Video 3: Device Security

Topics in this Module

Welcome to NAU's Information Security Essentials training. This module includes the following topics:

- Locking Your Computer
- Sensitive Information Storage
- Antivirus Software
- Software and Operating System Updates
- Encryption
- Public Computers
- Smartphones, iPads, and Tablets

To learn more about these topics, click "continue". To jump straight to the tutorial quiz, "jump to quiz".

What is on my Computer?

If you're like most people, you access a lot of information on your computer. In addition to the files stored on your computer, you may also use your computer to access NAU email, PeopleSoft LOUIE account information, SalesForce or OnBase information, perhaps student information if you are taking classes, and on occasion even your bank account or other personal accounts. Now, what if we told you that someone who gained access to your computer could have access to any of these things? That's pretty scary, right?

Luckily, there are a few steps you can take to prevent others from gaining access to both your work and home computers, and the information on them.

Lock your computer

You should always make sure your computer is locked or logged off before you leave it unattended. Even if you are only going to be away from it for a few minutes. Locking your computer ensures that no one else will be able to access it while you are away. Locking your computer is a really simple process and only takes a second. The easiest way to lock a Windows machine is to hold down the windows logo on your keyboard and the L key together. Then, when you get back to your computer, hold down Ctrl, Alt, and Delete together and then enter in your password. On a Mac, you will need to configure your computer first to require a password after sleep or screen saver begins. To learn how to configure your Mac and lock it quickly, view this tutorial.

Sensitive Information Storage

Data cannot be lost from a machine if it is not there. Do not collect or store sensitive information on your computer such as social security numbers and dates of birth. If you are collecting sensitive data it should be stored securely and in a proper location. In general, avoid storing it locally, on laptops, or on a computer at home. If you aren't sure how to store sensitive information, ASK! Start by calling the Solution Center at 523-1511.

Antivirus Software
An up-to-date antivirus software installed on your computer is an important step towards insuring the security of your computer. Antivirus software is used to prevent, detect, and remove malicious software on your computer.

Because antivirus software is necessary for any secure desktop and laptop, it is mandatory on all NAU owned computers, including Apple computers. If your computer is on the NAU domain, it is automatically installed on your computer. If it is not on the NAU domain, you can download free anti-virus software. Please visit the NAU ITS website for a list of options. If you're not sure if your computer is on the NAU domain call the Solution Center.

Updates
Updating is another critical step in securing your computer. As companies discover flaws in their software, they release patches in the form of updates to cover security holes in their software. By keeping your computer and all the software on your computer up-to-date, you can ensure that your computer will be protected from the latest security threats.

Updating Your Software
If you have a Windows computer on the NAU domain, common software, such as your computer's operating system, AntiVirus software, and Java, will download software updates automatically, but you will still need to restart your computer to install the updates. You will receive a pop-up message on your computer when these updates are ready. We suggest that you regularly check your computer for any out of date software and set up automatic software updates when possible. For Macs, you will receive a notification at the top of your computer that you have an update. Whenever you see this notification, update your Mac immediately. It will only take a few minutes.

If your computer is not on the NAU domain or is a Mac, we recommend that you check software such as your operating systems, your antivirus, programs such as Adobe products, browsers such as Firefox and Chrome, and plugins such as Java and Flash regularly for updates. Many software packages have the option to set up automatic updates and we highly recommend that you do this. For more help keeping your computer up-to-date, check out the links we have provided you on this slide.

Encryption
If you need to store sensitive information on a laptop or a portable storage device, such as a flash drive or an external hard drive, you do run the risk of losing these devices or having them stolen. This is why all NAU owned Windows laptops should have encryption software installed and activated. We highly recommend that you encrypt other portable devices that are used for NAU business. Encryption will give your data an extra layer of protection beyond just a system password. With encryption, no one can get access to the data on your device, even if they remove the hard drive and connect it

to another computer. NAU offers support for hard drive encryption. If you would like assistance or have any questions regarding hard drive encryption, please contact the Solution Center.

Public Computers
Sometimes, you may need to access information from a computer in a public lab, such as one of NAU's computer labs. In these cases, be cautious accessing and storing sensitive information.

You should never access or save any sensitive information on a public computer. You cannot be sure that what you are saving will not be accessible to others who log on to that same computer.

Public Computers
As you peruse the web, your web browser remembers lots of information, such as sites you've visited, files you've downloaded, and sometimes even personal information you've entered into websites. You may not want other users who use the computer after you to see this information. Private web browsing allows you to browse the Internet without saving your history. However, private web browsing isn't necessarily secure web browsing. It will not make you anonymous or protect your information from the web; it just won't track your browsing history on that computer. You should still be cautious about what information you are accessing or inputting on a public computer, even with private browsing enabled. Enabling private web browsing will be specific to the particular browser you are using. To learn how to enable private web browsing, please see your browsers support information.

Public Computers
You should always log off a public computer before you walk away from it so that your information is protected before others use the computer. Click on the link below to learn how to log off a computer.

Smartphones, iPads, and Tablets
Desktops and Laptops are not the only type of computers we need to worry about anymore. Many of us are using smartphones, iPads, and tablets that have apps that allow us to access our NAU accounts, bank accounts, and other personal accounts at the touch of a button… and they fit in our pockets and bags. Because of their portability, these devices are more susceptible to loss and theft. The convenience of apps also means that anyone who has access to your device, may also have access to the information your apps connect you to.

Smartphones, iPads, and Tablets
This is why it's very important to use the security and lock features available on your device. If you're going to access your NAU Iris Exchange email or calendar on your phone, iPad, or tablet, you will be required to have a passcode in order to access your

device. Passcodes lock access to your device unless you have the code to unlock them. Passcodes protect access to the data stored on your device. You do not need to enter your passcode to answer an incoming call on your phone.

Smartphones, iPads, and Tablets

In the case of loss or theft, most phones and tablets provide a web-based tool to help you locate a missing device, such as Find my iPhone, Find my iPad, and Where's my Droid? These devices use the GPS on your device to show you its current location on a map, and, in the event you can't recover it, you can erase all the data on your device using this web service.

If you do lose your phone or tablet and you have accessed NAU resources such as your email or calendar on it, we recommend calling the Solution Center and changing ALL of your passwords in addition to these other tools.