Abstract

Phishing is a type of attack in which cyber criminals tricks the victims to steal their personal and financial data. It has become an organized criminal activity. Spoofed emails claiming to be from legitimate source are crafted in a way to lead victims to reveal their personal, financial data by misdirecting them to the counterfeit website. This research paper presents a novel approach to combat the Phishing attacks. An approach is proposed where user will retrieve the one time password by SMS or by alternate email address. After receiving the one time password the web server will create an encrypted token for the user's computer/device for authentication. The encrypted token will be used for identification, any time user wishes to access the website he/she must request the new password. The one time password as name implies will expire after single use. The one time password and encrypted token is a smart way to tackle this problem.

References

Index Terms

Computer Science  Security

Keywords
Phishing attacks and prevention  Anti phishing  SMS  One Time Password  OTP  Authentication
X509Certificate2

Encryption

Client Identity and APPT