

CyberGuard



A intelligent, robust suite for modern security integrity scans and phishing threat detection/Prevention



By: DK, Joyce, Zippy, Karanja and Nissi

27 January, 2026

Overview

01 Introduction

02 The Problem

03 Objectives

04 Methodology

05 Analysis

06 Phishing Results

07 Conclusion

08 END



Introduction

Welcome to CyberGuard, your personal security auditor for the modern web. In an era where an 8-character password can be cracked in mere minutes, we believe that security should not be a luxury—it should be a standard.

Our project, provides instant feedback on digital safety. Whether you are checking the strength of a new password or scanning a suspicious URL for phishing indicators, CyberGuard delivers the intelligence you need to stay ahead of evolving threats

The Problem

- **The Blacklist Failure:** Every day, over 560,000 new pieces of malware are detected. Because traditional blacklists only store "known" bad items, they often stop only 19% of modern threats, leaving a massive security gap for new attacks
- **The Human Vulnerability:** Password habits are at an all-time low—94% of users reuse the same password across multiple accounts. This has led to a surge in brute-force attacks, which now account for 37% of all successful web breaches
- **The AI Threat: Phishing** is getting harder to spot; AI-generated phishing emails now have a 54% click-through rate, compared to just 12% for human-written ones.



Objective

Design a smart system to solve a real world problem

For students to understand advanced computing concepts and how system development leads to intelligent solutions



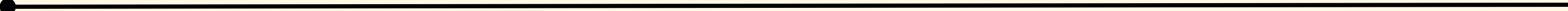
Methodology

Heuristic Intelligence (The Brain)

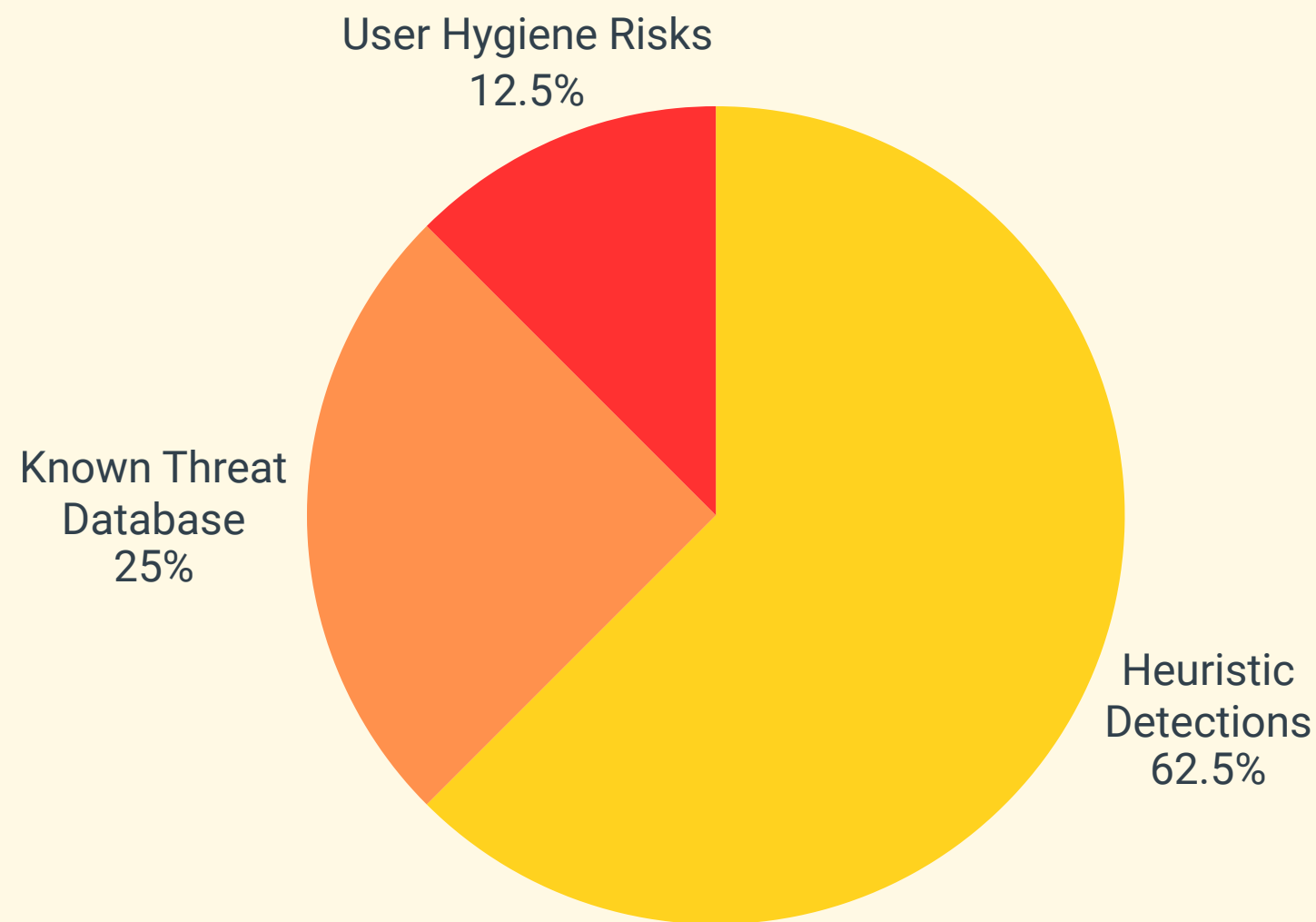
We use Regular Expressions (Regex) as "digital stencils" to analyze the DNA of a threat in real-time. Instead of checking a list, our engine recognizes suspicious patterns and complexity instantly, allowing the app to catch unknown threats that blacklists miss.

Cryptographic Rigor (The Shield)

We leverage the `window.crypto` API to pull high-entropy noise from system hardware. This ensures that every key generated is "Cryptographically Secure" (CSPRNG), reaching over 104 bits of entropy—making it mathematically unguessable by modern computers.

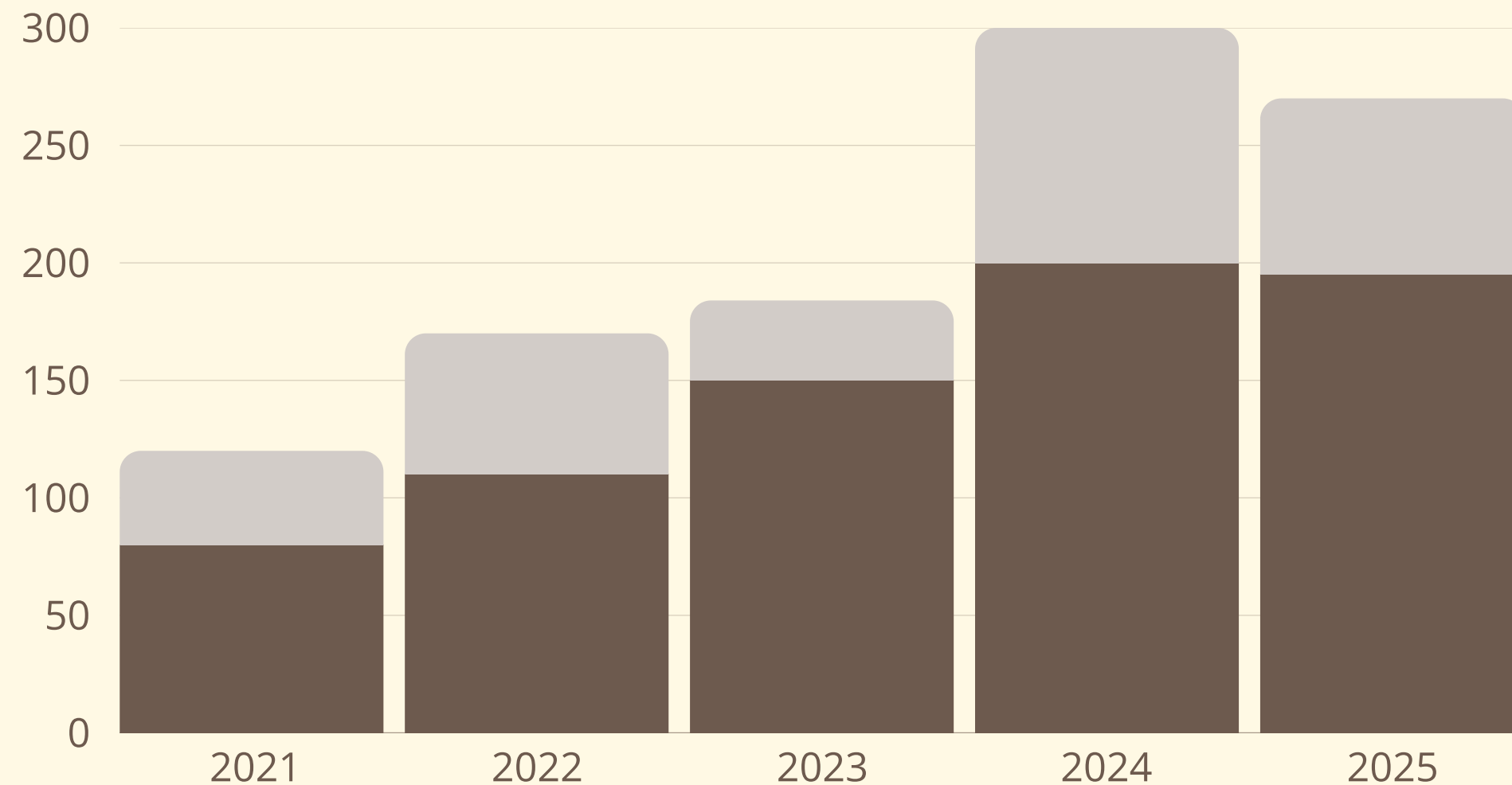


Audit Result Analysis



- **Heuristic Detection (62.5% - Yellow):** This represents the "Zero-Day" and brand-new threats caught by our Pattern Recognition engine. While traditional tools miss these, our heuristics identify them by their suspicious "DNA".
- **Known Threat Database (25% - Orange):** This covers "Signature Matching"—checking against established blacklists of known malicious URLs and passwords that have already been cataloged.
- **User Hygiene Risks (12.5% - Red):** These are critical vulnerabilities found in the user's behavior, such as password reuse (which affects 94% of people) or high "shoulder surfing" risks

The Phishing Surge (2021–2025)



- 2021 | The Rise to #1: Phishing officially became the most reported cybercrime globally, claiming 50% of all internet crime victims.
- 2022 | The AI Pivot: The "ChatGPT Era" began. Phishing volume skyrocketed as scammers used Generative AI to eliminate typos and create perfect social engineering lures.
- 2023 | The 1,200% Surge: Attack frequency exploded. AI tools allowed attackers to bypass traditional security filters at a scale never seen before.
- 2024 | Quality Over Quantity: While mass spam slowed, "Spear Phishing" (targeted attacks) became more lethal, driving the average breach cost to a staggering \$4.88 million.
- 2025 | The Deepfake Era: By Q1 2025, attacks hit record highs. The primary threat has shifted to AI-driven voice and video "Deepfakes," leading to a projected 400% rise in successful scams.

Conclusion

CyberGuard successfully bridges the gap between high-level security protocols and everyday user habits. By simplifying password and URL auditing, we have transformed complex data into actionable safety measures, proving that users don't need to be security experts to stay protected—they just need the right tools

The digital landscape is constantly evolving, and threats are becoming more sophisticated. We believe that security should not be a luxury; it should be a standard. Knowledge is the best defense, and understanding the "why" behind security is the first step toward true safety

Developed by DK, Joyce, Zippy, Karanja, and Nissi, this project serves as a foundational step toward a more transparent digital ecosystem. We empower users to identify vulnerabilities—from brute-force math to deceptive phishing domains—before they can be exploited

Stay proactive, stay curious, and continue auditing your digital presence. Thank you for joining us in our mission to make the web a safer place, one scan at a time.



Thank You

Presented By: DK, Joyce, Zippy,
Karanja & Nissi

[Check our Web Page here →](#)