Detecting Phishing Websites

Falestine Abusiam

April 9, 2025

CSIT 100

Have you ever clicked on a website that looked completely real, only to find out later it was fake? These fake sites are known as phishing websites. They're built to trick people into giving away personal information like usernames, passwords, credit card numbers, or even their social security numbers. The people who make these sites often copy the look of popular websites, like a bank or an online store, to make them look trustworthy. Once you enter your information, the scammers behind the website can steal it. Phishing has become one of the most common and dangerous online threats. As the internet becomes more important in our everyday lives for shopping, banking, school, and even doctor visits, phishing scams have more chances to fool people. These scams can lead to serious problems like identity theft, stolen money, and hacked accounts. That’s why it’s so important to find better ways to detect phishing websites quickly and accurately.

Older methods of detecting phishing websites relied on blacklists, lists of websites known to be dangerous. But this method isn’t perfect. Scammers constantly create new fake websites, and by the time one site is added to a blacklist, it might already be too late for someone who visited it. As IPQualityScore explained, “phishing websites often mimic well-known brands or platforms in an attempt to steal credentials or personal information” (IPQualityScore). Because of this, we need better tools to detect phishing websites in real time.“Advanced machine learning & AI phishing detection keeps your employees and clients fully protected from phishing attacks with real-time URL threat scanning.”This shows how powerful machine learning really is when it comes to stopping phishing threats. Tools like IPQS don’t just look at blacklists, they use live data and behavior analysis to scan websites in real time. This makes it much harder for scammers to sneak past defenses, even with new links that haven’t been used or seen before. Because of machine learning, systems like this can quickly spot risky patterns and respond faster than older security methods ever could.This is where machine learning can help. Machine learning is a type of artificial intelligence where computers learn to recognize patterns from data. Instead of being programmed with exact instructions, machine learning models are trained on examples. In phishing detection, they are trained on examples of both real websites and phishing websites, learning to tell the difference.

Barracuda Networks says that “AI-powered detection goes beyond known threats and can stop zero-day phishing attacks” (Barracuda Networks). A zero-day attack is a new scam that hasn’t been seen before, so older detection methods might miss it. Machine learning can catch these newer scams because it doesn’t rely on a simple list of known bad sites, it looks at patterns and behaviors instead.*“*Our AI engine detects and blocks socially engineered attacks in real-time, including spear phishing, business email compromise, and account takeover.”This highlights how machine learning is not only useful for detecting random phishing attempts, but also more targeted and dangerous scams. Spear phishing and business email compromise attacks are harder to catch because they often look like normal communication from someone you trust. Barracuda’s AI-powered tools analyze the content, sender behavior, and context of messages to spot signs that something isn’t right. This makes email protection much smarter and more effective, especially in business environments where a single mistake can lead to major security breaches.

So what exactly does a machine learning model look at when it’s checking if a site is safe or not? One clue is the URL, or website address. Check Point explains that “URL filtering involves examining the links included in an email for likely phishing pages. This includes known malicious URLs, lookalike URLs, or other URLs whose structure or content makes them suspicious”(Check Point). These strange details are hard for people to spot, but a machine learning model can analyze thousands of URLs quickly and accurately. URL filtering is a security technique that checks the links in an email to see if they might lead to dangerous websites. It looks for links that are already known to be harmful, links that try to mimic real websites, like using a slightly misspelled brand name, or links that have unusual structures that make them seem suspicious. This helps prevent users from clicking on phishing pages that could steal personal information or install malware. “Phishing emails commonly include embedded links that point toward phishing pages. These pages could be designed to trick the user into handing over their login credentials or may serve malware to the user.”These websites are made to look real so that users are tricked into entering their login information, passwords, or other personal details. In some cases, the site may also try to install malware on the user’s device. This is why it’s important to carefully check links in emails before clicking on them.

Another red flag is the way the site asks for information. ID Agent points out that phishing emails and websites often include “unexpected requests for personal information or login credentials,” and try to create a sense of urgency (ID Agent). For example, an email might say “Your account will be locked in 24 hours, click here to fix it.” Scammers do this to make people act without thinking. One of the primary signs of a phishing attempt is the use of urgent or threatening language “A common tactic used by phishers is to create a sense of urgency or fear. They might claim that your account has been compromised, or that you need to confirm your details immediately to avoid account closure or other negative consequences." ​This strategy pressures recipients into acting quickly without fully evaluating the legitimacy of the request. By understanding this tactic, individuals can be more cautious and discerning when confronted with such messages, thereby reducing the risk of falling victim to phishing scams.​

Perception Point highlights how sophisticated phishing websites have become. According to them, “some phishing websites use secure HTTPS protocols and display realistic-looking layouts and branding to mislead users” (Perception Point). This means that even if a website looks secure using the “https” in the address bar it might still be fake. That’s why we need smarter tools like machine learning to analyze more than just surface details. "Phishing is a form of cyberattack where attackers attempt to trick individuals into revealing sensitive information by impersonating a trustworthy entity via electronic communication."This definition underscores the deceptive nature of phishing attacks, highlighting how cybercriminals exploit trust to manipulate individuals into disclosing confidential data. By masquerading as legitimate organizations or contacts, these attackers craft convincing messages that prompt recipients to take actions such as clicking on malicious links or providing personal information. Understanding this tactic is crucial for developing effective detection and prevention strategies, as it emphasizes the importance of verifying the authenticity of communications and being cautious with unsolicited requests for sensitive information.​

To build a phishing detection system using machine learning, the first step is to gather a dataset. These datasets usually include a list of both legitimate websites and phishing websites. Each site in the dataset is labeled as either real or fake. Next, different features are extracted from the websites, such as the length of the URL, use of special characters, presence of HTTPS, and domain age. These features are then used to train machine learning models. Some of the most common models used in phishing detection include Decision Trees, Support Vector Machines (SVM), Logistic Regression, and Random Forests. Each of these models has strengths and weaknesses, but all of them are able to learn the patterns that separate phishing websites from real ones. Once the model is trained, it’s tested on new data that it hasn’t seen before. This helps check how well it can detect new phishing websites. The performance is measured using accuracy, how many sites it got right, precision, which is how many of the flagged sites were actually phishing , and recall how many of the phishing sites it caught. Many studies have shown that machine learning models can detect phishing websites with over 90% accuracy.

One of the great things about machine learning is that it improves over time. As more websites are analyzed and more data is collected, the models can continue learning and updating. This is very helpful because phishing techniques change quickly. A model that learns over time is more likely to keep up with new tricks and tactics. Python is one of the most popular programming languages used to build machine learning models. Libraries like scikit-learn, TensorFlow, and Keras make it easier to create, train, and test models. Researchers and cybersecurity professionals often use these tools to build systems that can scan websites in real-time. While machine learning offers many benefits, it’s not perfect. Models can make mistakes, especially if the training data is not high quality. For example, if the dataset is too small or doesn’t include a wide variety of phishing websites, the model might not learn very well. It’s important to make sure the training data is diverse and up to date.

Another issue is that some phishing websites are very well-made and don’t have obvious signs of being fake. These sites may pass basic checks, which means even advanced models need to work with other tools and security measures to be effective. Phishing detection works best when it combines machine learning with good cybersecurity habits, like checking the source of emails and not clicking on suspicious links. Large companies like Google, Microsoft, and Barracuda are already using machine learning in their email and web security tools. As mentioned earlier, Barracuda Networks says their AI-powered systems can detect new threats that older tools miss. This shows that machine learning is already making a real difference in the fight against phishing.

In addition to corporate tools, there are also open-source projects and academic studies exploring better phishing detection methods. These efforts are important because they help improve cybersecurity for everyone, not just large businesses. By sharing models, data, and research, the tech community can stay ahead of the criminals creating phishing websites. Another interesting development is the use of browser extensions that use machine learning to scan websites before you visit them. These extensions can check the URL, content, and structure of the page in real time and warn users if something seems suspicious. This helps protect users even if they don’t recognize the warning signs themselves. In schools, there’s also a growing interest in teaching students about phishing and cybersecurity. As more young people grow up using the internet, it’s important to help them understand how to stay safe online. Tools that use machine learning can be part of that education, showing how technology can be used for protection.

To sum it up, phishing websites are a major online threat, but machine learning gives us a powerful way to fight back. Instead of relying on slow, outdated tools like basic filters or blacklists, we can now use smart systems that actually learn and improve over time. These models don’t just react to known threats, they can recognize new scams by analyzing patterns, behaviors, and even subtle clues in website structures or URLs. That means they can catch scams faster and more accurately than ever before, even when dealing with completely new phishing tactics. As phishing scams continue to evolve and become more convincing, our defenses must evolve too. Machine learning offers a flexible, constantly improving solution that helps security systems stay one step ahead of attackers. When combined with user awareness, strong email filters, and good cybersecurity habits, machine learning can play a big role in protecting both individuals and businesses. Together, these tools and practices help make the internet a safer, more secure place for everyone.

# Works Cited

Barracuda Networks. “Phishing and Impersonation Protection.” Barracuda, https://www.barracuda.com/products/email-protection/phishing-protection.

Check Point. “Phishing Detection Techniques.” Check Point Software, https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/phishing-detection-techniques/.

ID Agent. “Key Indicators of Phishing.” ID Agent, https://www.idagent.com/blog/key-indicators-of-phishing/.

IPQualityScore. “Malicious URL Scanner & Threat Detection.” IPQualityScore, https://www.ipqualityscore.com/threat-feeds/malicious-url-scanner.

Perception Point. “Phishing Detection: Identifying Phishing Emails and Websites.” Perception Point, https://perception-point.io/guides/phishing/phishing-detection-identifying-phishing-emails-and-websites/.