Online Privacy
Concepts and Tools

Rob Caluori
Director of IT, Westchester Library System

Prepared for WLS Board Meeting:
January 30, 2016
YOU
YOU
Risks    Tools    Action
• The “Cloud”
  • There is no magical cloud
  • The cloud is made up of servers you just can’t see or touch

• Plain-text information (data) exchange
  • Via websites
  • Via one-to-one communications (email, SMS)
  • Via media (USB flash drives, CDs, etc)

• Search and browsing history and patterns

• Shared / generic passwords

• Malware / Ransomware / Spyware
• Private Cloud vs Public Cloud
• Securing Plain Text Information
  • Web Traffic – TOR Browser

• TOR – The Onion Router
  • Provides privacy by hopping traffic through anonymous proxies.
  • Three proxy system, an Entrance Relay, Middle Relay and an Exit Relay
  • All traffic (including the URLs and headers) is encrypted except the final exit
How Tor Works: 2

Step 2: Alice’s Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
• Securing Plain Text Information
  • Files and Emails – GPG / PGP

  • GPG (GNU Privacy Guard) / PGP (Pretty Good Privacy)
    • Public key locks the data, Private key unlocks it
  • Encrypt file for transport over the Internet or on media
  • Encrypt text of an email
    • Remember subjects are still in plain text
• Shared / generic passwords
  • Single / Same Sign-on (SSO) systems help reduce usernames and passwords
  • Password sharing tools to control access to a shared password (LastPass)

• Search and browsing history and patterns
  • Privacy-friendly search engines (DuckDuckGo, Disconnect Search, StartPage)
  • Privacy / Incognito mode – use with caution

• Malware / Ransomware / Spyware
  • Malware - Malwarebytes
  • Ransomware - System snapshots / Backups – Make your PC disposable
  • Anti-virus – Keep it up to date!
• Providing tools to patrons
  • Choice of browsers including TOR Browser
  • Kleopatra / GPA
  • Default search engine to Disconnect, DuckDuckGo, StartPage
• Providing training on privacy tools / digital literacy to library staff
• Supporting TOR – Setting up a “significant” relay
• Securing PCs to protect resources
• Implementing SSO whenever possible