Verify the Authenticity of the Remote GT User

Begin verifying the GT User’s identity:

1. First, check recent CAS authentication logs in IAT for person requesting remote help.
   a. Check to see if the user is successfully using CAS.
      i. If logs show recent logins but a person calls in then they are more likely a hacker.
      1. Be very careful vetting accounts which have been recently accessed successfully.
      1. Be very careful vetting accounts which have been recently accessed successfully.
      ii. What is the last date of successful CAS Login?
          1. More recent means more likely to be a hacker.
      iii. Recent successful CAS logins - apps & times
          1. Are there big gaps here? Big gap ==> more likely to be the real GT User.
      iv. Number of successful CAS logins since the last password change
          1. If frequent successful CAS logins ==> more likely to be the real GT User.
   b. When was the password changed last?
      i. Recent password changes may indication the GT User is real and really needs help.
   c. If the Person comes up as suspicious – DO NOT VET or Support.
      i. The TSC process is to refer the ticket to senior TSC management
      ii. The process CSRs should use is to refer the ticket/request to CyberSecurity
2. If the GT User’s identity looks legitimate, please proceed with support via the Passport Vetting Admin.
   a. See Passport Vetting Admin Tool Quick Reference Guide