Prevention and Awareness for Your Home Network

Crucial Takeaways from Our Presentation:

Updates and AntiVirus
Keeping your operating system up to date is one of the most important steps to take when preventing malicious attacks. Instructions can be found at the following links to ensure that your Windows or Mac operating systems are up to date:

Microsoft Windows Update:

Microsoft Windows Defender:

Apple macOS Update:
https://support.apple.com/en-us/HT201541

Sophos Anti-Virus
As an employee at the U of A, you have access to the home version of Sophos’ antivirus software. For more information about Sophos Endpoint Security and Control, visit the following link:
https://softwarelicense.arizona.edu/sophos-endpoint-security-and-control

VPN
The University of Arizona’s VPN (Virtual Private Network) can be used to create a secure tunnel to prevent hackers from intercepting your activity on the web and stealing your information. Use the link below to get more information about the University’s VPN:
https://it.arizona.edu/service/ua-virtual-private-network-vpn

Personal WiFi Security
All WiFi routers come preconfigured with a generic login to the administrator settings. This is a crucial setting to change, and many routers’ admin passwords go unchanged. Find instructions below from some of the major router manufactures on how to login and change the admin password on your router. If you do not have a router from one of these manufacturers, try a Google search with your router’s manufacturer name and “change default admin password”. 
Information Security and Data Classification

Campus Security Policy
The University has a robust and informative information security policy. More info on that can be found here:

https://security.arizona.edu/policy

Data Classification
Knowing what type of files you work with, and where those files should be stored, is an integral part of working with University data. For more information on this, follow this link:

https://security.arizona.edu/data-classification-and-handling-standard

HTTPS and SSL Certificates
Instructions on checking a website's SSL certificate:

https://support.mozilla.org/en-US/kb/secure-website-certificate

Backups
Local
Backing up your data can be as simple as plugging in a flash drive, external hard drive, or other disc media. Without backups of your data, all information (including pictures, crucial documents, etc.) will be lost.
Windows has a built-in suite of apps to make sure your data is backed up, and that your computer is making "restore points" to revert to if necessary. For more information on configuring these apps, follow the link below:

https://support.microsoft.com/en-us/help/17127/windows-back-up-restore

Apple has a built-in data backup application on their operating system called the 'Time Machine.' Using this tool only requires an external hard drive. Instructions on setting that up can be found below:


Cloud-Based
There are many cloud-based backup options available with subscription fees. The advantage with cloud-based backups, is that you would not be at risk of losing your information if your backup media was a physical drive within your home. The links are for one good option for this service, among many:

https://www.carbonite.com/