UNIVERSITY of WASHINGTON

CYBER SAFETY 101

The following tips are provided to help manage and safeguard your digital information and online presence.

PRIVACY

- Develop a strategy for how to interact online, including tactics for dealing with conflicts.
- Think long-term: Once you share information online, it can be difficult or even impossible to remove your digital fingerprint.
- Make informed decisions about the privacy of your identity, location, affiliations and actions.
- Before you act, think about the intended and unintended uses of information.
- Review what information is available about you online.
- Be aware of the open and private aspects of online groups, forums and comment sections.

SECURITY

- Secure confidential and personal information on devices.
- Use encryption.
- Review good password practices; don't reuse passwords for different accounts.
- Remember: Data sent over public wireless networks, as well as information on public computers and kiosks, may be accessed by others.

PREPARE

- Review and consider modifying privacy preferences on devices, browsers and apps.
- Verify that privacy settings align with your privacy strategy.
- Control who can view your profile, contact information and posts.
- Limit location services to the apps and friends you want to track you.

REPORT

- **Cyberstalking is a crime.**
- If you see anything that is an imminent threat to your physical safety or that of others, call 911.
- Report incidents of cyberstalking or cyber harassment to the UWPD at 206-685-UWPD.
- For security concerns about UW systems, accounts and information, email **help@uw.edu.**

If you are experiencing online behavior that raises safety concerns, SafeCampus can help provide support and connect you to resources: 206-685-SAFE (7233) or safecampus@uw.edu.

This page will be updated as additional resources become available.