OFFICE OF THE CISO
UNIVERSITY of WASHINGTON

Information Security Risk Advisory
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. There is also potential for these behaviors to continue after election day into the new year and beyond. UW staff, faculty and students may be targeted because of their personal or institutional beliefs or their area of research.

This harassment can be upsetting and traumatic, but you do not have to deal with it alone. SafeCampus consultation and resources are available to you or anyone you know that has been targeted. They can be contacted 24 hours a day, 7 days a week at 206-685-7233 or online.

Things to Do

The following tips and resources may help you develop a strategy to secure your personal data and the University's institutional information.

Online attackers may work alone or organize to target you directly. They may search social media pages and online public databases for personal details about you. They may use information, such as your location, to threaten you or family members, or manipulate photos of you. They may contact your employer or co-workers to discredit or shame you.

Privacy

- Learn about digital wellness and identity theft at on the UW Privacy Office website at: https://privacy.uw.edu/yourprivacy/
- Identify what data is available about you online and on which websites this information resides.
- Take steps to remove any information that you are uncomfortable having on the Internet.
- Understand how to spot, prevent, report, and recover from, identity theft: https://privacy.uw.edu/yourprivacy/learn-about-identity-theft/

Security

- Turn on two-factor authentication (2FA) for all your accounts, including email, social media accounts, and any accounts that may hold your financial data.
- Change your passwords if you suspect you are being targeted for online harassment. Use a password manager, such as LastPass, to create and store long, unique passwords for all your online accounts. Note that it is not recommended to use the same password on multiple accounts.
- Monitor your bank and other financial accounts and set up alerts to be informed of any unusual activity and check social media accounts for suspicious logins.

- Consider making social media accounts private during an attack to secure your personal information.
- See the UW Office of the CISO website for online training and best practices to secure your personal information and UW data.

SafeCampus

SafeCampus is the University of Washington's violence-prevention and response program supporting students, staff, faculty and community members in preventing violence. They offer violence prevention and response training and can help you with a threat assessment to determine how best to respond to a situation. Visit the SafeCampus website for more information.

Resources

UW Privacy Office

UW SafeCampus

UW Social Media Guidelines

Coalition Against Stalkerware

New Beginings Technology Safety

Online Harassment Field Manual

Online Safety Speak Up and Stay Safer Guide

Digital First Aid Kit

Digital Safety: Protecting against targeted online attacks

National Cyber Security Alliance, "Stay Safe Online"

Crash Override Network "Preventing Doxing"

The Cyberbullying Research Center