Week 2: Creating complex passwords and keeping them secure

Passwords are the key to almost everything we do online. We have multiple passwords that we use nearly every day. Choosing hard-to-hack passwords and managing them securely can sometimes seem daunting. Fortunately, there are simple ways to make your passwords as secure as possible. Doing so can keep hackers from taking over your accounts, and prevent theft of our information and money.

These tips will help make your digital life more secure.

Never reveal your passwords to others. Your login credentials protect information as valuable as the money in our bank account. Nobody needs to know them but you. If someone is asking for your password whether it is online, via a phone call, text or in an email, it is a scam.

Use different passwords for different accounts. That way, if one account is compromised your other accounts will be at less risk.

Double Your Login Protection: Enable multi-factor authentication (MFA) whenever possible to ensure that the only person who has access to your account is you. Use it for banking, social media, Apple iCloud and any other service that requires logging in. Learn more about MFA and how to turn it on for many popular websites or check the 2FA directory to see if a web site offers it as an option.

Length trumps complexity. The longer a password is the better. Use at least 15 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, “applesandcaramelyum”. You can even use spaces: “apples and pumpkin yum”.
- 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, relatives names, 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: “Apples & caramel YUM!”

In order to make changing your password a smooth process, we provide some recommendations and instruction.

1. Make sure you have 15 to 20 minutes free. Most of the time changing a password will only take a few minutes. However because it's possible to make a mistake or mistype a new password (thus locking you out of your account) it's best to do this when you have some free time and when the CP IT Help Desk is open. Our hours are Monday-Friday, 8am-5pm

2. Collect all your devices in one place (cell phone, laptop, tablet (i.e. iPad) - anything you check email with)

If you utilize your credentials to login to a computer right from the desktop on campus or via VPN (when working from home):
1. Press Ctrl + Alt + Del keys together on your keyboard to get the security screen.
2. Click "Change a password".
3. Specify the new password for your user account:

If you are off campus logging into Outlook online (web mail) with your username and password:
Please reach out to help desk at 1-800-373-7521 or helpdesk@ssndcp.org to let us know some good days and times we can assist with resetting your password to one you prefer. Under no circumstance should you share your desired password via email. We would like to assist you in making the change over the phone.

3. Once your password has been changed, go to each of your mobile devices and update the password field with your new password.

Keeping password secures

Use a password manager. Password management tools, or password vaults, are a great way to organize your passwords. They store your passwords securely, and many provide a way to back-up your passwords and synchronize them across multiple systems. One such example of a password manager is LastPass, utilized in various departments and by individual committee members, etc. It allows you to create a master password and then store all your other passwords within your account so you need to remember the one master password and eliminating the need for notebooks, post-it notes and spreadsheets.

If you have questions or need any assistance please reach out to us at 800-373-7521 or helpdesk@ssndcp.org