STOP. THINK. BEFORE YOU CLICK.

- Think before giving websites permission to download anything on your computer
- Think before letting a website post advertisements and put add-ons onto your browser
- Think about what information you post online, ask yourself the following questions—if you say "no" to any of these you may not want to post
    - Is it True?
    - Is it Helpful?
    - Is it Inspiring?
    - Is it Necessary?
    - Is it Kind?
- Think about who can see it
- Think, not everyone is a friend, some are trolls and hackers who may use your information for illegal activities (identity theft, fraud, clone your computer/phone, steal financial information from you or your parents/guardians, etc.)
- Know who you are "Friending" online—because not everyone is who they say they are online

STOP.
THINK.
BEFORE
YOU
CLICK.

INFORMATION

Red Mountain LIBRARY

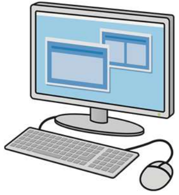
DIGITAL SAFETY

REDMOUNTAINLIBRARY.WEEBLY.COM/

CONSIDERATIONS

REMEMBER
The internet is forever

- Anything you post online or have done online is stored in the cloud by servers
- Some information may get deleted within 10 to 20 years
- But, some people may have saved what you posted and it could come back to hurt you in the future, just watch the news about what has come to haunt politicians, celebrities, etc.
- Nothing is as private as you wish it was



Public Computers

- Don't save passwords
- Log out before you leave
- Saving a document to the computer? Password protect it, so only you can open it.
- Remember what computer you use
- Don't click yes for anything—ask the computer monitor/teacher/librarian if it is safe to click "ok" or "yes" on it first
- Don't change any settings on the computer, as it is not yours and most organizations make sure security settings are set to a maximum to protect the computers and the servers
- When in doubt, ask the computer monitor/teacher/librarian
- Remember, there is NO privacy on a public computer

LOOK FOR RED FLAGS

- Does the website ask you to sign up or give permission for something before you can use it or play on it? If yes, it may not be safe.
- Try not to click on a link in an email; type in the URL instead.
- Phishing sites are made to look real—these websites are used by hackers for illegal activities
- Password protect your devices (Wi-Fi network (hub), smartphones, and other smart devices such as smart TVs)
- Use free Wi-Fi networks with caution
- Know whose Wi-Fi you are using—just because its free doesn't mean its safe
- Look for https:// in the URL, especially if you are buying something, if it doesn't don't use it
- Check bank statements—as you get older and have more financial records, check them for inaccuracies or purchases you didn't order and report them
- Check your email properly
  - Beware of "phishing" emails, which use a hook such as asking you to confirm security information in order to steal your personal data
  - Spam email is getting more and more sophisticated so never respond to any emails with your account information or passwords
  - Banks will never ever ask for your information in this way. If in doubt, call the bank directly to check or, better still, delete the email.
  - Check the e-mail address or LOGO, does it match what the business or organization normally use or is it a little off?

MAINTAINING SAFETY

Passwords

- At least 8 characters long
- Be random with words
- Use numbers in place of letters
- Don't use personal info for passwords
- Don't use one password for everything

Set Your Security Settings

- All social media sites have security settings, just go to your account settings menu
- Know who you are sharing information with
- E-mail security needs to be set up too
  - Create backup security for resetting your passwords
  - Set sharing settings for files, calendars, etc. to be view only
- Re-check settings after updates that they weren't reset to defaults
- You control what people know about you, set limits so you can share personal information (phone number, e-mail, physical location, etc.) when you want to

Antivirus software

- All computers come with a basic antivirus software, but make sure it is turned on and settings are at maximum

Update your software

- It is good to double check that your software is up to date
- Updates ensure current bugs, glitches, and/or weaknesses in security are fixed/added as developers come out with new stuff all the time