**Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis**

**Author**: Sandhya Mishra, Devpriya Soni

From: ELSEVIER 2020

**Abstract:**

Smartphones' popularity and internet connectivity make them susceptible to phishing and smishing. Our 'Smishing Detector' model minimizes false positives in identifying malicious messages, using modules like SMS Content Analyzer, URL Filter, Source Code Analyzer, and APK Download Detector. Experimental results show a strong 96.29% accuracy, outperforming other security models. This system provides effective protection against mobile phishing and smishing attacks.

**Introduction:**

During smishing, attackers design the user interface wisely so that the user is unable to identify the minor differences between a legitimate website and fake website created by the attacker. They copy the source code of the legitimate website to create a fake web page that will look similar to a legitimate web page but these websites could re-direct the user to other malicious links. Also, attackers modify the URL to create a fake URL that looks like URL of a legitimate website.

A diagram of a computer program

Description automatically generated with medium confidence

**Proposed work:**

SMS Content Analyzer verifies the presence of URL, self an- swering link (SAL), phone number and email id in the SMS. Messages containing URL or SAL are transferred to URL Filter. Messages containing email id and phone number are processed for blacklist check. Then messages are forwarded for text pre- processing.

A diagram of a computer program

Description automatically generated

* Source code analyzer
* APK Download Detector
* URL filter

**Implementation result and evaluation:**

* A smishing detection system, built in Python with Jupyter Notebook, tackles fraudulent messages aiming to steal user data.
* It utilizes four modules:
* SMS Content Analyzer: Examines message content for suspicious keywords and phrases linked to smishing.
* URL Filter: Checks URLs against blacklists of known malicious sites.
* Source Code Analyzer: Scans source code of attached APK files for hidden threats.
* APK Download Detector: Downloads and analyzes APK files linked in messages.
* The system leverages a custom dataset of 5858 messages, including 538 smishing attempts and 5320 legitimate messages.
* Evaluation reveals an impressive 98.5% accuracy in identifying smishing messages.
* This multi-pronged approach combats diverse smishing tactics, including URL manipulation and malicious file downloads.
* Beyond keyword analysis, the system delves deeper into URLs, source code, and APK files for comprehensive detection**.**

A screenshot of a computer

Description automatically generated

**Screens screenshot of a computer

Description automatically generated**

**Comparative analysis:**

Goel et al.'s Smishing Classifier lacks false-positive elimination, categorizing legitimate APK downloads as smishing. Further verification of website legitimacy is crucial, as login pages and self-answering links from trusted sources may trigger false positives. Our proposed system includes user consent verification during APK downloads, a novel approach to mitigate false positives and enhance detection accuracy in mobile security**.**

**A screenshot of a computer

Description automatically generated**

**Conclusion and Future work:**

The paper presents Smishing Detector, using SMS content analysis and URL inspection to classify smishing messages. It includes modules like SMS Content Analyzer, URL Filter, Source Code Analyzer, and APK Download Detector, achieving 96.29% accuracy with Naive Bayes. Compared to existing models, it offers heightened security against smishing attacks. Future plans involve integrating additional security measures like a Malware detector to enhance application security and prevent personal information leakage. Practical implementation on the Android platform is envisioned, offering real-time smishing detection and prevention.