b'

Google\xe2\x80\x99s method for preventing Phishing attacks

- Difficulty Level :\nEasy
- Last Updated :\n13 Aug, 2018

Technology giant Google has recently revealed the method it uses to prevent phishing attacks on its employees. Google has told that its employees have been using physical U.S.B security keys instead of the traditional passwords method for authentication.

What is phishing.?
Phishing is a type of attack where the intruders disguising as trustworthy agents attempt to gain your personal information such as passwords, credit card numbers or any other information.
For example: You may receive a mail from some attackers who disguise as bank officials asking you to reset your password for your net banking account as there has been a data breach, as you go to the site and login, the attackers get your login id and passwords, thus they can now access your account.

Physical Security Keys: Physical security keys are replacements for passwords. Whenever you have to login to some account or get access you insert the usb (which acts as the key) into your system and press a button on it, that\xe2\x80\x99s it, no need to remember crazy and long passwords, no OTP worries. These physical keys resemble the vehicle keys that we use.

Google revealed that the use of physical keys has made its employees safer to phishing attacks. It was revealed that there had been no phishing attacks for almost 2 years now. Physical security keys look like a promising alternative to the age-old methods of passwords. With recent attacks revealing that even your fingerprints can be cloned, these physical keys could be the future of authentication systems.

My Personal Notes\n*arrow_drop_up*

Add your personal notes her

Save

'