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 one of the most organized crimes of the 21st century. It 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. More specifically in computing, phishing is a criminal activity using social engineering techniques to fraudulently acquire sensitive information such as usernames and passwords by attempting to trick users of popular websites by emailing them fake versions of the website to provide their credentials to.
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. Phishers have become more skilled at forging websites to appear identical to the expected location, even including logos and graphics in the phishing emails to make them more convincing.
Why are the victims of phishing vulnerable?	There are dangerous new advanced phishing methods that utilize personal information that is easily available to the public in order to produce plausible and believable attacks that directly target victims. Methods such as social phishing and context aware phishing are perfect examples of attacks utilizing the massive amount of public information to increase the effectiveness of their scams. One study shows that victims are 4.5 times more likely to fall for a phishing attempt if it is from a personal contact or personally relates to them. Phishers have also started to develop a psychology behind their emails that plays off urgency, greed or trust. Combined with the legitimate look and feel of the spoofed websites, 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, Jul 7, 2022 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 when it came to phishing during the examined quarter.
What are the evolving trends in phishing?	An Adversary-in-the-Middle (AiTM) phishing attack involves the theft of session cookies to steal private data and even bypass authentication layers. Today, most sites that you click on will ask your permission to use cookies to tailor your online experience more closely. In short, cookies track your online activity to understand your habits. They 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. There are many kinds of cookies out there. Some are necessary, and some simply are not. AiTM attacks are concerned with session cookies. These are cookies that temporarily store user data during a web session. These cookies are immediately lost once you shut down your browser. AiTM attacks have been a particularly pressing issue for Microsoft 365 users, with attackers contacting targets and asking them to log into their 365 accounts. The malicious actor will impersonate an official Microsoft address in this swindle, which is also typical in phishing attacks. The goal here is not just to steal login information, but to bypass the victim's multi-factor authentication (MFA) or two-factor authentication (2FA) layer. These are security features used to verify an account login by requesting permission from a separate device or account, such as your smartphone or email.