10.11. 网络钓(10.11. Phishing Attacks)

10.11. 网络钓

10.11. Phishing Attacks

   Wide deployment of this and similar protocols may cause end-users to   become inured to the practice of being redirected to websites where   they are asked to enter their passwords. If end-users are not
   careful to verify the authenticity of these websites before entering   their credentials, it will be possible for attackers to exploit this
   practice to steal resource owners' passwords.
   Service providers should attempt to educate end-users about the risks   phishing attacks pose and should provide mechanisms that make it easy   for end-users to confirm the authenticity of their sites. Client
   developers should consider the security implications of how they   interact with the user-agent (e.g., external, embedded), and the   ability of the end-user to verify the authenticity of the
   authorization server.

To reduce the risk of phishing attacks, the authorization servers MUST require the use of TLS on every endpoint used for end-user interaction.

Revision #1
Created Wed, Mar 25, 2020 11:25 PM by □□
Updated Wed, Mar 25, 2020 11:25 PM by □□