* 1. **Classification of phishing attack techniques**
* Phishing websites are challenging to an organization and individual due to its similarities with the legitimate websites. There are forms of phishing attacks such as: (Các trang web lừa đảo gây khó khăn cho tổ chức và cá nhân do sự giống nhau với các trang web hợp pháp. Có các hình thức tấn công lừa đảo như sau:)
  + Technical subterfuge refers to the attacks include Keylogging, DNS poisoning, and Malwares. (Kỹ thuật lừa đảo liên quan đến các cuộc tấn công bao gồm Keylogging, DNS poisoning, và Malwares.)
  + In these attacks, attacker intends to gain the access through a tool / technique. On the one hand, users believe the network and on the other hand, the network is compromised by the attackers.
  + Social engineering attacks include Spear phishing, Whaling, SMS, Vishing, and mobile applications. (Các cuộc tấn công kỹ thuật xã hội bao gồm Spear phishing, Whaling, SMS, Vishing, và ứng dụng di động.)
  + In these attacks, attackers focus on the group of people or an organization and trick them to use the phishing URL.
* Apart from these attacks, many new attacks are emerging exponentially as the technology evolves constantly.

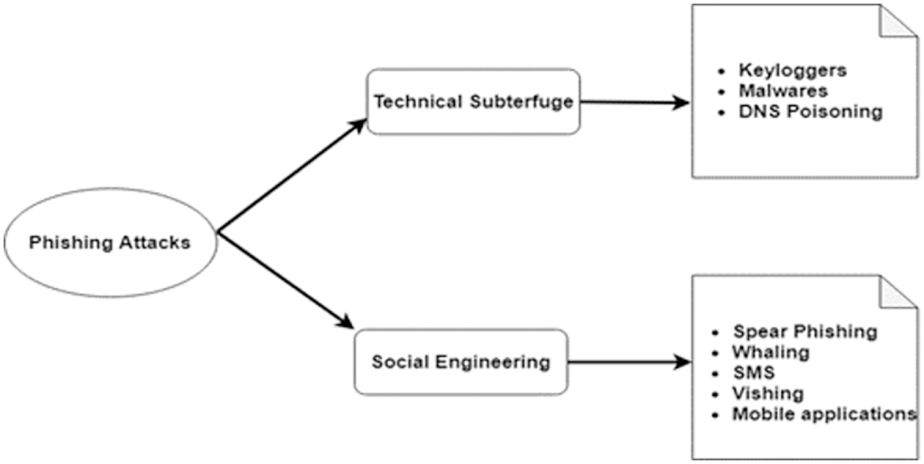


Image 1.2

* 1. **Phising detection approaches**

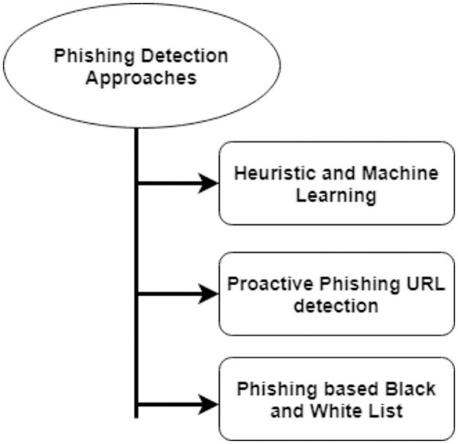


Image 1.3

* Heuristic and Machine Learning(Tiếp cận Hueristic và Học Máy):
  + Heuristic Approaches: These methods rely on predetermined rules or patterns to identify phishing attempts. This may involve analyzing various elements of emails or websites, such as URL structure, content, sender details, and visual indicators. (**Các Phương pháp tiếp cận Heuristic**: Những phương pháp này dựa vào các quy tắc hoặc mô hình đã được xác định trước để nhận diện các nỗ lực lừa đảo qua mạng của kẻ tấn công. Điều này có thể bao gồm việc phân tích các yếu tố khác nhau của email hoặc trang web, như cấu trúc URL, nội dung, chi tiết người gửi và các chỉ báo hình ảnh.) While heuristic approaches are easy to implement, they may struggle with detecting sophisticated attacks.
  + Machine Learning Approaches: Machine learning techniques can automatically learn patterns and attributes of phishing attacks from data. Features like email headers, URL properties, content, and sender details can be extracted and used to train machine learning models. (Các Phương pháp Học Máy: Các kỹ thuật học máy có thể tự động học các mẫu và thuộc tính của các cuộc tấn công phishing từ dữ liệu. Các đặc trưng như tiêu đề email, thuộc tính URL, nội dung, và chi tiết người gửi có thể được trích xuất và sử dụng để huấn luyện các mô hình học máy.) Models such as decision trees, random forests, support vector machines (SVM), or deep learning architectures can be utilized for classification. Machine learning approaches can adapt to evolving phishing tactics but necessitate labeled data for training.
* Proactive Phishing URL Detection: Proactive phishing URL detection entails identifying and blocking phishing URLs before they can reach potential victims. This typically involves continuously scanning the web for new phishing URLs and analyzing their characteristics to ascertain their malicious intent. (Phát hiện URL giả mạo một cách chủ động: Phát hiện URL giả mạo một cách chủ động liên quan đến việc xác định và chặn các URL giả mạo trước khi chúng có thể tiếp cận nạn nhân tiềm năng. Điều này thường liên quan đến việc quét liên tục trên web để tìm các URL giả mạo mới và phân tích các đặc điểm của chúng để xác định ý định độc hại của chúng.)
* Methods such as web crawling, content analysis, and comparing similarities with known phishing URLs can be employed for proactive detection. Upon identification, phishing URLs can be added to blacklists or flagged for further examination.
* Phishing-based Black and White Lists:
  + Blacklists: These comprise known phishing URLs, domains, IP addresses, or sender email addresses. Continuously updated based on the latest phishing threats, blacklists are used to prohibit access to malicious resources. When an incoming email or website request matches an entry on the blacklist, it is identified as potential phishing and can be blocked or subjected to additional scrutiny.
  + Whitelists: These contain trusted URLs, domains, IP addresses, or sender email addresses known to be legitimate. Whitelisting aids in reducing false positives by permitting access solely to recognized safe resources. However, maintaining whitelists can be challenging due to the dynamic nature of the web, and it may not be suitable for all environments.
* Danh sách các trang web đen và trắng:
  + Danh sách đen: Bao gồm các URL, tên miền, địa chỉ IP hoặc địa chỉ email người gửi đã biết là giả mạo. Được cập nhật liên tục dựa trên các mối đe dọa giả mạo mới nhất, danh sách đen được sử dụng để cấm truy cập vào các nguồn tài nguyên độc hại. Khi một email đến hoặc yêu cầu trang web khớp với một mục trong danh sách đen, nó được xác định là giả mạo tiềm năng và có thể bị chặn hoặc chịu sự kiểm tra thêm.
  + Danh sách trắng: Chứa các URL, tên miền, địa chỉ IP hoặc địa chỉ email người gửi được biết là hợp pháp. Danh sách trắng giúp giảm thiểu các kết quả dương tính giả mạo bằng cách chỉ cho phép truy cập vào các nguồn tài nguyên an toàn đã được công nhận. Tuy nhiên, việc duy trì danh sách trắng có thể gặp khó khăn do tính chất động của web, và nó có thể không phù hợp với tất cả các môi trường.

1) Sự xuất hiện của địa chỉ IP trong URL:

Các trang web hợp pháp thường không sử dụng địa chỉ IP trong URL của họ để cho người dùng truy cập. Khi một địa chỉ IP được sử dụng trong URL, nó gợi ý ý định xấu, có thể nhằm mục đích đánh cắp dữ liệu nhạy cảm.

2) Sự xuất hiện của ký tự @ trong URL:

Kẻ lừa đảo đôi khi sử dụng ký tự “@” trong URL để lừa dối trình duyệt bỏ qua tất cả mọi thứ trước nó, chuyển hướng người dùng đến một địa chỉ có thể gây lừa đảo, thường nằm sau ký tự “@”.

3) Số lượng dấu chấm trong tên miền:

Các URL lừa đảo thường chứa nhiều dấu chấm. Ví dụ, trong URL: http://shop.fun.amazon.phishing.com, “phishing.com” là tên miền thực sự, trong khi việc bao gồm “amazon” nhằm mục đích lừa người dùng nhấp vào. Các URL lành tính thường có trung bình ba dấu chấm.

4) URL hợp pháp hiếm khi sử dụng dấu gạch nối:

Kẻ lừa đảo thường chèn dấu gạch nối (-) vào tên miền để tạo ra ấn tượng chính thống. Ví dụ, trang web thực tế là http://www.onlineamazon.com nhưng kẻ lừa đảo có thể tạo ra một trang web giả mạo khác như http://www.online-amazon.com để làm nhầm lẫn người dùng vô tội.

5) CHUYỂN HƯỚNG URL:

Sự xuất hiện của “//” trong đường dẫn URL cho thấy người dùng sẽ được chuyển hướng đến một trang web khác. Nếu “//” được tìm thấy trong đường dẫn URL, đây là đặc điểm của một URL giả mạo.

6) Token HTTPS trong URL:

Kẻ lừa đảo có thể thêm “token HTTPS” vào phần tên miền của URL để lừa dối người dùng, như trong ví dụ này: <http://https-www-paypal-it-mpp-home.soft-hair.com>.

7) Gửi thông tin qua email:

Các kẻ lừa đảo có thể sử dụng chức năng “mail()” hoặc “mailto” để chuyển hướng thông tin người dùng đến email cá nhân của họ. Nếu những chức năng này xuất hiện trong URL, thì đây là một dấu hiệu của phishing.

8) Dịch vụ TinyURL:

Dịch vụ TinyURL cho phép kẻ lừa đảo rút ngắn các URL dài của trang web lừa đảo để che giấu chúng. Mục tiêu là để chuyển hướng người dùng đến các trang web lừa đảo.

1. Khái niệm SVM:

SVM là một thuật toán học có giám sát được sử dụng cho phân loại và hồi quy. Ý tưởng cơ bản của SVM là tìm một siêu phẳng tốt nhất trong không gian nhiều chiều để phân tách hai lớp dữ liệu (ví dụ, hai lớp dữ liệu này được gán nhãn “lừa đảo” và “không lừa đảo”). Giả sử chúng ta có một tập dữ liệu về các trang web, trong đó mỗi trang web được mô tả bằng các đặc trưng(features) như độ dài đường dẫn, số lượng liên kết, tỷ lệ chữ viết hoa, v.v. SVM có thể học từ tập dữ liệu này để xây dựng một mô hình phân loại, dự đoán xem một trang web mới có khả năng là lừa đảo hay không dựa trên các đặc trưng tương tự.

1. Ứng dụng của SVM trong việc phát hiện các trang web lừa đảo:
   * 1. Phân loại nhị phân:

+ SVM là một thuật toán phân loại nhị phân, giúp phân loại dữ liệu thành hai lớp khác nhau (ví dụ: lừa đảo và không lừa đảo).

+ Trong trường hợp phát hiện trang web lừa đảo, SVM có thể được sử dụng để xác định xem một trang web có khả năng là lừa đảo hay không dựa trên các đặc trưng(features) của nó.

* + 1. Học từ dữ liệu huấn luyện:

+ SVM học từ dữ liệu huấn luyện, trong đó các trang web đã được gán nhãn (lừa đảo hoặc không lừa đảo) và tìm ra siêu phẳng tốt nhất để phân tách hai lớp dữ liệu.

* + 1. Đặc trưng của trang web:

+ SVM sử dụng các đặc trưng(features) của trang web (ví dụ: đường dẫn, nội dung, thông báo) để xác định xem trang web có khả năng là lừa đảo hay không.

* + 1. Ứng dụng thực tế:

+ SVM đã được áp dụng rộng rãi trong việc phát hiện trang web lừa đảo, email spam, phân loại văn bản, và nhiều lĩnh vực khác.

1. Các bước để phân loại các trang web là lừa đảo hoặc không lừa đảo dựa trên các đặc trưng của chúng:

+ Bước 1: Thu thập dữ liệu huấn luyện

* Chúng ta cần một tập dữ liệu gồm các trang web đã được gán nhãn là lừa đảo hoặc không lừa đảo.
* Mỗi trang web sẽ được biểu diễn bằng các đặc trưng như độ dài đường dẫn, số lượng liên kết, tỷ lệ chữ viết hoa, v.v.

+ Bước 2: Tiền xử lý dữ liệu

* Chúng ta sẽ chuẩn hóa và rút trích các đặc trưng từ URL của trang web.

+ Bước 3: Xây dựng mô hình SVM

* Chúng ta sẽ sử dụng SVM để tạo một mô hình phân loại.
* SVM tìm ra siêu phẳng tốt nhất để phân tách hai lớp dữ liệu (lừa đảo và không lừa đảo).

+ Bước 4: Huấn luyện mô hình

* Chúng ta sẽ huấn luyện mô hình SVM trên tập dữ liệu huấn luyện.

+ Bước 5: Dự đoán và đánh giá

* Chúng ta sẽ sử dụng mô hình đã huấn luyện để dự đoán xem một trang web mới có khả năng là lừa đảo hay không.
* Đánh giá hiệu suất của mô hình bằng các chỉ số như độ chính xác, độ nhạy, độ đặc hiệu, v.v.