BEST PRACTICES FOR

PASSWORD USAGE

AVOID CLICKING LINKS IN EMAILS

A common way that passwords are compromised is through **phishing**. Phishing emails are designed to trick users into surrendering their University login credentials on phony web pages.

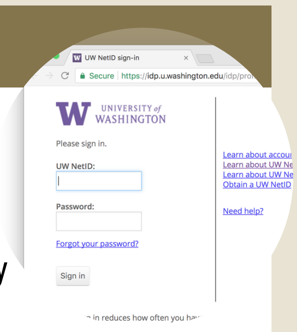
Don’t use email to send personal or financial information, and delete any emails that ask you to confirm or divulge your personal or financial information.

If you come across a phishing scam that specifically targets the University of Washington, please contact **help@uw.edu.**

DON'T RE-USE PASSWORDS ACROSS ACCOUNTS

Never reuse your UW NetID password on any other account.

If you use the same password for different purposes, a cyberthief can learn the passwords from a less secure site or application and then use it to exploit other accounts. Immediately change default passwords, including those on wireless routers in your home.



UW NetID sign-in ×

Secure | https://idp.u.washington.edu/idp/pro

UNIVERSITY of WASHINGTON

Please sign in.

UW NetID:

Password:

Forgot your password?

Sign in

in reduces how often you ha

Learn about accou
Learn about UW Ne
Learn about UW Ne
Obtain a UW NetID

Need help?

USE CAUTION ON WIRELESS NETWORKS & PUBLIC COMPUTERS

Avoid using such computers in public spaces, to log into your school, work, or financial accounts. Public computers and kiosks, such as those at a hotel, may be infected with **malware** that steals your passwords.

Wireless networks in public places are subject to **eavesdropping**, and cybercriminals can easily trap passwords and other information without the user's knowledge. If you do use public WiFi, use a virtual private network (VPN) service.

USE UNIQUE PASSWORDS & PASSPHRASES

Use a combination of numbers, lower-case and upper-case letters, and symbols.

Instead of a password, consider using a passphrase to make a long password that is meaningful only to you.

Use spaces or special characters to make passphrases random and long, yet memorable.

Each character added to a password makes it *exponentially* more difficult to crack.

Never use publicly available or personal information for your passwords.

USE SECURE SERVICES FOR SECURE CONNECTIONS

Password managers can be used to create, store, and access complex passwords as you need them.

Multi-factor authentication or MFA such as *Duo* adds an additional layer of protection in addition to your password.

eduroam, a wireless service, allows users to securely access the Internet from institutions throughout the world.

HuskyOnNet, UW's VPN service, provides an encrypted connection to the UW from remote locations.

MORE INFORMATION
https://ciso.uw.edu/education/online-training/#passwords

CONTACT
Email: ciso@uw.edu | Phone: 206-685-0116