Changing Your Password (and Avoiding Associated Pitfalls)

GT Account

You can change your GT account password online at: https://passport.gatech.edu (login required) or by calling the OIT Technology Support Center (TSC) at 404.894.7173. You can also do it in person at the TSC (Clough Building, Room 215). By default, your GT password expires every 120 days. If you are Duo enrolled (more information), your GT password expires every 365 days. Password requirements are as follows:

- Must be between 11 and 23 characters in length
- Must contain at least 3 character classes
  - Upper case alphabetic: A-Z
  - Lower case alphabetic: a-z
  - Numbers: 0-9
  - Special: !@#$%^&, and others
- Cannot contain your name or your GT account name
- Cannot be the same as any of the last 3 passwords used

More requirement information can be found here: https://passport.gatech.edu/password

College of Computing (CoC) Account

You can change your CoC account password online at: https://support.cc.gatech.edu/resources/forms/coc-account-password-reset (VPN or on-campus connection required) or by calling the TSO Help Desk at 404.894.7065. You can also do it in person at any of the TSO Help Desk locations listed here: https://support.cc.gatech.edu/services/helpdesk Your CoC password expires every 2 years. CoC password requirements are listed below.

- Must be at least 11 characters in length
- Must contain at least 3 character classes (as defined above)
- Cannot contain your name or CoC account name
- Cannot be the same as any of the last 3 passwords used

It is advisable to change your CoC password whenever you change your GT password to avoid confusion, but it is not mandatory. It is also good practice to log out and back into your CoC desktop computer after changing your password to avoid any issues with authenticated services.

Common Pitfalls and Additional Steps

When changing any passwords, it is necessary to update those same passwords on any mobile devices

which access email or other information related to the associated account. This step, if left undone, can cause account lockouts (or other issues) when the mobile device attempts to connect using the previous password. Other related causes of account lockouts are cached credentials for network drives (network home directory or adminfs folders), cached WiFi credentials, or Mac OS password caching (Keychain). Most mobile devices and Windows 10 devices should prompt for a new password when reconnecting to a resource after a password change. A how-to for clearing Mac OS Keychain passwords can be found at the following link.

https://support.cc.gatech.edu/support-tools/howto/removing-stored-passwords-os-x

If you have trouble updating your password on any of your devices, please contact the TSO Help Desk (helpdesk@cc.gatech.edu or 404-894-7065).

Password Managers

With the increasing complexity of password requirements, it can be difficult keeping up. It is highly recommended to use a password manager to control the password clutter. There are many different clients available and interested parties can find more information in the following reviews:

http://www.cnet.com/news/best-password-managers/
http://www.pcmag.com/article2/0,2817,2407168,00.asp

In addition, GT has a site license for LastPass, a popular and very capable password manager. More information about LastPass can be found here: https://faq.oit.gatech.edu/content/lastpass-faq