Use passwords that can’t be easily guessed — and do not share them. Consider using a password manager.

Make backup copies of files or data you do not want to lose — and store them securely in UBox or OneDrive.

Do not store sensitive information.

Beware of scams — including social engineering, phishing, and impersonation.

Use only trusted, secure websites (https) and Wi-Fi networks like UConnect and ULink.

Do not install or download unknown or unsolicited programs or apps.

Protect your computer with antivirus software, security patches, and updates.

Be careful about what you share, install, and accept on social media. Do not click on suspicious links.

Shut down, lock, log off, or put your devices to sleep before leaving them unattended — and make sure they need a secure password to start up or wake up.

Secure your devices at all times — lock them up or carry them with you.

Lock your windows, doors, drawers, etc., before leaving an area unattended. Never share an access code, card, or key.

Email addresses, phone numbers, and other public information — including student majors and employee titles — are all available on University of Utah websites. This makes U students, faculty, and staff prime candidates for targeted attacks.

Good information security habits aren’t just for geeks — they can keep your personal information safe, protect your devices from viruses, and prevent theft.

Report lost or missing university/personal computing equipment to the University of Utah Department of Public Safety (UUDPS). If the items were stolen off-campus, contact the local authorities.

UUDPS can be reached at 911 (for emergencies) or 801-585-COPS (2677)

A lost or stolen device also can be reported through an online UUDPS form.

You also can report a security incident to iso@utah.edu or soc@utah.edu, or call your respective central IT help desk: Main campus, 801-581-4000, option 1; University of Utah Health, 801-587-6000.