UNIVERSITY *of* WASHINGTON

Online Safety Strategy

https://ciso.uw.edu/education/risk-advisories/online-safety-strategy/

This election season, there is potential for an increase in online harassment ranging from inappropriate comments to invasive doxing, cyberstalking, threats of violence and hate speech. Individuals at UW could be targeted for personal or institutional beliefs, or areas of research. The following tips and the resources listed at the URL above may help. SafeCampus consultation and resources are available at **206-685-7233** or **https://www.washington.edu/safecampus/**

PRIVACY

1. Learn about digital wellness and identity theft at **https://privacy.uw.edu/yourprivacy/**
2. Make informed decisions about the privacy of your identity, location, affiliations, and actions.
3. Before you act, think about the intended and unintended uses of information.
4. Review what information is available about you online.
5. Be aware of the open and private aspects of online groups, forums, and comment sections.

SECURITY

1. Secure confidential and personal information on devices using pins, strong passwords and multi-factor authentication.
2. Encrypt data, devices, and connections whenever appropriate.
3. Review good password practices, and don't reuse passwords for different accounts.
4. Remember data sent over public wireless networks is accessible to others.
5. Keep in mind that information on public computers and kiosks may be accessed by others.

PREPARE

1. Review and consider modifying privacy preferences on devices, browsers and apps.
2. Verify these privacy settings align with your intentions to share.
3. Control who can view your profile, contact information, and posts.
4. Limit location services to the apps and friends that you don't mind tracking you.

RECOVER

UW systems, accounts, and information:

1 Find out about how to report incidents involving UW data and information on the Report an Incident page on the UW Privacy Office website. **https://privacy.uw.edu/report/**

Your own systems, accounts, and information:

2. Review the list of external resources linked from the url address above.

3. You may wish to seek private legal counsel on how best to protect yourself.

The above are basic considerations to help you manage your information online. It is not an exhaustive list of steps you can take to prevent identity theft, cyber bullying, or other malicious activities. Go to the url listed in header of this page for more resources.