PROBLEM STATEMENT

Phishing has been a major issue for security for a long time without a good solution in place. The problem with phishing is that a holistic solution that works to protect users securely from being phished does not exist. As the defenses against phishing have evolved, so have the current phishing methods. As a result, the need for more advanced methods of security to identify phishing scams is important.

What is Phishing?	Phishing is defined as a type of malware or a term for where someone sends out a spoofed email to random victims to try to get personal information about them and is using social engineering techniques to fraudulently acquire sensitive information.
What is the problem with phishing?	The problem with phishing is that attackers constantly look for new and creative ways to fool users into believing their actions involve a legitimate website or email, even including logos and graphics in the phishing emails to make them more convincing.
Why are the victims of phishing vulnerable?	One study on phishing shows that victims are 4.5 times more likely to fall if it is from a personal contact or personally relates to them. Phishers have also started to develop a psychology behind that plays off urgency, greed or trust. Combined with the legitimate look and feel, even more cautious and aware users can fall victim to their attacks.
What are lasting effects of phishing?	Beyond monetary damages, businesses that are breached lose public trust and must work to secure their databases. Many companies are required to notify their customers of a breach, pay regulatory fines, and lose customers as a result.
Which are the industries/sector being targeted?	Published by Statista Research Department, During the first quarter of 2022, 23.6 percent of phishing attacks worldwide were directed toward financial institutions. On top of that, web-based software services and webmail accounted for 20.5 percent of attacks making these two the highest targeted industries.
What are the evolving trends in phishing?	Now phishing attack involves the theft of session cookies to steal private data and even bypass authentication layers. Cookies are small text files of data that can be sent to your server every time you click on a new webpage, which therefore gives certain parties the ability to monitor your activity and bypass the victim's multi-factor authentication (MFA) layer. These are security features used to verify an account login such as your Smartphone or email.