INCREASING SOPHISTICATION OF PHISHING ATTACKS

NCA-06122301

Overview

Phishing attacks involve manipulating individuals into opening an infected email attachment, clicking on a malicious link, or giving up sensitive information, such as usernames and passwords or bank information. These attacks may manifest as phishing emails, phone calls, or text messages, aiming to exploit individuals through manipulation. User account credentials are valuable targets for cybercriminals because they can be used to access personal and organizational networks. Email-based phishing attacks have become the most common way for attackers to obtain user credentials.

Lately these bad actors have taken things up a notch by leverage AI to improve the sophistication of their attack approaches. This involves using AI to conduct thorough research on potential victims, and creating personalized messages to effectively deceive them into divulging sensitive information. This advanced approach shows how phishing attacks are getting more sophisticated and finding new ways to catch people off guard.

Preventive Measures

1. Be careful about the emails you open and the links you click on.
2. Don't enter your personal information on any website that you don't trust.
3. Use strong passwords and keep them safe.
4. Organisations and individuals should engage in continuous education and remain abreast of potential phishing threats.
5. Report suspected incidents to relevant contacts.