Good Computing Practices

Alan J. Raul
alan@alanraul.com
SLO Bytes Presentation
October 4, 2020

1. Router Security
    a. https://routersecurity.org/
    b. Secure your Wi-Fi
2. Use a VPN (Virtual Private Network)
    a. https://en.wikipedia.org/wiki/Virtual_private_network
    b. Private Internet Access
        i. https://www.privateinternetaccess.com/
3. Use a Ad Blocker
    a. AdBlock
        i. https://getadblock.com/
4. Use a Password Manager
    a. LastPass
        i. https://www.lastpass.com/
    b. DO NOT include e-mail, bank or government passwords in your password manager
5. Create a “disaster recovery plan”
6. Separate your Operating System from your DATA by partitioning
    a. Use the Windows built-in partition tool or a third-party tool
    b. Acronis Disk Director
        i. https://www.acronis.com/en-us/personal/disk-manager/
    c. GNOME Partition Editor
        i. https://gparted.org/
    d. Parted Magic
        i. https://partedmagic.com/
7. Backup Types
    a. Operating system backup
        i. This includes the OS installed, updated, configured, programs installed and configured.
        ii. The OS and applications are activated
    b. Data backup
        i. This includes data which you have created which cannot easily, if at all, be recreated.
            1. Pictures, music, videos, Word or Excel documents and more

8. Backup Software
    a. Acronis True Image
        i. https://www.acronis.com/en-us/personal/computer-backup/
    b. Macrium Reflect 7 Free Edition
        i. https://www.macrium.com/reflectfree
    c. 2BrightSparks SyncBackFree
        i. https://www.2brightsparks.com/freeware/index.html
9. Backup locations
    a. On-site
        i. Preferably a Fireproof box or safe
    b. Off-site
        i. Safety deposit box
        ii. A trusted friend or relative
        iii. Online backup service
10. Backup devices
    a. External hard drive enclosure
    b. USB flash drive
    c. NAS (Network Attached Storage)

Miscellaneous Good Computing Practices

- Keep software and programs up to date – In other words DO NOT use Windows 7 and/or Office 2010!
- Enable Automatic Updates
- Keep Windows Defender updated
    - Install Malwarebytes if needed (FREE or Paid version)
        - https://www.malwarebytes.com/mwb-download/
- Be suspicious of external downloads and emails
    - Keep an eye on the news for security incidents.
    - Beware of scams
    - Do not install or download unknown or unsolicited programs/apps to your computer, phone, or other devices.
- **An advantage of being a paid SLO Bytes member is that we share information on the latest security incidents, Windows updates and application updates.**
- Wipe data from old technology completely
- There is probably more I could list but this should hit the main points.