The Threats

- Malware Infections
  - Drive-by-Downloads – vulnerable software
  - Social Engineering – misplaced trust
- Trusted third-party compromises

Defend Yourself against Web-based Attacks

Run the Latest Version

- Update your browser (Internet Explorer, Firefox, Chrome, Safari)
- Update your browser’s plug-ins (Flash, Java, QuickTime, etc)

Enable click-to-play in your web browser and keep your browser plugins updated

- Qualys BrowserCheck browsercheck.qualys.com
- Mozilla Plugin Check www.mozilla.org/plugincheck
- Secunia PSI secunia.com/vulnerability_scanning/personal

Stop, Think, Click (or don’t)

- Be skeptical, exercise common sense. Don’t automatically trust every link or offer.
- If you’re not sure, don’t click the link, verify...
  - VirusTotal www.virustotal.com/#url
  - McAfee SiteAdvisor siteadvisor.com
  - BrightCloud URL/IP Lookup www.brightcloud.com/tools

Java & Javascript

- Java – if you don’t need it, uninstall it. If you do need it, consider disabling it in your web browser if you can.
- Javascript – consider the use of these tools to selectively disable Javascript on a site by site basis:
  - NoScript (Firefox) noscript.net
  - ScriptSafe (Chrome) goo.gl/EG8EP
Defending Yourself against Malware

1. Don’t run as Administrator
2. Keep your Operating System (OS) Updated
3. Use up-to-date Antivirus software & scan regularly

Use AntiVirus (AV) Software

- There is no silver bullet. No product can protect against all threats.
- Antivirus software should be updated automatically and updated often.
- Some AntiVirus software options to consider:
  - Microsoft Security Essentials (Win 7) www.microsoft.com
  - Microsoft Windows Defender (Win 8) www.microsoft.com
  - Kaspersky Anti-Virus (Win) usa.kaspersky.com
  - Malwarebytes (Win) (on-demand) www.malwarebytes.org
  - Super Antispyware (Win) (on-demand) www.superantispyware.com
  - Avast! (Mac / Win) www.avast.com

Update Your Software

Most Targeted Software
- Oracle Java
- Adobe Flash
- Adobe Reader
- Microsoft Office
- All web browsers

Secunia Personal Software Inspector (PSI)
- Scans your Windows computer for outdated software and either updates them automatically or provides direct download links to the most recent versions.

AppFresh for Mac
- http://metaquark.de/appfresh/mac

Defend Yourself against Email Threats

Avoid SPAM - Protect your e-mail address
- Avoid using your UF e-mail address for non-UF purposes
- Avoid giving your personal e-mail address to anyone other than family, friends, or business associates
- Create and use a separate e-mail address or use “throw-away” e-mail addresses for public use
- Consider use of: spamgourmet.com mailinator.com trashmail.net spamex.com

Phishing Attacks

How to catch a Phish –

Phishing messages usually...
- attempt to build credibility by spoofing a real company, brand, or yes, even a major state university
- create a false urgency requiring a quick response – threaten to close your account if you don’t reply
- insist on a call to action - click a link or reply with information
Don’t take the bait –
- Be suspicious by default of any e-mail with and urgent request for personal information
- Don’t use the links in an email. Manually enter the web address in your browser.
- Ensure that you’re using a secure website when submitting credit card or other sensitive information via your Web browser.
- Never give out account or personal information by email.

Choosing a Good Password  \( \text{Entropy + Length} = \text{strong password} \)
- Choose a combination of letters, numbers and symbols, mixing uppercase and lowercase letters
- Be sure your password doesn’t form a real word that can be looked up in a dictionary.
- Choose a combination that makes sense to you and is easy for you to remember but isn’t obvious to others. Consider basing your password on a phrase.
  - “To be or not to be, that is the question” becomes “tobe,ornot,tobe,the?”
- Create a unique password for each site by generating a password recipe.
- A password recipe is a custom formula that combines a good base password, padding characters, and information specific to a site to form a strong personalized and unique password. Some examples:
  - base + padding + domain = tbontb%amzn or lLoveDietCoke+fb
  - padding+base+padding+domain+padding = ..123SW2nd+BOA.. or !123SW2nd+FB!

Password Managers
- LastPass - lastpass.com
- 1Password - agilebits.com
- mSecure - msevensoftware.com
- Master Password - masterpasswordapp.com

Data Security

No system is completely secure.
Things happen.  Defend yourself.
- If you have important files stored on your computer, back them up.
- Use encryption software when storing sensitive data.
- Remember the 3-2-1 Rule...
  - 3 backup copies, 2 storage media types, 1 off-site backup site

Backup Data Options:
- second internal hard drive - out of sight, set it up and forget it
- external hard drive or network attached storage (NAS) device - bundled backup software
- CD-Rom, DVD, Blue-Ray media - inexpensive, one-off backups, manual process
- USB Flash drives - limited capacity but highly portable, available with encryption
- Online services – CrashPlan (crashplan.com), Carbonite (carbonite.com), Mozy (mozy.com), SpiderOak (spideroak.com), Waula (waula.com)
- Trust No One - Use private-key, pre-Internet encryption
- \textit{Never store unencrypted UF Restricted Data in the cloud}
Encryption Tools

- Windows BitLocker (Win)
- FileVault (Mac)
- VeraCrypt (Mac/Win/Linux) ([veracrypt.codeplex.com](http://veracrypt.codeplex.com))
- WinZip ([winzip.com](http://winzip.com)), 7-Zip ([7-zip.org](http://7-zip.org)),
- AES Encrypt (Mac/Win/Linux) ([aescrypt.com](http://aescrypt.com))
- USB flash drives or external hard drives that support hardware level encryption

UF’s Mobile Computing and Storage Devices Policy
[www.it.ufl.edu/mobile-computing-storage-devices](http://www.it.ufl.edu/mobile-computing-storage-devices)

Wireless Security at Home

- Spend 10 minutes getting to know your device - Read the manual!
- Change your default Administrator Password
- Enable Encryption (WEP, WPA, WPA2)
- Change the default SSID
- Apply MAC Address Filtering
- Consider using OpenDNS for domain name service

Wireless Security on the Road

- Turn off your wireless adapter when you’re not using it
- Verify the SSID belongs to the public provider
- Use encryption when available
  - https:// SSL for websites
  - UF VPN – [https://vpn.ufl.edu](http://https://vpn.ufl.edu)
- Avoid accessing sensitive sites and using hotel Internet kiosks