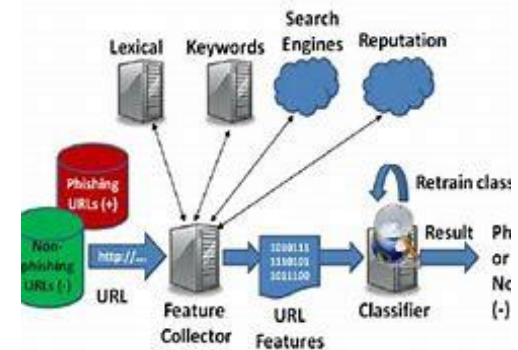


Define CS, fit into CC	<p>1. CUSTOMER SEGMENT(S) CS</p> <p>Protect yourself and your family against malicious websites with the platform for free.</p> <p>With the platform, protecting your staff, data, brand, and your customer from malicious websites has never been easier.</p> <p>Proactively protect multiple customers against malicious websites at once with all-in-one platform. The platform can be used for government embeds to provide 100% security and privacy.</p>	<p>6. CUSTOMER CONSTRAINTS CC</p> <p>An exhaustive systematic search was performed on all the indexing databases. The state-of-the-art research related to the web phishing detections was collected.</p> <p>The papers were classified based on methodologies. A taxonomy was derived by performing a deep scan on the classified papers.</p> <p>The contributions listed in this survey are exhaustive and lists all the state-of-the-art development in this area.</p>	<p>5. AVAILABLE SOLUTIONS AS</p> <p>Legitimate websites prevent web scraping by several techniques in respect to obfuscation using CSS sprites to display important data, replacing text with images.</p> <p>Spam filtering techniques are used to identify unsolicited emails before the user reads or clicks the link.</p> <p>When the website detects that the IP address and device information of the user who is logging in does not match the commonly used information, it is necessary to verify the authenticity of the user</p>	Explore AS, differentiate
Focus on J&P, tap into BE, understand RC	<p>2. JOBS-TO-BE-DONE / PROBLEMS J&P</p> <p>This article is the first of a series of three related to the challenges that we faced to detect phishing attacks at scale with constraints on accuracy and performance.</p> <p>In this article, we will describe how—starting mainly from the email stream—we identify suspicious links and then fetch the content from the associated webpages.</p> <p>In the next article, we will describe how suspicious webpages are analyzed and assessed in real-time, with a focus on Supervised Learning techniques.</p>	<p>9. PROBLEM ROOT CAUSE RC</p> <p>A phishing attack is a type of cybersecurity threat that targets users directly through email, text or direct messages.</p> <p>During one of these scams, a cybercriminal will pose as a trusted contact to steal data from an unsuspecting user such as login information, account numbers and credit card information.</p> <p>While there are several types of phishing, the main purpose behind all of them is it to steal sensitive information or transfer malware</p>	<p>7. BEHAVIOUR BE</p> <p>Customers should take a “trust no one” approach when opening email. Check and verify the “From” address of the email. By carefully reading the email copy, users can typically spot something that seems “off” including:</p> <p>An email with an “urgent” request or An email offering the user something that’s “too good to be true”. Check grammar and spelling. Poor grammar and misspelled words in an email can be red flags</p> <p>Avoid clicking links or attachments in emails from unfamiliar sources to the given solutions.</p>	Focus on J&P, tap into BE, understand RC
Identify strong TR & EM	<p>3. TRIGGERS TR</p> <p>I have found the following four psychological triggers that ecommerce platforms should adopt to increase customer urgency and drive sales: Utilize the personal touch, encourage loyalty Incentivize customers.</p> <p>4. EMOTIONS: BEFORE / AFTER EM</p> <p>Greed- Clicking on fake successful messages.</p> <p>Urgency-Hackers use fake security alerts with exclamation marks.</p> <p>Helpfulness-Hackers and cyber criminals use major tragedies to appeal for help but they are only helping themselves.</p>	<p>8.CHANNELS of BEHAVIOUR CH</p> <p>We would create an interactive and responsive website that will be used to detect whether a website is legitimate or phishing.</p> <p>This website is made using different web designing languages which include HTML, CSS, JavaScript and Python.</p> <p>This website is more useful to the user and it is user friendly also. This of course is why confidence tricks never work.</p>	<p>10. YOUR SOLUTION</p>  <p>The diagram illustrates the solution architecture. It starts with two input sources: 'Phishing URLs (+)' (red cylinder) and 'Non-phishing URLs (-)' (green cylinder). These feed into a 'URL' input, which then goes to a 'Feature Collector'. The 'Feature Collector' outputs 'URL Features' to a 'Classifier'. The 'Classifier' produces a 'Result' (Ph or Not) and a 'Retrain class' feedback loop. The 'Feature Collector' also receives input from 'Lexical', 'Keywords', 'Search Engines', and 'Reputation' sources.</p>	Identify strong TR & EM