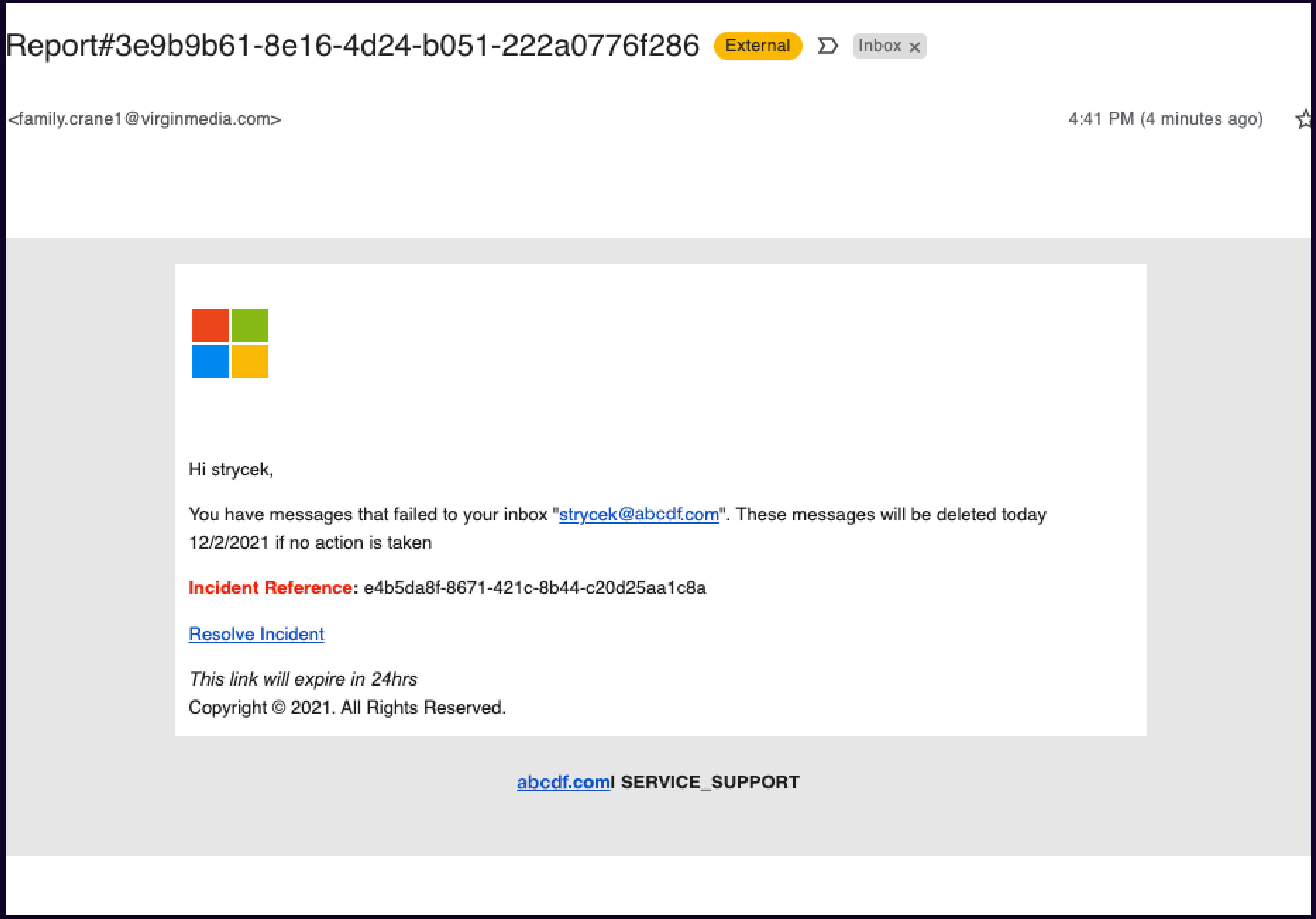
Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff

# Spear Phishing

These email message are sent to specific people within an organization, usually high privilege.



Report#3e9b9b61-8e16-4d24-b051-222a0776f286

<family.crane1@virginmedia.com> 4:41 PM (4 minutes ago)

Hi strycek,

You have messages that failed to your inbox "strycek@abcdf.com". These messages will be deleted today 12/2/2021 if no action is taken

**Incident Reference:** e4b5da8f-8671-421c-8b44-c20d25aa1c8a

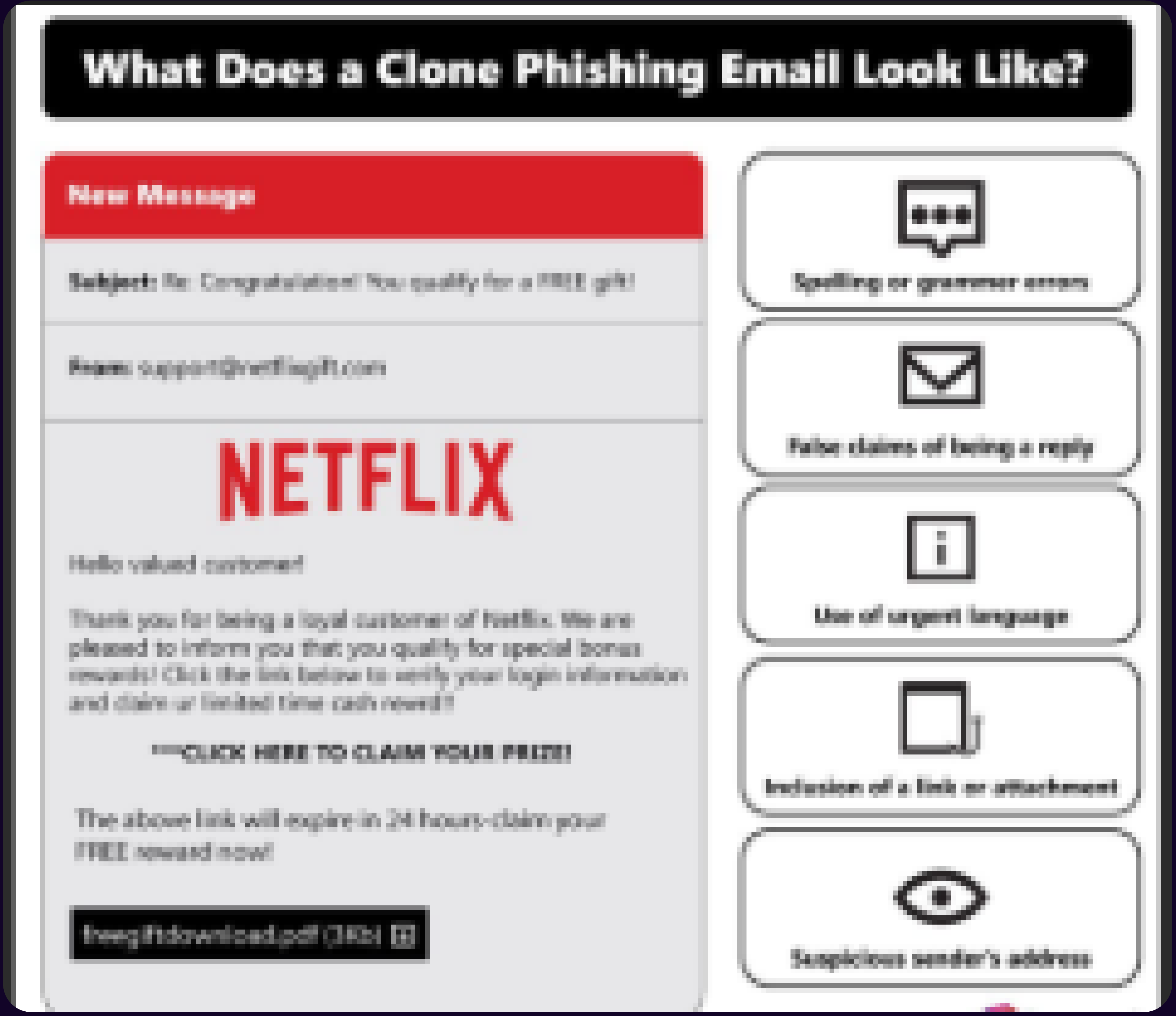
Resolve Incident

*This link will expire in 24hrs*
Copyright © 2021. All Rights Reserved.

abcdf.coml **SERVICE_SUPPORT**

# Clone  Phishing

In this type of phishing,the attacker clones a genuine or legitimate email that you might have received  from an authentic sender but sent from spoofed email id



What Does a Clone Phishing Email Look Like?

New Message

**Subject:** Re: Congratulation! You qualify for a FREE gift!

**From:** support@netflixgift.com

NETFLIX

Hello valued customer!

Thank you for being a loyal customer of Netflix. We are pleased to inform you that you qualify for special bonus rewards! Click the link below to verify your login information and claim ur limited time cash reward!!

***CLICK HERE TO CLAIM YOUR PRIZE!

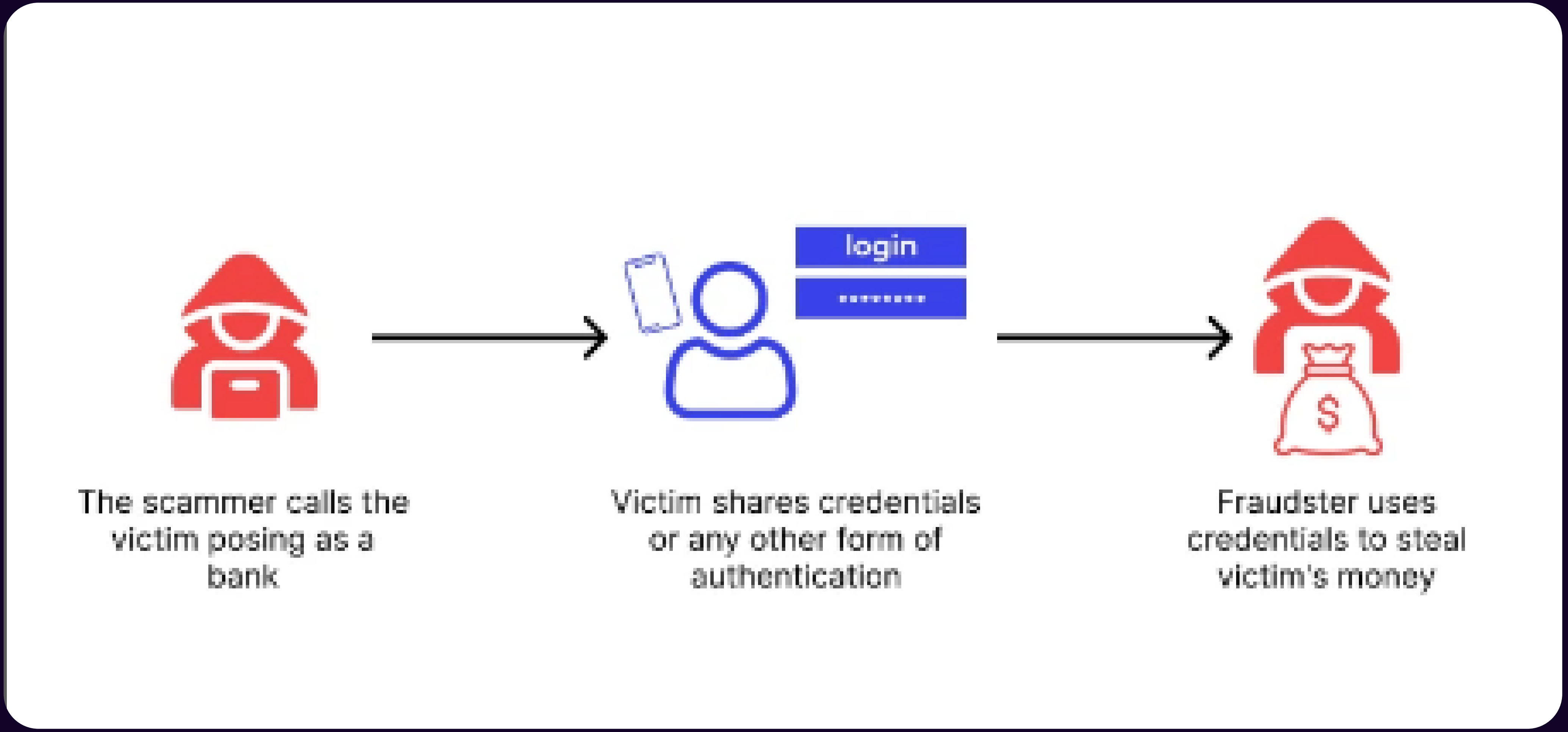
The above link will expire in 24 hours-claim your FREE reward now!

freegiftdownload.pdf (3Kb)

Spelling or grammar errors
False claims of being a reply
Use of urgent language
Inclusion of a link or attachment
Suspicious sender's address

# Voice Phishing

Vishing or voice phishing is the use of fraudulent phone calls to trick people into giving money or revealing personal information



The scammer calls the victim posing as a bank

Victim shares credentials or any other form of authentication

Fraudster uses credentials to steal victim's money

# Project Goal

The main objective of this project is to develop an **AI-powered system** that can automatically detect whether a given URL is **legitimate or a phishing attempt.** By using machine learning techniques, the system learns to identify patterns and characteristics commonly found in ph ishing URLs and flags them accordingly. This solution helps improve online safety by protecting users from fraudulent websites designed to steal personal or financial information.

**Key Features & Workflow:**

1. **User Input: URL Submission**
   - The user provides a URL through a simple web interface.
   - Example: http://secure-login.paytm-verification.com

2. Feature Extraction

- The system analyzes the URL using various rules and extracts relevant features that indicate suspicious behavior, such as:
    - Length of URL
    - Use of special characters (@, -)
    - Presence of IP address instead of domain
    - Use of HTTPS or not

3.Machine Learning Prediction

- A pre-trained Logistic Regression or SVM model processes these features.
- The model has learned from a labeled dataset of phishing and legitimate URLs.

4. Output & Explanation

- The system displays the prediction: "Phishing" or "Legit"
- Confidence score is shown (e.g., 97% Phishing)

# TOOLS:

## Tech Stack

- Frontend: HTML/CSS – Designs the user interface.
- Backend: Flask (Python) – Connects the frontend to the machine learning model.

## 🤖 ML Model

- Scikit-learn using SVM or Logistic Regression for classifying URLs as phishing or safe.

## 📊 Dataset

- Uses phishing datasets from UCI or Kaggle containing labeled data for training and testing the ML model.

# PREVENTIONS FROM PHISHING ATTACK

- Known what a phishing scam look like
- Don’t click on that link
- Don't give your info to undecured site
- Rotate your Password regulary
- install firewall
- install anti phishing software
- check mail or text on website

# 🌐 Real-World Use Cases

- Email Gateways: Scan incoming email links via Outlook/Gmail APIs.
- Browser Extensions: Warn users of suspicious URLs in real-time.
- Enterprise Firewalls: Block malicious sites on internal networks.
- Training Tools: Simulate phishing to educate employees.
- API for SaaS: Offer URL checking in antivirus, chat apps, CRMs. of body text

# 🚀 Future Enhancements

- ✅ File Scanning: Analyze email attachments for malware.
- ✅ NLP Analysis: Understand context and detect social engineering.
- ✅ Reputation Scoring: Use VirusTotal, WHOIS, and blacklists.
- ✅ Live Updates: Auto-train model with real-time threat feeds.
- ✅ Cloud + Feedback: Add a dashboard & user reporting system.t

# Thank you