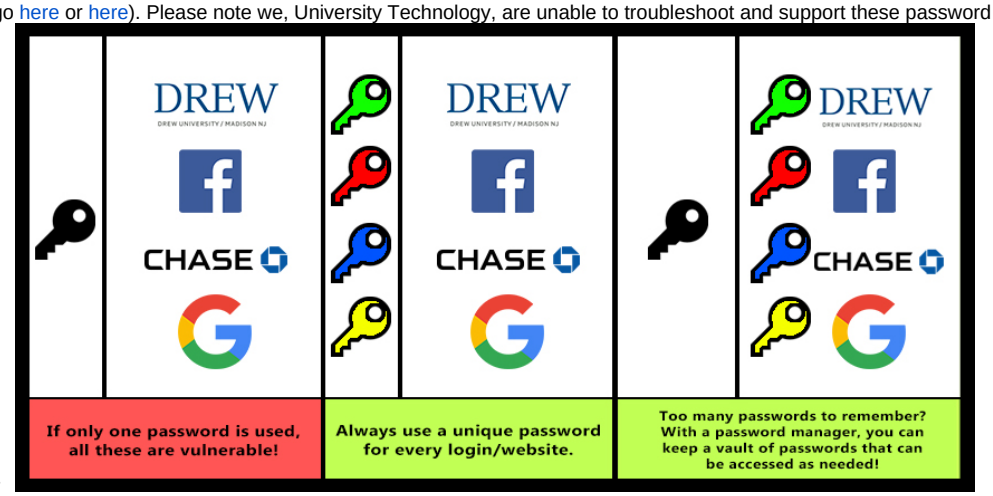
Passwords - Best Practices

Passwords are the key to almost everything you do online. They grant us access to our finances and confidential records, protect us from others impersonating us online, etc. It is vital to choose passwords that are difficult to hack/guess.

Important Tips To Make Your Virtual Life More Secure

- **Never reveal your passwords to others**. You probably wouldn't give your ATM card and PIN to a stranger and then walk away. So, why would you give away your username and password? Your login credentials protect information as valuable as the money in your bank account. Nobody needs to know them but you—*not even the tech department*. If someone is asking for your password, it's a scam.
- **Use different passwords for different accounts**. That way, if one account is compromised, at least the others won't be at risk. "How can I remember all these passwords" you might ask? Consider a password manager like KeePass, Lastpass, RememBear, or 1password. (To learn more, go here or here). Please note we, University Technology, are unable to troubleshoot and support these password managers.
  - 

- **Use two factor authentication**. Here at Drew, faculty, staff, and student staff with access to confidential information are required to use the two factor authentication software Duo, which we support.
- **Length makes for a more secure password over complexity**. The longer a password is, the better. Use at least 16 characters whenever possible.
- **Make passwords that are hard to guess but easy to remember.**
  - To make passwords easier to remember, use sentences or phrases. For example, "applepieandicecream". Some systems will even let you use spaces: "apple pie and ice cream".
  - Avoid single words, or a word preceded or followed by a single number (e.g. Password1). Hackers will use dictionaries of words and commonly used passwords to guess your password.
  - Don't use information in your password that others might know about you or that's in your social media (e.g. birthdays, children's or pet's names, car model, etc.). If your friends can find it, so will hackers.
- **Complexity still counts.** To increase complexity, include upper and lower case letters, numbers, and special characters. A password should use at least 3 of these choices. To make the previous example more secure: "@pple Pie & 1ce Cream!"

Reviewed June 14, 2023