



Top 5 Tips to Secure Data

ois.uw.edu



Choose strong passwords, keep them secure, and use 2FA

Review best practices for managing passwords and don't reuse passwords for different accounts. Consider using a password manager.

Use multi-factor authentication (MFA) for an extra layer of security. Find info about Duo, a two-factor authentication (2FA) service, on IT Connect.

More tips at <https://ois.uw.edu/site/files/passwords.pdf>



Don't fall for phishing

Think before you click. Don't automatically click on links in emails.

Don't open unexpected attachments.

See more phishing resources at <https://ois.uw.edu/education/#phishing>

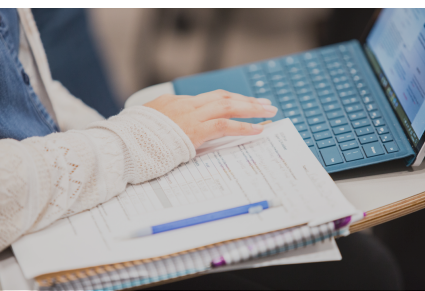


Update, patch and use antivirus software

Keep all devices and software updated to the latest version.

Stay up to date with patches.

Use antivirus software. A free version of Sophos antivirus is available here: <https://itconnect.uw.edu/wares/uware/sophos-anti-virus-software/>



Secure wireless communication with eduroam

Remember: data sent over public wireless networks is accessible to others.

eduroam is a free, secure Wi-Fi service available to the UW community.

More information: <https://itconnect.uw.edu/connect/uw-networks/campus-wi-fi/eduroam/>



Use Husky OnNet when working remotely

Husky OnNet provides a secure connection to UW systems from off campus.

It is a free virtual private network service (VPN) for students, staff and faculty.

More information: <https://itconnect.uw.edu/connect/uw-networks/about-husky-onnet/>

