Transcript Mobile Devices

Instructions
This training is approximately 8 minutes long. You can speed it up or slow it down using the controls in the player.

For each best practice mentioned, additional resources are listed in the navigation bar labeled “Links” on this webpage. An accessible transcript can be accessed or downloaded from the “transcript” link.

Introduction
Did you ever wake up in the morning and realize that you didn’t know where your smartphone or laptop was?

What ran through your mind when your realized you wouldn’t, for some unknown amount of time, have access to your email, contacts, photos, music, and other personal data?

How did you feel as it dawned on you that your device and the information stored on it might be picked up–and possibly accessed or even stolen by a stranger?

The reality is that mobile devices, such as smartphones, tablets, iPads, and laptops play an important role in many people’s lives.

If you are one of those people, the following 12 tips will help you consider some of the risks of using mobile devices to access and store personal and UW institutional information, and what you can do to help protect that information.

1. Use passwords and pins.
Passwords on laptops, along with passcodes and pins on smartphones, are an important defense and a simple step in deterring unauthorized access if your device is lost or stolen.

2. Use eduroam and Husky OnNet for wireless security.
Wireless networks are subject to eavesdropping. Cybercriminals can use tools to view login credentials, spreadsheets, credit card information, and just about anything you do or store on your device.

Fortunately, there are two free services available for the UW community:
• Use eduroam, an encrypted WiFi service, when you are on the UW campus
• Use Husky OnNet, a virtual private network, to access University data from remote locations
You will find more information about both tools in the Links menu.

3. Keep your device operating systems (OS) and apps updated and patched.
New vulnerabilities are continually discovered on mobile device platforms, so keep the OS and applications updated and patched to the latest version to allow security updates. For iOS and Android, check for system updates in the “Settings” menu.

4. Encrypt your devices.
Passwords and pins make it difficult for someone to unlock your smartphone or computer, but

encryption goes a step further and makes the data unreadable. Follow the instructions provided by the manufacturer to encrypt the data on your device.

5. Install antivirus or other mobile security software on your devices.
It depends on whether you are using a laptop, iPhone, iPad, Android, or other type of device as to which type of data protection software you will want to use, but there are antivirus, anti-malware, and endpoint protection suites that are helpful for securing your devices from malicious attacks and unintended data disclosure.

Click “Sophos” in the Links menu to find information on UW’s IT Connect page about antivirus and other protective software. The section labeled “For your personal computer or device” will provide instructions for downloading free or low-cost Sophos antivirus, Home Premium, and/or endpoint protection, depending on your device and operating system.

6. Install apps from trusted sources.
Depending on the devices and applications you use, there are many ways that apps can affect your data. Some devices are prone to malware, such as ransomware that can lock up your files until you pay money to cyberthieves. Some devices may be vulnerable to rogue apps that are developed to look like trusted brands, but ultimately, they steal your data. Another problem is data leakage, which occurs when you inadvertently agree to give an app access to data that it doesn’t need and shouldn’t have.

Only install apps from trusted sources, check reviews and updates to make sure they are from trusted developers, only download apps that you absolutely need, and get rid of ones that you are not using.

7. Consider enabling software that allows you to find your device.
iPhones, iPads, Androids, and other devices have software that help you locate your device if it’s lost. Consider using this feature to help you track down your device. If you decide to use it, check your settings to be sure it is enabled as soon as you start using the device.

8. Enable remote wipe.
Just in case you don’t have any luck locating or recovering your device, enable remote wipe on your smartphone so that you can erase the data in case it is lost or stolen.

9. Back up your data.
Let’s say you’ve lost your device. You used “Find my device,” but you couldn’t recover it, and then you wipe the data. Now what? You’re going to want to have a backup. Always keep your data backed up. I’m going to say that again. Always keep your data backed up; it’s critical in case you lose your device, or if it stops working, or if you get hit by ransomware.

10. Dispose of devices properly.
Don’t recycle, trade in, sell, donate, or surplus your device before wiping the data off of it or your information could end up in the wrong hands. That doesn’t mean just deleting files and applications; you should use tools such as factory reset on smartphones or use DBAN or built-in tools for laptops to completely erase the data.

11. Know the UW policies.
A few UW Administrative Policy Statements (APS) are helpful in considering the use of mobile devices to store and access University information.

One of these is APS 2.4, which defines three types of data:

- Public
- Restricted
- Confidential

Get to know about these UW data classifications, and keep them in mind as you manage information on your device.
Additionally, please be aware that APS 55.1 says this:
“Employees are expected to configure mobile devices that are used to conduct UW business, whether personally owned or provided by the UW, in such a way that protects University information. Click APS 55.1 in the links menu for more information.

12. Don’t forget physical security.

- Never leave your laptop or mobile device unattended,
- Record serial numbers on all devices and keep them accessible,
- When traveling, lock up devices that are left in your hotel room, and
- Consider using temporary devices for international travel.

And one more thing:

Report incidents: If a device that you use to access UW data is lost or stolen, report it. Click “Report” in the links menu for more information.

Thanks for listening, and thanks for safeguarding UW information.