DIGITAL SECURITY BASICS

Your digital security and privacy have never been more important. Faculty across the nation and on your campus are facing politically-motivated smear campaigns, harassment, threats, and doxing. Protect yourself with these tips from Faculty First Responders and the AAUP.

Digital Security Recommended Practices

- Use strong, complex, unique passwords and passcodes for your accounts and devices.
- Employ a password manager like 1Password or BitWarden to manage your passwords for you.
- Do not use your web browser to save passwords.
- Enable two-factor authentication whenever possible.
- Use fake answers for security questions, and keep a log of these answers.
- Install software updates immediately.
- Restart your devices regularly.
- Back up your data frequently to both the cloud and a physical external hard drive.
- Use encrypted messaging and calling services for sensitive activities. The best is Signal.
- A personal Zoom account (not your work account) is a secure site for online meetings.

Contact Us for Personalized Advice

Faculty First Responders, an AAUP partner, is available any time for peer-to-peer counseling related to harassment of academic workers, digital security, and doxing. FFR offers free webinars and workshops about academic freedom to groups of any size.

Contact Heather Steffen, FFR Assistant Director, for more information:
facultyfirstresponders@gmail.com

Digital Privacy Recommended Practices

- Search your name on common search engines and document what info is available about you online.
- Opt out from data broker sites that display your personal info (address, phone number, etc.).
- If you have the resources, use an online identity protection service like Incogni or DeleteMe.
- Set social media accounts to their maximum privacy settings.
- State in your social media bios that the views expressed there are your own and do not represent your employer (no need to name the employer).

Using Campus Devices and Services

- Maintain at least two email accounts: your institutional (work) email and a personal email account.
- Never use campus email, devices, or wi-fi for organizing or other sensitive activities. Even if you feel you have “nothing to hide” from your employer, legal discovery, or a public records request, it is also your responsibility to protect your contacts’ privacy and security.
- Instead, invest in a paid VPN (virtual private network) or use the Tor browser.
- Bottom line, use employer-provided resources only for work activities.

Get the Resources

- Access links and resources by scanning this code with your phone’s camera.