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, and human resources data, you are responsible for protecting that data. Loss or unauthorized disclosure of private data harms individuals and the University, can cause reputational repercussions, or violate state and federal laws.

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. In the event of suspected unauthorized access to or disclosure of University data, contact **abuse@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 email account." This can lead to theft, including identity theft. Phishing messages may be obviously fraudulent, or may look like information provided by the University.

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 fraudulent email, and feel free to ask us at **phishing@umn.edu** if an email is fraudulent.

ENABLE SECURITY FEATURES ON YOUR DEVICE

If your device is lost or stolen, private information on it could be accessed by whoever has the device.

Look for USB drives with encryption, and turn on encryption whenever possible. If traveling abroad, check with the State Department to ensure 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 and/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 when notified. When you enter sensitive information on a website, look for URLs that begin with "https://" and a padlock. Also use the U's Virtual Private Network (VPN) or Eduroam when off campus or using a public network.

CHOOSE STRONG PASSWORDS AND KEEP THEM SAFE

An unauthorized person can use many tools to guess or steal a weak password, then use it to access your personal information, email, academic work, and University private data, or to send malicious email impersonating you.

To prevent this, choose a strong password that includes multiple types of characters. Use two-factor authentication where available. If you suspect your University password has been stolen, change your password and contact **abuse@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 service provider.