Protecting Yourself in a Hostile Online World
On Campus

• Pomona provides security to your College computer while on campus
• Antivirus software
• Firewall and network segmentation
• Active monitoring
Your College Computer

• Security updates – just say yes
• Alert ITS immediately if you are seeing signs of viruses or malware
  • Can include popups, slowness, crashing, errors
• Do not let your children or family members use your College computer
• Always lock your computer or device when you step away
Your Home Computer & Devices

• Security of your home computer & devices is your responsibility
• Keep software up-to-date with the latest security updates
• Install and keep antivirus software up-to-date
• Encrypt your hard drives
• Don’t use removable storage like USB flash drives, external HDs, etc.
• When working on College data, use the Terminal Server
• Do not use an Administrator account – create a separate “standard” user account for every day use
Your Password – the keys to kingdom

• NEVER share your password with anyone
• Use different passwords for different services
• If you have trouble remembering your password, use a Password Manager, or keep a physical list of passwords locked away
• Always think twice before entering your password anywhere
• Avoid easy to guess words and bio info for passwords
• If you think your password may be compromised, change it immediately
On the Road

• If you can do without the device, don’t take it
• Make sure that your device is encrypted & protected with a password or passcode
• Back up all of your devices before you leave and leave the back ups at home or in the cloud.
• Do not leave computers or devices unattended
• Use hotel room safes when you are not in your room
• Be wary of your surroundings at all times
  • Don’t stare at your phone or appear distracted while using devices in public
  • Don’t listen to loud music or wear big headphones
Crossing Borders

• Turn off biometric readers on your devices (TouchID, FaceID)
• Consider getting an inexpensive or disposable device to use such as a “burner phone” for your travel abroad
• Restore your device to factory defaults before crossing borders
• Power off devices before crossing borders
• Remove social media apps from your devices
Be wary of wireless networks

• Confirm the name of the network with wi-fi provider before connecting
• Avoid FREE WIFI networks at the airport (or anywhere)
• Use VPN
• Avoid banking and other sensitive activities on public wi-fi networks
You are the first line of defense

- Trust no one – if it sounds too good to be true, it probably is
- Be wary of any e-mail that implies urgency or exhorts you to quick action
- Don’t go chasing waterfalls – please stick to the river and lakes that you’re used to (aka be cautious when using Google)
- If you think your computer has been compromised, do not call phone numbers proffered onscreen, call ITS first
- Never allow unknown, unsolicited “tech” people to connect to your computer
Keep a low profile

• If you use Social Media, do not put personal information online
• Adjust your privacy settings to the most secure levels
• Do not allow “friends of friends” to see your posts or information
• Do not post when you are on vacation or not home
• Avoid unnecessary risks like games, apps, and surveys that install in your social media profile
When you’re online, everything that’s free has a price
Further Reading

• IT Security Blog: http://research.pomona.edu/itsecurity/
• Stay Safe Online: https://staysafeonline.org
• Like “Facecrooks” on Facebook

Getting help from ITS

ITS Service Desk: (909) 621-8061 or x18061 servicedesk@pomona.edu