# **Stay Safe Online - Student Tips**



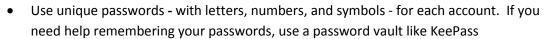
**Review your Social Media Privacy settings -** customize your privacy settings and think about what you share. Be careful talking about your location, or anything that you wouldn't want Grandma - or a future employer - to see.

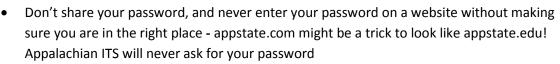
**Don't link your social media accounts together -** one hacked account gives the hacker access to all linked accounts

**Be aware of online scams -** don't get lured by phishing! Report attempts to get your username, password, or other personal information to <a href="mailto:phish@appstate.edu">phish@appstate.edu</a>

**Log Out before you walk away from a public computer -** logout of your MountaineerApps account and the public computer

### Use good passwords and keep them safe





### **Keep clean machines**

 Make sure your device and software is set to install regular updates, and use Antivirus software

Back up your files with an external device and/or MountaineerDrive

# **Connect Safely**



THINK

 Use a secure wireless connection, like "asu" wireless network, or be aware that you are on a public connection when you connect to public wireless

Use https whenever you transmit confidential information to a website

# Be careful where you click

- Use official sites like Google Play Store to download apps, and review what they want to access
- Don't open questionable email attachments or click on ads on websites

#### Resources

security.appstate.edu/students for security tips and resources for students

support.appstate.edu/students for free antivirus software, and other support information for students

security.appstate.edu/phishing lists reported phishing attempts



Our **Technology Support Center** can troubleshoot problems, and remove virus and spyware from your devices.

See something suspicious?
Report Issues Promptly -Call the
ITS Help Desk at 828-262-6266