**AI-Powered Fake Login Page Detection (Phishing Hunter): A Review of State-of-the-Art Research**

The growing sophistication of phishing attacks—especially through deceptive login pages—has led to the emergence of artificial intelligence (AI) as a critical defense mechanism. This review synthesizes key research contributions that explore the design and deployment of AI-based systems for detecting fake login interfaces, often referred to as "Phishing Hunters." These systems leverage advanced machine learning techniques, including deep neural networks and natural language processing, to identify fraudulent pages with high precision and real-time capability.

**1. Deep Learning for Visual Phishing Detection: Identifying Fake Login Pages in Real-Time**

* **Authors**: David Oluremi
* **Published**: April 2025
* **Abstract**: This study introduces a convolutional neural network (CNN)-based model designed to detect fake login pages by analyzing visual elements such as layout structure, color schemes, and logo positioning. The system demonstrates real-time detection capabilities with over 95% accuracy, making it suitable for integration into browsers and security platforms.
* **Link**: [ResearchGate](https://www.researchgate.net/publication/390883004)

**2. AI-Based Phishing Detection Using Multi-Feature Analysis**

* **Published**: March 2025
* **Abstract**: This paper investigates the application of AI algorithms to detect phishing websites based on URL features, SSL certificate validation, domain age, and content semantics. The integration of image recognition and NLP techniques allows the system to detect spoofed elements and misleading textual cues effectively.
* **Link**: [IJRPR](https://ijrpr.com/uploads/V6ISSUE3/IJRPR41047.pdf)

**3. Phish-Defence: Malicious URL Detection via Deep Recurrent Neural Networks**

* **Authors**: Aman Rangapur, Tarun Kanakam, Dhanvanthini P
* **Published**: October 2021
* **Abstract**: Focused on lightweight and high-speed phishing detection, this paper presents an RNN-based model that analyzes URL strings without requiring external metadata. The method is optimized for edge computing, offering reliable zero-day phishing detection across low-resource devices.
* **Link**: [arXiv](https://arxiv.org/abs/2110.13424)

**4. WebPhish: Detecting Phishing Web Pages via Embedded URL and HTML Analysis**

* **Authors**: Chidimma Opara, Yingke Chen, Bo Wei
* **Published**: November 2020
* **Abstract**: WebPhish employs an end-to-end deep neural network trained on embedded representations of raw URLs and HTML content. By modeling character-level semantic dependencies, the system achieves a detection accuracy of 98.1%, outperforming conventional phishing detection methods.
* **Link**: [arXiv](https://arxiv.org/abs/2011.04412)

**5. HTMLPhish: Deep Learning-Based Detection Using Raw HTML Content**

* **Authors**: Chidimma Opara, Bo Wei, Yingke Chen
* **Published**: August 2019
* **Abstract**: HTMLPhish introduces a CNN-based framework for phishing detection through direct analysis of HTML documents. The system effectively captures the structural and semantic patterns of phishing content and achieves a classification accuracy of over 93% across a dataset of 50,000+ webpages.
* **Link**: [arXiv](https://arxiv.org/abs/1909.01135)

**Conclusion**

AI-driven phishing detection systems represent a significant leap forward in cybersecurity. The reviewed literature highlights the effectiveness of combining visual analysis, textual semantics, and structural heuristics to detect deceptive login interfaces. These approaches not only enhance accuracy and response time but also pave the way for scalable and robust browser-integrated defense solutions.