Internet Safety & “Fake News”

Thurs., Aug. 9, 9:30-11:30am Saratoga Springs Public Library

Presented by

Kathy Handy, Computer Instructor at Saratoga Springs Public Library
Mary Ratzer, Reference Librarian at Saratoga Springs Public Library, Author, Educator
Tena Tyler, Senior Editor for Engagement at the Times Union
Internet Safety

• Virus Protection Software
• Firewall
• Spyware and Malware Protection (often through Virus Protection Software)
• Use up-to-date browsers such as Google Chrome, Safari, Microsoft Edge, Mozilla Firefox
• Update Operating System & Software (including browsers) when needed
Internet Safety Tips

- Use **strong** passwords
- Use **2 Factor Authentication** when you can
- Always log out of any application you log into such as email, especially on a public machine
- Avoid using **public** Wifi for things like banking or purchasing online
- For a personal, home wifi connection, make sure it is **password protected** and that it uses **WPA2** or the latest in security protection from your provider.
Website Check

- Who authored the site?
- **Green** address
- Did the site appear in a Google Search *without* AD identification?
- What is the site’s purpose or mission statement?
- Is contact information readily available?
- Has the site been updated recently?
- Does the “About” section detail the organization’s physical location?
- Award-winning?
- Browser verification (certificates or security)

Don’t believe everything you read or see…use critical thinking skills and think like a detective or reporter…
Email – as a general rule-of-thumb...

- **DELETE** any message that looks suspicious **BEFORE** opening it
- **DO NOT** click links in email messages, especially if there is an urgency in the message or strong emotion conveyed.
- **DO NOT** dial phone numbers appearing in an email.

**Note:** Phone Calls driven by con-artists also occur, and it is a good idea to allow a message machine to screen your calls. Some claim to be Microsoft, some claim to be the IRS – these fakes usually have a strong sense of urgency wanting you to pay OR ELSE. Don’t fall for them.
Social Media...

• Be cautious of Memes and Photos
  • Photos can carry malicious code
  • Be wary of photos of which you do not know the origin (PC World 3/27/2014)

• How to protect yourself on Facebook
  (NYT article, 3/19/2018)
  • https://www.nytimes.com/2018/03/19/technology/personaltech/protect-yourself-on-facebook.html

• Always check privacy settings as well as all settings in social media accounts such as location services, who can see your information, and more.

https://www.digitaltrends.com/social-media/facebook-i-button-fake-news/

Twitter: verify button
Facebook: information button
An example of how *true* information can be turned into misinformation or disinformation...or “fake news,” and why it’s important to keep critical thinking skills in tact!

Disinformation (Feb. 2018) – great example from WSJ – a 5.5 min. video

**The Big Loophole That Helped Russia Exploit Facebook: Doctored Photos**

https://www.wsj.com/articles/the-big-loophole-that-left-facebook-vulnerable-to-russian-propaganda-1519314265
Visit guides.sspl.org/computerclasses

- For more resources and research
- To click links in these PowerPoint slide shows
- To click links in printed handouts
- For more critical thinking practice
- Look for
  - Internet Safety Basics
  - Fake News: How to Detect it

in the green sidebar shown here: