Verify applications before downloading

Some apps could be harmful to your mobile device, either by carrying malware or by directing you to a malicious website that may collect your information (such as credit card numbers). Make sure that you download apps from a well-known trusted source such as Google Play or the Apple App Store.

Mobile devices and University data

If you use your mobile device for University business, you must classify the data created, accessed, transmitted, or stored on the device to ensure the appropriate controls to protect University data are in place.

Learn how at **z.umn.edu/dataclassification**.

Any records related to University business (including text messages, voicemail messages, emails, and other electronic communications) are University records whether they are on a University-issued or a personal device. Business-related records that the University should retain must be kept on University (not personal) systems and devices, and you should delete business-related information as soon as it is no longer needed.

In addition, if you are part of the University Health Care Component and handle health information, you must register your mobile device with the Health Sciences Technology.

Learn how at **z.umn.edu/UHCmobile**.

Follow safe disposal practices

When you are ready to dispose of your device, be sure to remove all University or personal information first.

Learn how at **z.umn.edu/clearyourdevice.**

Promptly report a lost or stolen device

University-purchased devices can be remotely deactivated or wiped, preventing email or other data from being exposed if they are lost or stolen. Promptly notify University administrators if a device is stolen or misplaced that was used to access or store University data.

Report a lost or stolen device to **help@umn.edu** or **security@umn.edu.**

security@umn.edu

®

chat.it.umn.edu

☎ 612.301.4357 (1-HELP)

help@umn.edu

it.umn.edu/walk-in

®

secure U

Securing Mobile Devices

z.umn.edu/SecureU

Mobile Devices (such as iPads, Android tablets, smartphones, and more) must be appropriately secured to prevent University data from being lost or compromised, and to mitigate other risks to the University of Minnesota.

Mobile devices owned by the University of Minnesota or that contain private data belonging to the University of Minnesota need to have a remote lock and/or reset abilities enabled and available to University administrators, in order to best protect University information.

Follow these easy guidelines to help keep your mobile devices safe and secure

Password-protect your mobile device

Physical security is a major concern for mobile devices, which tend to be easily lost or misplaced. If your mobile device is lost or stolen, a device password may be all that stands in the way of someone acquiring sensitive data.

Choose a strong password! The security of your system is only as strong as the password you select to protect it. If possible, use a complex password or a drawn pattern instead of a simple 4-digit PIN.

Review University guidelines for selecting a secure passphrase or password at **z.umn.edu/passphrase.**

Encrypt your device

Your mobile device may be configured with saved passwords that would enable anyone to access your email, banking or credit card information, or University data.

Encryption is your device's ability to convert information into a code to prevent unauthorized access. Essentially, it scrambles up your data when your device is locked, making it only accessible to someone with the right access.

Encryption automatically comes with the iPhone/iPad 3 and later, and Android phones/tablets that run Android 4.4 KitKat and later OS versions.

Sensitive documents, if stored on the device, should be additionally encrypted if possible.

Permanently delete any University data stored on your device as soon as it is no longer needed.

Tip: Check your device settings to see if you can easily turn on encryption!

Use only secure WiFi networks

Your accounts and passwords should never travel unsecured over a WiFi network. Insecure WiFi network traffic can be easily recorded. Any sensitive data, especially login information, should always be viewed or entered via a secure WiFi connection.

Tip: Most modern mobile devices will warn if a network is insecure!

Keep your operating system up to date

To reduce security threats, you need to accept updates and patches to your mobile device's operating software. You can enable automatic updates by the device manufacturer (for example, Samsung), operating system provider (such as Android), service provider (like Verizon, AT&T or Sprint), and/or application provider (for instance, Google or Apple).

Examples of University information to protect

- Academic
- Research
- Financial
- Contact Information
- Correspondence (such as your University email)

Disable applications and services

Reduce security risk by limiting your device to only necessary applications and services. You won't need to manage security updates for applications you don't use and may even conserve device resources like battery life.

Tip: Bluetooth is an example of a service that can open your device to unwelcome access if improperly configured. You can easily turn it on and off in the settings.

Avoid jailbreaking

Tampering with your mobile device factory security settings makes it more susceptible to attacks, or makes it more likely that your device could attack other systems.

Definition: To **jailbreak** a phone is to hack it so that you have unrestricted access to the entire operating system and can make changes outside of default or factory device settings.