Passwords & Passphrases

ois.uw.edu/ncsam

Make them unique

Use different passwords for different accounts so that if one account is compromised, the others won't be at risk. University accounts have been compromised because of passwords that were re-used on other services & accounts.

Make them long and complex

The longer and more complex a password is, the harder it is for adversaries to compromise your account. Use at least 16 characters and a combination of letters, numbers, and symbols whenever possible.

Use a password manager

Password managers are a great way to organize your passwords. They provide a way to back up your passwords and synchronize them across multiple systems.

Change default passwords

Malicious hackers sometimes use tools that search networks for devices and applications that are still using the default username and passwords set by the vendor. Immediately change the default password on any account, device, or system you are responsible for, including wireless routers in your home.

Checklist

- ☐ Avoid using UW NetID passwords on other accounts.

- ☐ Use multi-factor or two-factor authentication for added protection.

- ☐ It's recommended to create passwords with at least 16 characters.

- ☐ Use a passphrase to make your password both long and memorable.

- ☐ Using a combination of letters, numbers, and keyboard characters will make your password more complex.

- ☐ Password managers can help you create long, random passwords for your accounts.

- ☐ If you think your UW Net ID password has been stolen, change it immediately and report it to help@uw.edu.

W OFFICE OF INFORMATION SECURITY
UNIVERSITY *of* WASHINGTON
Information Technology