CYBER CARNIVAL 2026

CYBER CARNIVAL

PROBLEM STATEMENT

URL SAFETY CHECKER

OUR PROBLEM REVOLVES AROUND:

- PHISHING ATTACKS INCREASED BY OVER 150% IN RECENT YEARS.
- FAKE URLS AND MALICIOUS WEBSITES ARE INCREASINGLY SOPHISTICATED.
- SMALL BUSINESSES AND STUDENTS LACK AFFORDABLE REAL-TIME PROTECTION TOOLS.
- EXISTING SOLUTIONS ARE EITHER:

1. EXPENSIVE
2. COMPLEX
3. NOT USER FRIENDLY

KEY ISSUE:

USERS CANNOT EASILY IDENTIFY WHETHER A URL IS MALICIOUS BEFORE CLICKING.

TEAM NAME

FORTIFI

BATCH

2025

CYBER CARNIVAL

TEAM MEMBER DETAILS

S.NO.	NAME	BATCH	REG. NO.	MAIL ID	MOBILE NO.
1.	SHRUTI MISHRA	2025	25BCY10042	SHRUTI.25BCY10042@GMAIL.COM	7459810606
2.	DHANRAJ CHOUDHARY	2025	25BCE10624	DHANRAJ.25BCE10624@GMAIL.COM	9326388093
3.	C. SAHASRA LAKSHMI	2025	25BCY10241	SAHASRA.25BCY10241@GMAIL.COM	7302037061
4.	KUMARI LAXMI	2025	25BCY10206	KUMARI.25BCY10206@GMAIL.COM	9204024476

CYBER CARNIVAL

SCALABLE & FUTURE-READY ARCHITECTURE

IDEATION

VERIWEB IS AN INTELLIGENT WEB-BASED URL SAFETY ANALYSIS SYSTEM THAT EVALUATES SUSPICIOUS LINKS BEFORE USERS CLICK THEM. IT COMBINES RULE-BASED DETECTION, HEURISTIC ANALYSIS, AND THREAT INTELLIGENCE APIS TO CLASSIFY URLS AS SAFE, SUSPICIOUS, OR MALICIOUS.

WHAT THE USER HAS TO DO?

1. COPIES A LINK
2. PASTES IT TO VERIWEB
3. CLICKS TO CHECK

WHAT VERIWEB DOES?

1. CHECKS IF THE LINK LOOKS SUSPICIOUS
2. GIVES A SAFETY SCORE
3. TELLS USER IF IT IS SAFE OR RISKY
4. SUGGESTS WHAT TO DO NEXT

HOW IS OUR SOLUTION UNIQUE?

1. EASY TO USE FOR ANYONE
2. NO INSTALLATION NEEDED
3. WORKS IN REAL TIME
4. GIVES CLEAR RESULTS
5. USES SMART CHECKING INSTEAD OF FIXED RULES

HOW THE CHECKING WORKS?

1. LENGTH OF URL
2. TOO MANY DOTS IN LINK
3. MISSING HTTPS
4. SUSPICIOUS WORDS IN LINK

CYBER CARNIVAL

METHODOLOGY

REPOSITORY LINK :

HTTPS://GITHUB.COM/SAHASRA25BCY10241-KALI/FORTIFI_HACKATHON:

USER INPUT

THE USER ENTERS A WEBSITE LINK INTO THE FORTIFI SYSTEM. THIS LINK IS SUBMITTED FOR SAFETY CHECKING.

URL PROCESSING

THE SYSTEM CLEANS THE LINK AND PREPARES IT FOR ANALYSIS. UNNECESSARY SPACES OR FORMATTING ISSUES ARE REMOVED.

FEATURE EXTRACTION

THE SYSTEM CHECKS IMPORTANT DETAILS LIKE URL LENGTH, SYMBOLS, AND STRUCTURE. THESE DETAILS HELP IDENTIFY SUSPICIOUS PATTERNS.

PATTERN ANALYSIS

THE LINK IS COMPARED WITH PATTERNS FROM KNOWN SAFE AND UNSAFE WEBSITES. THIS HELPS DETECT POSSIBLE PHISHING BEHAVIOR.

PREDICTION

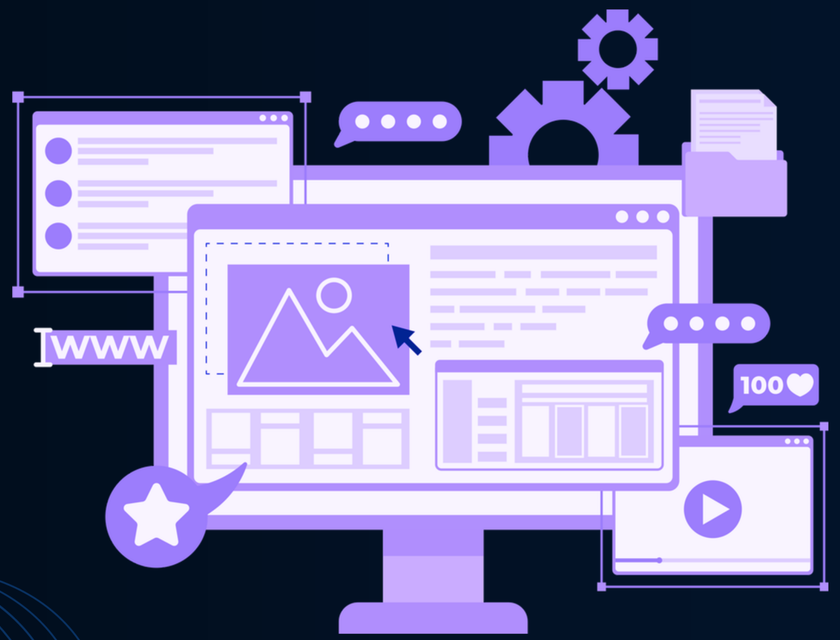
THE TRAINED SYSTEM PREDICTS WHETHER THE LINK IS SAFE OR UNSAFE.
IT USES LEARNED DATA FROM PREVIOUS EXAMPLES.

RISK EVALUATION

THE TRAINED SYSTEM PREDICTS WHETHER THE LINK IS SAFE OR UNSAFE.
IT USES LEARNED DATA FROM PREVIOUS EXAMPLES.

CYBER CARNIVAL

TECHNICAL APPROACH



PROGRAMMING LANGUAGE: PYTHON

USER INTERFACE: STREAMLIT

CODING: VS CODE

MANAGING LIBRARIES: ANACONDA

LIBRARIES USED:

- NUMPY
- PANDAS
- SCIKIT-LEARN
- STREAMLIT
- MATPLOTLIB
- RE (REGULAR EXPRESSIONS)

CYBER CARNIVAL

FEASIBILTY AND VIABILITY

IS IT FEASIBLE?

EASY DEVELOPMENT
- USES SIMPLE PYTHON LIBRARIES
- BEGINNER-FRIENDLY TOOLS
- NO COMPLEX HARDWARE REQUIRED

LOW COST
- USES FREE DATASETS
- OPEN-SOURCE SOFTWARE
- NO PAID TOOLS NEEDED

TIME MANAGEABLE
- SIMPLE STEP-BY-STEP PROCESS
- EASY TESTING AND IMPROVEMENT

IS IT VIABLE?

REAL-WORLD NEED
- CYBER FRAUD IS INCREASING
- MANY USERS NEED PROTECTION
- GROWING DEMAND FOR ONLINE SAFETY

TARGET USERS
- STUDENTS
- ELDERLY PEOPLE
- SMALL BUSINESSES
- GENERAL INTERNET USERS

FUTURE GROWTH
- CAN BECOME BROWSER EXTENSION
- CAN EXPAND TO MOBILE APP
- CAN ADD MORE SECURITY FEATURES

CYBER CARNIVAL

RISKS & CHALLENGES

POSSIBLE RISKS & CHALLENGES

- NEW FAKE WEBSITES APPEAR DAILY
- SOME SAFE SITES MAY LOOK UNSAFE
- DATA NEEDS REGULAR UPDATES

HOW WE HANDLE THEM?

- UPDATE DATA REGULARLY
- IMPROVE CHECKING METHODS
- ADD MORE FEATURES IN FUTURE

CYBER CARNIVAL

TARGET AUDIENCE

WHO IS THE TARGET AUDIENCE?

MOST PEOPLE CANNOT READ A URL AND SPOT A HIDDEN IP ADDRESS OR A "HOMOGRAPH" ATTACK (WHERE 'A' IS REPLACED BY A CYRILLIC CHARACTER). THIS TOOL ACTS AS A TRANSLATOR, CONVERTING COMPLEX TECHNICAL SIGNALS INTO A SIMPLE "SAFE" OR "SUSPICIOUS" VERDICT. IT BRIDGES THE GAP BETWEEN TECHNICAL SECURITY AND USER PERCEPTION.

STUDENTS

ELDERLY PEOPLE

NON TECHNICAL INDIVIDUALS

CYBER CARNIVAL

IMPACT & BENEFITS

IMPACT

- REDUCES PHISHING VICTIMIZATION
- ENCOURAGES RESPONSIBLE BROWSING
- IMPROVES CYBERSECURITY LITERACY

BENEFITS

- SOCIAL: SAFER DIGITAL INTERACTIONS
- EDUCATIONAL: CYBER AWARENESS
- ECONOMIC: PREVENTION OF FINANCIAL FRAUD

CYBER CARNIVAL

SCOPE OF PROJECT

IN SCOPE:

- ANALYZING THE URL STRING FOR LENGTH, SPECIAL CHARACTERS, AND SUSPICIOUS KEYWORDS.
- DETECTING IP ADDRESSES DISGUISED AS DOMAIN NAMES.
- IDENTIFYING COMMON URL SHORTENING SERVICES.
- GENERATING A PRINTABLE REPORT OF THE RISK FACTORS.

OUT OF SCOPE (FOR THIS VERSION):

- REAL-TIME SCANNING OF THE WEBSITE'S CONTENT (E.G., DOWNLOADING FILES)
- MACHINE LEARNING-BASED PREDICTION (PLANNED FOR FUTURE UPDATES).
- INTEGRATION WITH LIVE BROWSER EXTENSIONS

CYBER CARNIVAL

RESEARCH & REFERNCES

- OWASP PHISHING PREVENTION GUIDELINES
- GOOGLE SAFE BROWSING DOCUMENTATION
- WHOIS DOMAIN INFORMATION PROTOCOL

OPEN SOURCE USED:

- PYTHON REQUESTS LIBRARY
- REGEX LIBRARIES
- URL PARSING LIBRARIES
- FLASK / NODE FRAMEWORKS

CYBER CARNIVAL

FREQUENTLY ASKED QUESTIONS

HOW IS OUR SOLUTION DIFFERENT FROM ANTIVIRUS SOFTWARE?

- ANTIVIRUS WORKS AFTER INFECTION.
- OUR SYSTEM WORKS AT THE FIRST POINT OF INTERACTION – THE URL.
- IT IS PREVENTIVE, LIGHTWEIGHT, AND EDUCATIONAL.

HOW ACCURATE IS OUR URL CLASSIFICATION?

- USES MULTIPLE RULE-BASED SECURITY PARAMETERS.
- RISK SCORING SYSTEM REDUCES FALSE CLASSIFICATION.
- CAN BE ENHANCED WITH ML FOR IMPROVED ACCURACY.
- DESIGNED AS AN AWARENESS + DETECTION TOOL, NOT A REPLACEMENT FOR ENTERPRISE SECURITY.

WHY DID WE CHOOSE PYTHON AND STREAMLIT?

- PYTHON ENABLES FAST STRING PROCESSING AND PATTERN DETECTION.
- STREAMLIT ALLOWS RAPID DEPLOYMENT OF INTERACTIVE WEB APPS.
- LIGHTWEIGHT ARCHITECTURE — NO HEAVY FRONTEND FRAMEWORKS REQUIRED.

CAN THIS SYSTEM DETECT ALL PHISHING URLS?

- NO SYSTEM CAN GUARANTEE 100% DETECTION.
- OUR RULE-BASED MODEL DETECTS COMMON PHISHING PATTERNS.
- FUTURE INTEGRATION WITH THREAT INTELLIGENCE APIS CAN ENHANCE COVERAGE.

HOW CAN THIS PROJECT BE SCALED FURTHER?

- CONVERT INTO A BROWSER EXTENSION.
- INTEGRATE WITH GOOGLE SAFE BROWSING API.
- ADD MACHINE LEARNING-BASED CLASSIFICATION.
- DEPLOY ON CLOUD PLATFORMS.
- CREATE A MOBILE-FRIENDLY VERSION.

CYBER CARNIVAL

SUMMARY

THE 'URL SAFETY CHECKER' IS A HIGHLY FEASIBLE PROJECT FOR A FIRST-YEAR STUDENT AS IT RELIES ON OPEN-SOURCE TECHNOLOGY AND STANDARD LOGIC WITHOUT REQUIRING COSTS OR HIGH-END HARDWARE. IT IS VIABLE BECAUSE IT ADDRESSES THE CRITICAL, REAL-WORLD PROBLEM OF PHISHING WITH A LIGHTWEIGHT, USER-FRIENDLY SOLUTION. WHILE IT HAS LIMITATIONS LIKE HANDLING SHORTENED URLS, THESE CAN BE MITIGATED THROUGH A ROBUST SCORING SYSTEM AND FUTURE UPDATES.

Thank You!