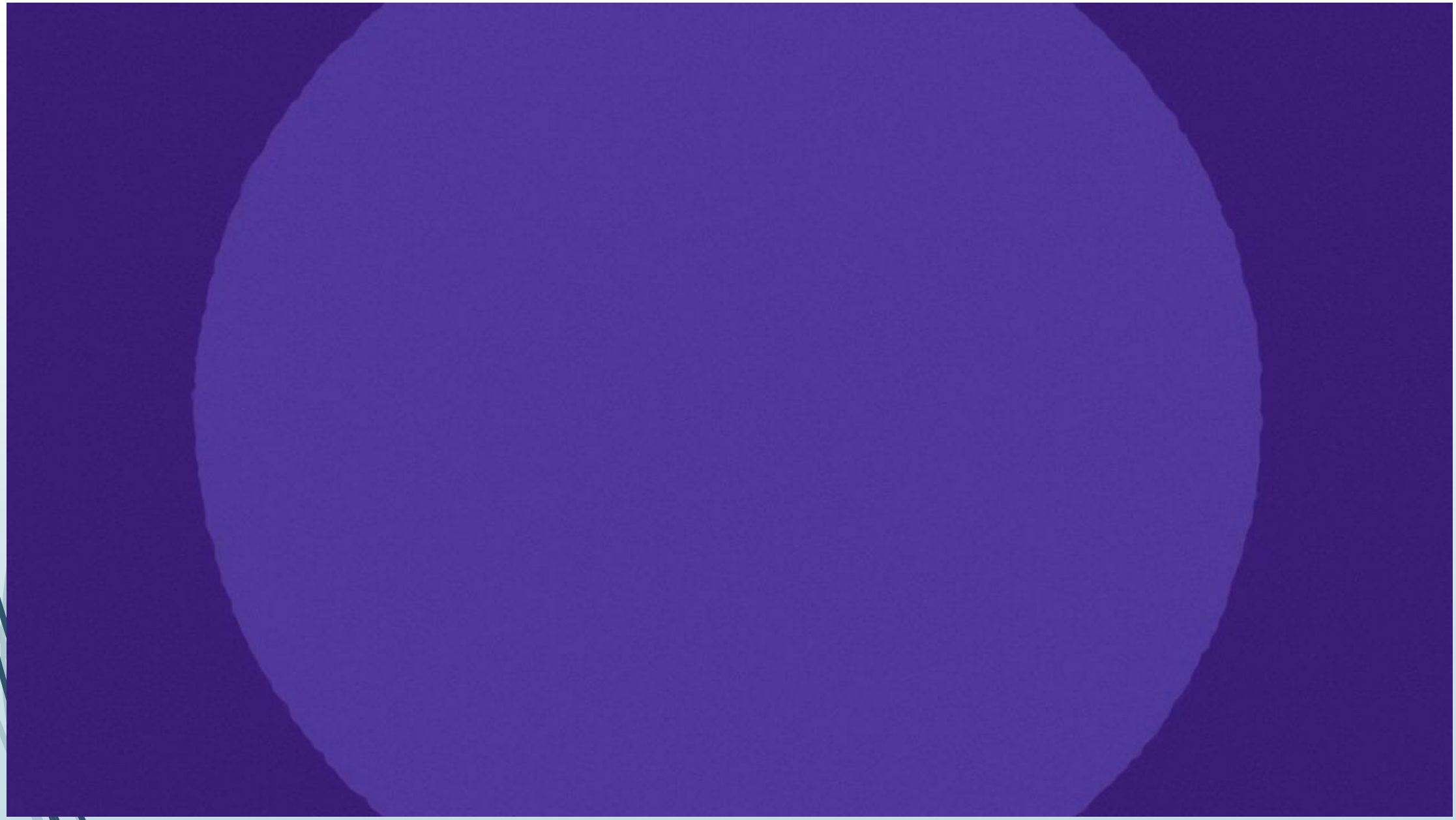
Internet Safety

Fall 2023

What Is the Internet?



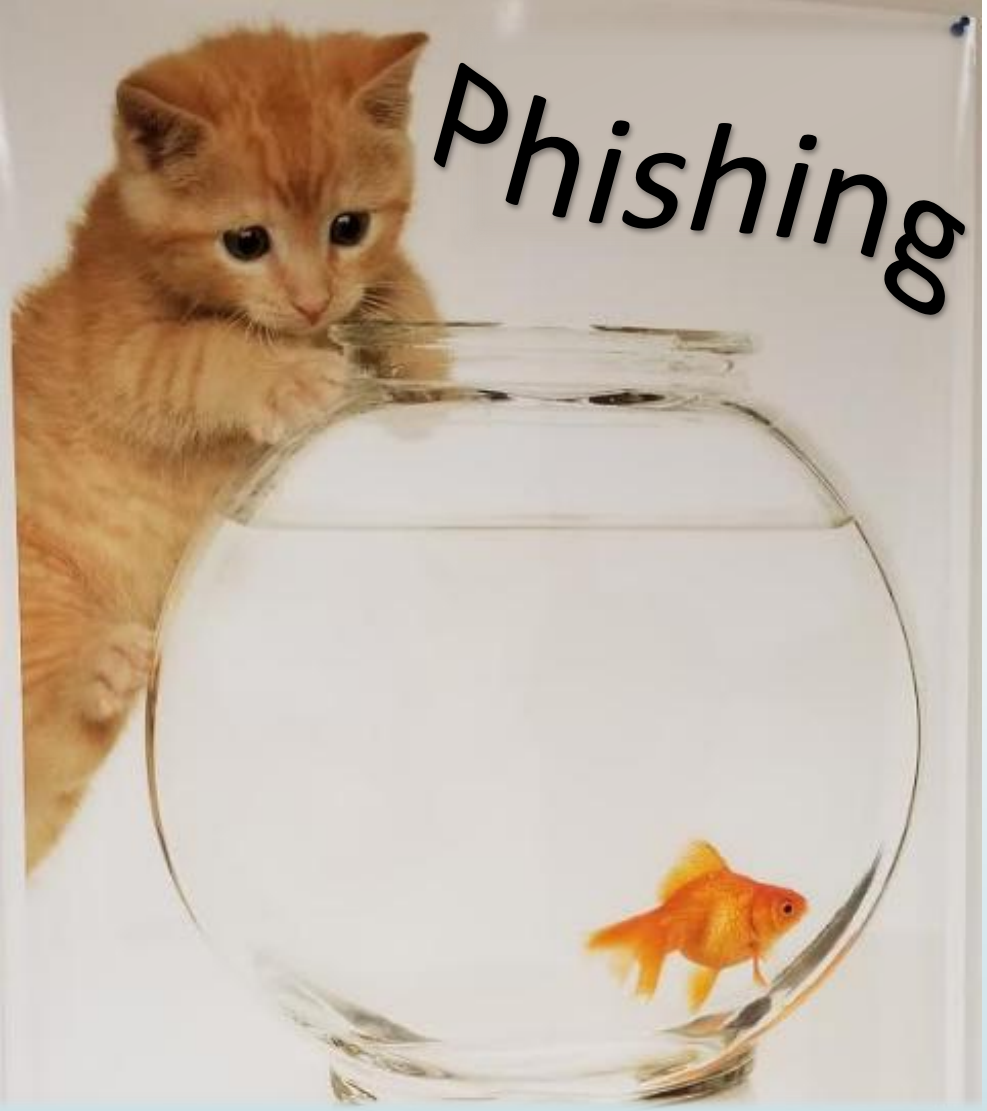
Browsers Connect Us to the Internet

- Browsers for desktop computers & laptops
- Browsers for tablets & phones

All About URLs (Uniform Resource Locators)

New to the Internet?

- **Here are some links for learning more about the Internet**
- http://www.internet101.org/category/internet-101/
- https://edu.gcfglobal.org/en/internetbasics/what-is-the-internet/1/
- http://www.seniorsguidetocomputers.com/internet.asp



Hackers and Other Threats

- Viruses
- Identity Theft
- Phishing
- Scams
- Ransomware
- Hijacked Email
- Bloatware
- Adware
- Popups
- Unwanted Toolbars and Downloads
- Unscrupulous Phone Calls

Common types of Malware

Virus

A virus is an executable type of malware that self-replicates by infecting and modifying a program's existing code and inserting its own code.

Trojan Horse

A trojan presents itself as or hides in a legitimate program. Once downloaded it can steal sensitive data by misleading the user into giving it special access.

Ransomware

Ransomware takes control over a computer and holds it hostage until a ransom is paid. If no payment is made, data will be deleted or released on line.

Rootkit

Once a root kit gains access to a computer's OS, it can conceal itself or other malware, execute files, and even make changes to a system. It's nearly undetectable.

Worm

A computer worm is a malware computer program that replicates itself in order to spread to other computers. It does not rely on human action.

Spyware

Spyware is a kind software that installs itself on to a computer and starts covertly collecting, tracking, and stealing the user's sensitive data.

DIGITAL **TRENDS**

Download Cautions

- Internet downloads have a well-earned reputation for containing malware and bloatware
- Download only from reputable sites
  - Check the URL for https
  - Know or research your download provider
- Read everything as you install
  - Bloatware often accompanies free software, even when from a reputable provider

Security Software

- Top software constantly shuffling
- Evaluating Security Software
  - Safety Detectives – links with discounts
  - PC Magazine
  - Cyber Magazine
  - Tech Radar
  - AV Test – Independent testing

Securing Internet Hardware

- Modems, Routers and Gateways
  - Without Password Protection – Anyone Can Hack into Your Online Computers
  - New Internet Hardware comes with Password Protection
  - Older Hardware can be Password Protected
    - Find original manual
    - Look up your model online & download instructions

Be Alert – Check First

- Look for https:// at the beginning of the address bar when viewing sensitive websites or data
- Hover mouse over links to check for the real address before clicking (Link)
- If a site doesn't look quite right, double check the address bar

Use Strong Passwords!!!

- Long passwords are harder to crack (at least 12 characters)
- Use all allowed character types
  - Alpha (A-Z) – upper and lower case
  - Numeric (0-9)
  - Special Characters (!, #, $, *, _, -, etc.)
- Make up acronyms
  - My Dog Has Fleas, and so do my five cats! = mDHF,&sdm5c!
- Test your passwords https://www.security.org/how-secure-is-my-password/
- Create a password system to use different passwords for different websites

2-Step Verification
a.k.a. multi-factor authentication

- Adds extra security in case a password is hacked
- Sign in using 2 factors
  - Something you know (password, personal info)
  - Something you have (cell phone, email, authenticator)
- Recommended for monetary and personal identity accounts like banking and health records

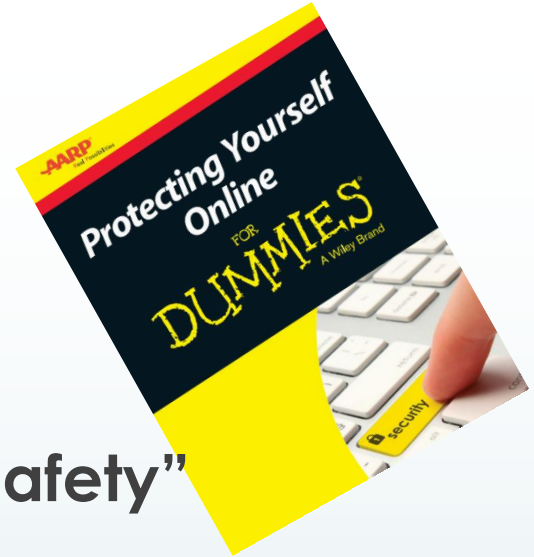
Too Many Cookies?

- A cookie is a small piece of data stored on the user's computer by the web browser
  - Stores information to be used when returning to a site
  - Such as your name, passwords, preferences, etc.
- Saves time for often visited sites
- May share your info with other entities (Trackers)
- Can be blocked and or deleted via settings/preferences
- Use privacy modes

Private Browsing Mode

- Let's you browse without accepting cookies or trackers
- Most browsers offer private browsing
  - Chrome uses Incognito Mode (Ctrl+Shift+N)
  - Bing uses InPrivate browsing (Ctrl+Shift+N)
  - Mozilla Firefox uses Private browsing (Ctrl+Shift+P)
  - Safari was the first to offer Private Windows (Cmd+Shift+N)
- Phones and Tablets
  - Android – 3-dot menu > New incognito tab
  - Apple – varies by device

Stay Informed



- Read AARP's "Protecting Yourself Online"
  - Especially Chapter 5 – "Shopping and Banking Safety"
- AARP also offers: http://www.aarp.org/money/scams-fraud/
- US Government Consumer Protection site: https://www.usa.gov/scams-and-frauds
- Federal Trade Commission: https://www.consumer.ftc.gov/features/scam-alerts
- Alerts from your bank and other financial institutions
- Be aware of breaking news about scams

If Your Email Is Hacked

- Change Your Password
  - Make it a secure password
- Enable Multi-factor Authentication
- Alert Your Contacts
  - Hint: Put yourself in your address book so you get a copy if you're hacked
- Use Your Email Provider's Website
  - Link to report abuse
  - Phone & email usually found in "Contact Us"

Report Fraud

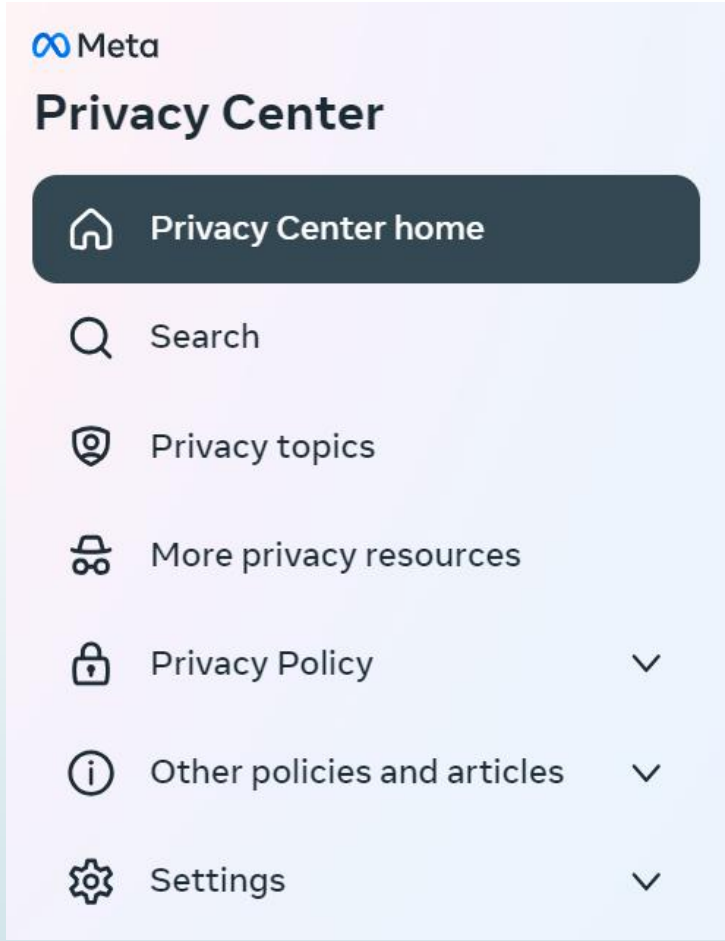
- Report Scams and Fraud
  - USA.gov offers links to report various scam types
- Report phishing emails to reportphishing@apwg.org
  - Report phishing tests to SPAM (7726) or
  - ReportFraud.ftc.gov

Stay Secure on Social Media

- Use Privacy Settings
- Check out what others see on your page
- Be careful what you post
- Be aware of how your accounts interconnect
- Consider using “false” data about yourself when sensitive information is required

Privacy on Facebook

- Search “View as”
  - Learn what others see (Public vs Friends)
- Right-click your avatar
  - Visit Settings & Privacy to change your settings
- Manage Profile settings
  https://www.facebook.com/privacy/center/
  - Go To Facebook Settings to control several factors



Stay Safe Shopping

- Use Well-Known, Secure Internet Sites
  - Internet Site also has Bricks and Mortar stores
  - Internet Site has https: in URL or takes the shopper to a secure https: link to complete the purchase
- Set up an email account specifically for shopping
- Use a strong passwords for your accounts
- Use a low limit credit card for purchases or
- Use PayPal or Google Wallet to complete a purchase
  - Consider low limit bank account
- Trust your gut and/or check with the BBB

VPN (Virtual Private Network)

- VPN Software creates a secure connection
  - Private browsing history
  - Hides physical location
  - Provides anonymity
  - Encrypts your output
- Possible disadvantages
  - May slow your internet speed
  - Cost

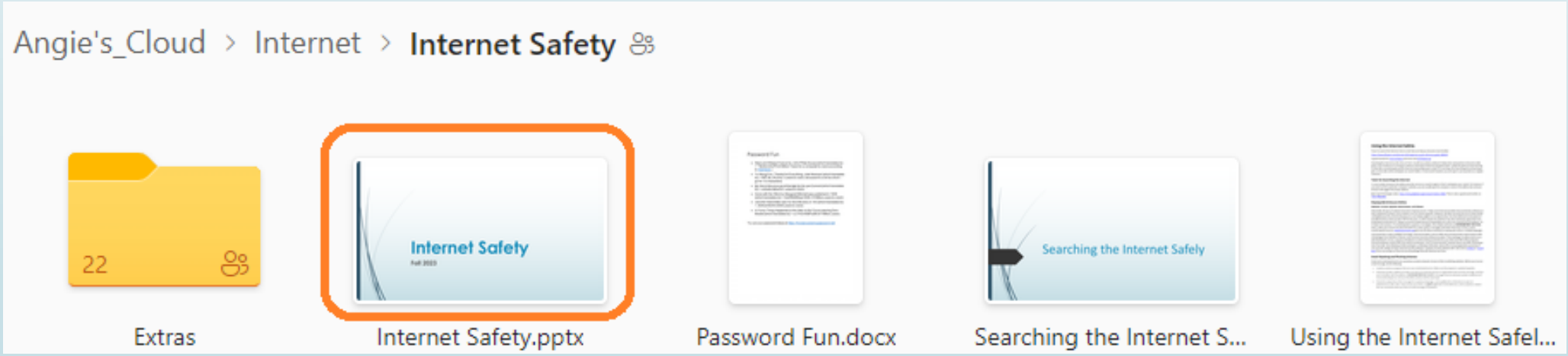
Additional reading:
https://whatismyipaddress.com/vpn

Seven Safety Moves You Can Make

1. Use reputable Internet Safety software and keep it updated
2. Be careful where you click (hover pointer to check the link)
3. Immediately close web pages that open unexpectedly (Alt+F4 or Esc)
4. Pop-up Blockers – check settings in browser
5. Buy genuine, recognized software and register it
6. Keep your software up to date
7. Regularly backup important files to external drive, cloud or backup service

Class Information Available

- This PowerPoint and supporting documents are available online.
- Go to https://angitech.me/learn
- Click on Angie's Cloud
- Locate the Internet folder and open Internet Safety



Other Resources

- Avoiding Online Scams from McAfee
- Internet Plans & Discounts for Seniors
- Chase Security Education
- Angie's Pages
  - Website – angitech.me/learn
  - Free Handouts – Angie's Cloud
  - Contact Angie