TAKING CONTROL OF YOUR ONLINE INFORMATION

- Google yourself to see what records each data broker has collected on you.
    - Conduct Google searches using your name, email address, phone number, home address, social media names, family information, etc.
        - Record your findings, as you will most likely need the URL/information from each page to identify which records you want removed.
    - To narrow down Google search results, use Google search operators.
        - site:
            - Limit search results to a specific website
                - **Example: "**123 Main St" site:whitepages.com
                    - Google will search for the address "123 Main St" only on the website whitepages.com.
        - -
            - Excludes words from your search
                - **Example:** jaguar -car -automobile -dealer
                    - Google will search for the word jaguar but exclude results that include the words car, automobile, and dealer.
        - " "
            - Use double quotations to search for an exact match
                - **Example:** "John Smith"
                    - Searching for "John Smith" would show results for exactly "John Smith", whereas searching for John Smith without double quotations would show results for John and/or Smith.
    - A custom date range can be set for searches on Google. Click on 'Tools' under the search box to locate this function.
    - The website https://www.google.com/advanced_search can also be used to conduct the above Google searches in a more user-friendly way.

- Remove your information from data collection sites.
    - Visit each site and follow procedures for opting out/removing your data.
        - Each site has a different process for removing data. Some may require sending in paperwork via mail, email, or fax.
        - Some data brokers may have information about you under multiple listings. If so, you may need to complete the removal process for each separate listing.
    - Data brokers – below are some of the most popular data brokers and the URLs to each of their opt-out pages:
        - Spokeo
            - https://www.spokeo.com/optout
        - Whitepages
            - https://www.whitepages.com/suppression_requests

- PeopleFinder
  - https://www.peoplefinder.com/optout.php
- Pipl
  - https://pipl.com/personal-information-removal-request
- FamilyTreeNow
  - https://www.familytreenow.com/optout
- PeekYou
  - https://www.peekyou.com/about/contact/optout/index.php
- InstantCheckmate
  - https://www.instantcheckmate.com/opt-out/
- Intelius
  - https://www.intelius.com/optout
- BeenVerified
  - https://www.beenverified.com/app/optout/search
- TruthFinder
  - https://www.truthfinder.com/opt-out/
- TruePeopleSearch
  - https://www.truepeoplesearch.com/removal
- FastPeopleSearch
  - https://www.fastpeoplesearch.com/removal

- https://wiki.onerep.com/
  - OneRep is a company that offers a paid service for removing your records. However, they also post instructions on how to manually remove records from many of the most popular data brokers (some of which are not included in this document).
- A paid data removal service can be used to remove this same data for you.
  - DeleteMe seems to be a popular paid service.
    - www.joindeleteme.com

- Delete social media accounts, or if you want to keep your social media accounts, then ensure proper privacy settings are turned on and being used.
  - Facebook
    - https://www.consumerreports.org/privacy/facebook-privacy-settings/
  - LinkedIn
    - https://www.consumerreports.org/privacy/linkedin-privacy-settings/
  - Twitter
    - https://www.kaspersky.com/blog/twitter-privacy-security/32447/
  - Instagram
    - https://www.consumerreports.org/privacy/instagram-privacy-settings/
  - Google
    - https://www.consumerreports.org/privacy/how-to-use-google-privacy-settings/

- Delete online accounts that you no longer need/use.
  - The websites below have published instructions on how to delete online accounts from many different company websites:
    - https://www.accountkiller.com/en/home
    - https://backgroundchecks.org/justdeleteme/

- Secure your online accounts with strong, unique passwords and multi/two factor authentication.
  - This will prevent account compromises and subsequently prevent sensitive personal information from being stolen.
  - Password security
    - Each online account should utilize a strong, unique password.
      - Do not re-use passwords! Every account should have a different password.
    - A strong password avoids common words/phrases, is at least 15 characters long (the longer the better), and contains a random mix of uppercase, lowercase, numbers, and special characters.
    - Alternatively, a passphrase, which is a sentence-like string of random words, can also be used. Passphrases are generally easier to remember than passwords.
    - Consider using a password manager to help manage your online account credentials.
    - The website https://www.haveibeenpwned.com/ can be used to see if your credentials have been exposed in known data breaches.
  - Multi/Two-factor authentication (MFA/2FA)
    - Many accounts allow you to turn on MFA/2FA, which will require you to also provide a one-time pin (OTP) code in addition to your password when signing into an account. This code is usually obtained via text message, email, or an authenticator application.
    - Even if a malicious actor were to learn your password, they would still need this OTP code to access your account.
    - The website https://twofactorauth.org/ is a good resource to check which online service providers offer MFA/2FA.

- Be aware of phishing attacks, which involve electronic communications sent by malicious actors who are attempting to steal sensitive information.
  - Do not click on any URLs or open any documents received in emails/texts that you were not expecting.
  - Email addresses can be spoofed. You could receive an email from somebody which appears to come from their actual email address when in fact it has come from a malicious actor using another email address. When replying to emails, double check the email address of the recipient to ensure you are replying to the legitimate email address of the intended recipient.
  - If you question an email, consider calling the sender via a known number to confirm they sent it.
  - Many organizations/websites have an 'Abuse' contact page/email address that phishing emails and other malicious content can be reported to.

- If somebody posts your personal information on a website/social media website, there are a few different options you can take to attempt to have this data removed.
    - Many social media sites have a 'report' function which lets you report specific users/posts.
    - Most websites have a 'contact us' form or contact information listed on the website that can be used to contact the webmaster to request they remove the information.
    - If there isn't any contact information listed on the site, you can use a website like https://centralops.net/co/ to locate additional contact information for people/companies associated with the website.