

Cybersecurity: Training Simulator for Cyber Security Employee

Students: Manuel Conrad, Isis Gomez, Michael Novas, Kirei Hausheer, Joaquin Prado
Instructor/Faculty: Masoud Sadjadi Florida International University



PROBLEM

Modern organizations face rising employee-targeted cyberattacks, including phishing, credential theft, and malware.



REQUIREMENTS

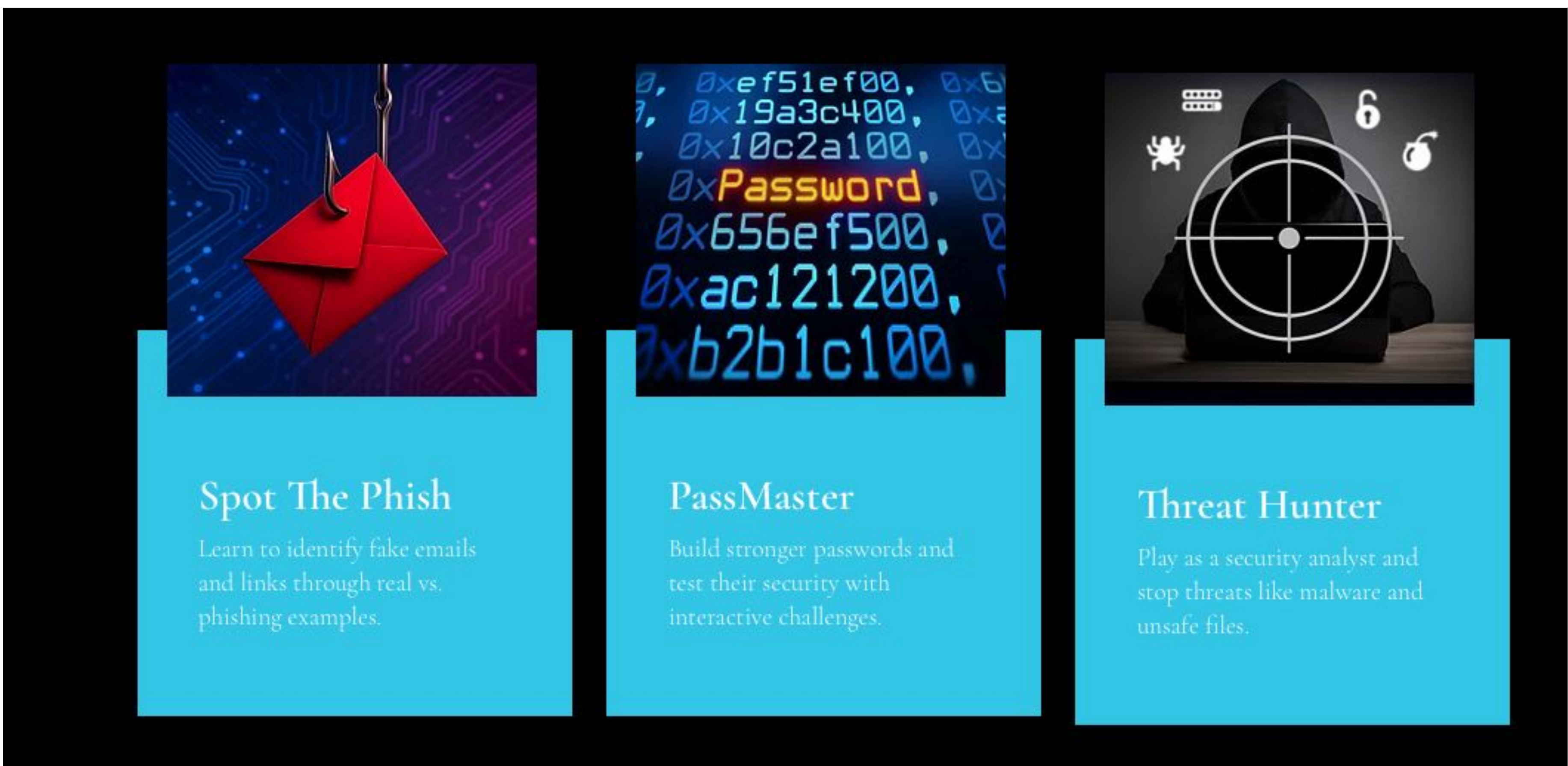
Many Cybersecurity threats like phishing and password misuse remain common among employees. Traditional training methods often lack engagement or practical context.

CURRENT SYSTEM

Traditional training is passive, outdated, and ineffective at building real-world recognition skills.

Employees need interactive, scenario-based training that develops practical instincts.

OBJECT DESIGN



SYSTEM DESIGN

- Web-based interface optimized for desktops
- Modular system: phishing, password, and threat finding
- Feedback is given and corrective information is provided if necessary
- UI accessible across browsers and screen sizes

SUMMARY

The **Cybersecurity Training Simulator** is a gamified educational tool that prepares employees for real-world cyber threats. It emphasizes learning through action and reinforces knowledge with scoring, feedback, and progress logs.

VERIFICATION

- Peer testing confirmed realistic phishing detection and flow
- Accessibility verified via manual checks and tools
- Feedback gathered during review and demo sessions
- All modules passed functional, usability, and performance testing

Team Contribution

The simulator was built across 6 agile sprints, each with a clear objective:

- Isis and Manuel:** Website design, phishing engine
- Joaquin:** Threat Hunter module, scenario design, and gameplay logic.
- Michael and Kirei:** Password strength tester, logic validation, accessibility checks, and testing *workflows*.