

# Staying Safe Online

---

---

---

---

---

---

---

---

- ## Anti-Virus Software
- Any major brand is good
  - Symantec, McAfee, Webroot, Trend Micro
  - They all provide anti-virus and anti-spyware in one package
  - Important to keep software updated at least weekly and pay for subscription yearly
  - Run scans on your computer bi-weekly
  - AVG and Avast are free options

---

---

---

---

---

---

---

---

- ## Malware
- Viruses, Trojans, Spyware
  - Collect and send user information to a central location for data mining
  - A hacker can end up “owning” your computer
  - Bogs down bandwidth, computer processing and can lead to data and privacy loss
  - Often comes with “FREE” software and also found on infected websites
- 

---

---

---

---

---


---

---

---

## Adware/Spyware

- Weather Bug
- Smiley Faces
- Browser Toolbars
- File Sharing Programs and Freeware
  - Be aware of what you're installing
  - All file sharing programs contain adware/spyware
  - Share files on your computer to the World!



---

---

---

---

---


---

---

---

## Avoid Identity Theft

- Think about the information you share on social networking sites. Consider almost everything public
- Look at your privacy settings and understand with whom you are sharing your information
- Consider all things posted in the digital world permanent. It is almost impossible to put the genie back in the bottle



---

---

---

---

---


---

---

---

## Online Safety

- Go over your credit card and bank statements at least monthly
- Track down any odd charges no matter the amount
- Often times a thief will make a small charge to see if the card is active, if no action is taken a large charge might happen soon after



---

---

---

---

---


---

---

---

### Online Safety

- Consider requesting a new card, with new account numbers once a year to thwart theft
- How many different stores, restaurants, and online stores have you made purchases at in the last year?
- Credit cards offer more protection online than do debit cards. See Fair Credit Billing Act
- Consider using PayPal



---

---

---

---

---

---

---

---

### Online Safety

- Create and use a free e-mail account for situations where you need to "sign up" or "login" for something on the web
- Do not respond to Spam e-mails by clicking on the "unsubscribe" link at the bottom of the e-mail
- Do not use the same password for multiple web sites, use variations



---

---

---

---

---

---

---

---

### Online Safety

- Do not respond to e-mail requesting personal or account information
- You are never going to be asked to provide this information via e-mail from a legitimate organization
- You did not win the Irish Lottery, nor does some guy in Africa really want to share his good fortune with you!
- Stop and think before you click



---

---

---

---

---

---

---

---

### Updates

- Keep your home computer patched and up to date, hackers attack long known computer problems that there are fixes for
- Use **Windows Update** - Internet Explorer – Safety - Windows Update
- Apple Icon - Software Updates
- Check many other programs on your computer that need to be updated by going to [secunia.com](http://secunia.com) and click on “Scan Your PC”

---

---

---

---

---


---

---

---

### Safe Browsing

- Most viruses and malware now come through the web browser from infected web sites. An up to date browser and up to date anti-virus software will prevent many problems
- Use either Firefox or upgrade to Internet Explorer 8, keep the browser up to date



---

---

---

---

---

---

---

---

### Internet Explorer 8

- Within Internet Explorer 8 there is a new feature called **InPrivate Filtering**
- **InPrivate Filtering** prevents websites from collecting and gathering information about web sites you have visited during your private session
- It enables you to block the common content that might provide information about your browsing
- Prevents targeted ads based on your browsing

---

---

---

---

---


---

---

---

## Internet Explorer 8

- To Enable **InPrivate Filtering**:  
Internet Explorer – Safety – **InPrivate Browsing**  
Opens a new browser window with the **InPrivate** indicator next to the address bar




---

---

---

---

---

---

---

---

## Firefox

- The latest version of Firefox has **Private Browsing** which will also protect your privacy
- To enable **Private Browsing** click on Tools -> Start **Private Browsing**




---

---

---

---

---


---

---

---

## Firefox

- Firefox has **Add Ons** that help prevent malware infections on your computer while surfing.  
Some popular **Add Ons** are:  
**Ad Blocker** – blocks most advertisements on web pages which can be a source of malware  
**Web of Trust** – warns you of dangerous websites




---

---

---

---

---

---

---

---

## Online Safety

- Be smart when you are online
- Stop and think before you click
- Good websites for more information:
  - [onguardonline.gov](http://onguardonline.gov)
  - [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)
  - [microsoft.com/protect/default.aspx](http://microsoft.com/protect/default.aspx)
  - [www.staysafeonline.info](http://www.staysafeonline.info)

---

---

---

---

---


---

---

---

## Wireless

- Turn on the built in security (encryption). Encrypts the wireless traffic so neighbors or others can't steal your connection and potentially access your computer
- Change the default SSID
- Be very careful what you do online with "free" or "public" access points. They can be very insecure



---

---

---

---

---


---

---

---

## Shared Resources

- Turn off Windows File and Printer sharing if not used
  - 1. Under Control Panel, Network connections, Right-click and choose Properties on your network connection.
  - 2. Highlight "File and Printer Sharing for Microsoft Networks" and click "Uninstall"
  - 3. Click Ok and you are done.
- If you do share files between systems, you can limit access with your firewall.



---

---

---

---

---


---

---

---

## Data Storage

- Store important documents on network drives (K:/R:), network drives are backed up nightly
- Be aware of what you store on USB drives. They are easily lost
- There should be no confidential information stored on laptops/pc internal hard disks.
  - \* If your job requires it, we can install encryption software on your work computer



---

---

---

---

---


---

---

---

## Physical Security

- Keep office doors locked
- Keep your laptop out of sight (store it in the trunk when leaving it in a car)
- Keep sensitive data locked in a file cabinet



---

---

---

---

---

---

---

---

# Thank You

Questions?

---

---

---

---

---

---

---

---