Handout 13

WAYS TO PROTECT YOUR DIGITAL FOOTPRINT

Easy Suggestions

- Keep your personal details private; think carefully before giving out your name, address or phone number online
- Never share your username, password, PIN numbers, bank account information, PPS number or credit card information with anyone
- Consider using non-identifiable usernames
- Treat your password like your toothbrush: don't share it with anyone, and change it often. Use strong passwords and vary them on different sites. Change them frequently
- Think before you post. Once posted, information can be difficult or impossible to remove
- Never post things that you don't want others to know about or that you wouldn't say to someone's face
- Be respectful of other people's content that you post or share (e.g. a photo that a friend took is their property, not yours - you should post it online only if you have their permission.)
- Conduct transactions only on a secure Wi-Fi connection that requires a password
- Use security or virus protection software
- Back up your data
- Always remember to log off when you have finished with an online service. Otherwise people could use your account and your personal information without your permission
- Remember that not everything you see, read or hear about online is true. People and websites may pretend to be something they're not.

Advanced Suggestions

- Change privacy settings; go to the websites you use most often (especially social networks) and check your privacy settings. If you've included personal information on your profiles, consider removing or reducing
- Block cookies on your web browser. When you surf the web, hundreds of data points are collected by the sites you visit to form a digital profile. This profile is then sold to companies around the world without your consent. By blocking cookies on your web browser, you can prevent some of this data collection
- Don't download apps from foreign countries. Some apps that access personal information either won't secure this data or, worse yet, sell it to other companies
- Remove any old accounts. Do a Google image search for old sites that may have your photo. Delete your accounts if you can. If not, update the accounts with a false name, email address and blank image
- Unsubscribe from mailing lists you no longer use, and frequently monitor the ones you do. Check to see if you've been involuntarily subscribed to a new mailing list and quickly unsubscribe. Check the privacy use policies of the mailing lists you've subscribed to so you can see if the owner can share your email and other information without your permission
- Don't share your personal information. Keep personal information private. This includes usernames, aliases, passwords, last names, addresses, photos and other important information
- Be mindful when you tag someone on social media sites like Facebook. Tagging gives you a lot of followers, but it also sends out information about you to others who might send it to others you don't know
- Be careful of what you say, text or post on your social media accounts. Comments, images and links can be stored virtually for ever and can be accessed by many people
- Be extra careful with geolocation services and requests to map your location. Some sites don't explain why they want this information. If they're not telling you why, you don't need to let them know where you are
- Use a secondary email address for opening up new accounts. This can help you monitor how some sites use your information. If you begin to receive unsolicited emails on that account, you know your information has been sold or passed along.