The Fundamentals of Information Security

A guide to safely using technology at the University of Minnesota

Know your data and how to protect University data

If you handle sensitive or private data, including student, health, research, or human resources data, you are responsible for protecting that information.

It is important that you familiarize yourself with the types of data entrusted to you, identify your data's security level, and apply University information security standards to protect your data, yourself, and the University. Learn more at **z.umn.edu/dataclassification.** In the event of suspected unauthorized access to or disclosure of University data, contact **security@umn.edu.**

Back up your data regularly

Backups are essential! Your hard drive could fail, you could lose your device or it could be stolen, or you could get a malware infection.

Regularly back up your data using an external hard drive, USB drive, or approved University service provider such as Google Drive or Box Secure Storage. Be sure to store physical backups in a secure location separate from your device.

Enable security features on your devices

If your computer, phone, USB drive, or tablet is lost or stolen, someone else could access the private information on it.

Look for USB drives with encryption and turn on device encryption whenever possible. If traveling abroad, check with the State Department that the country you're visiting allows encrypted devices.

Use your device securely

If you have older or unpatched software, cyber criminals may be able to exploit vulnerabilities to control your system or steal your information. Cyber criminals also may monitor or intercept your online activities and steal private data while you are using your device.

To keep your device current, enable automatic updates and install updates right away when notified. When you enter sensitive information on a website, look for URLs that begin with "https://" and a padlock. Use the U's Virtual Private Network (VPN) when off campus or using a public network, and use secure WiFi, such as eduroam, whenever possible.

Choose strong passwords and keep them safe

An unauthorized person can use many tools to guess or steal a weak password. A compromised password could be used to access your personal information, email, academic work, or University private data, or used to send malicious emails impersonating you.

To prevent this, choose a strong password that includes at least 16 characters with at least two out of four different character types. Learn how to create a strong password or passphrase at **z.umn.edu/passphrase**.

Use two-factor authentication wherever it is available, such as Duo Security. If you suspect your University password has been compromised, change it immediately and contact **security@umn.edu**.

Recognize and report email scams

Email scams (also known as phishing) are a common method used to get you to visit a fraudulent website, open an infected document, or log in to "validate your account." This can lead to theft. Phishing messages may be obviously fraudulent, or may look like genuine University correspondence.

Never give your password to an unverified party online, over the phone, or in person. The University will never ask you to provide your username and password via email. Learn to identify the signs of a phishing message at **phishing.it.umn.edu**, and feel free to ask us at **phishing@umn.edu** if an email is real or a scam.

z.umn.edu/SecureU