Faculty, staff and students are encouraged to use **two-factor authentication (2FA)** to protect their UNCG accounts and data. 2FA adds an extra layer of security when you log in by requiring an additional step using a physical device (“something you have”) after you log in using your UNCG username and password (“something you know”). The hardware tokens sold at the SpartanCard Center are one type of physical device, or “second factor,” that you may use with UNCG 2FA.

**Should I get one?**

- Using a hardware token as your second factor is *not required*. It is recommended that you use your **smartphone or mobile device** as your second factor.

- Hardware tokens cost money and come with added responsibility. They are most effectively used when you lack permanent access to a smartphone or mobile device, or as an *optional* backup device.

See “Compare Second Factor Options” at [go.uncg.edu/getsecure](http://go.uncg.edu/getsecure) for more information about the second factor device or devices that will work best for you.

**The Basics of Using Hardware Tokens**

- **How to authenticate using your hardware token**

  When you log in to your account or service with your UNCG username and password, a second login/authorization screen will appear. Click **Enter a Passcode**.

  On your hardware token, press the button to generate a new passcode, type it into the space provided on the login screen, and click **Log In**.

- **Guidelines**

  - Carry your token with you. A keychain is a good option. Do not leave your token unattended or accessible to others. Your token is unique to you, and its protections depend on your ability to maintain custody.

  - Lost or misplaced tokens must be reported to 6-TECH within 24 hours for deactivation. Reactivation is possible if the token is later found.

For more information about the UNCG 2FA hardware token program and instructions and guidelines for using the hardware tokens, please visit [go.uncg.edu/getsecure](http://go.uncg.edu/getsecure)