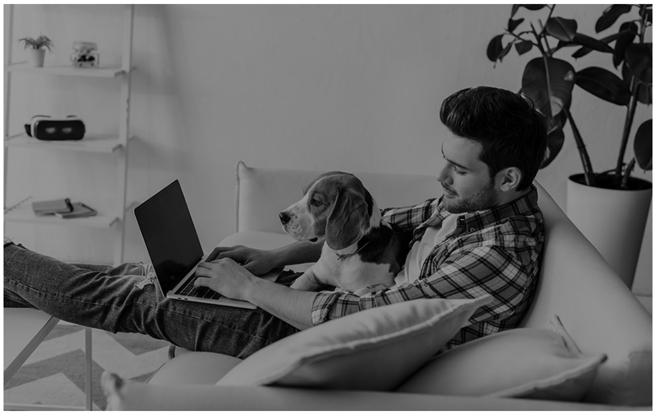
CENTRIWORKS

Personal Cybersecurity Tips

TOP 6 SECURITY PRACTICES FOR YOUR PERSONAL COMPUTING



Here are a few items that may make your life better and a little less susceptible to being taken advantage of by bad actors. These good security practices can save you a lot of trouble when things go bad. We hope this helps and if you have any questions please reach out to us.

1. USE ANTIVIRUS AND ANTIMALWARE SOFTWARE ON YOUR COMPUTER.

- BitDefender is better than nothing and these days it is rated among the best.
- Malware Bytes works wonders.

2. SECURE YOUR EMAIL ACCOUNT(S) AND USE A PASSWORD MANAGER

- Use a different password for all your accounts
- Track and create good passwords in a password manager like Dashlane, Keeper, LogMeOnce or Lastpass.
- If you use any of the major email providers (Gmail, Yahoo, etc.) at a minimum, set them up to use MFA (Multifactor Authentication). If you want encrypted email setup a Proton mail account. There are a few MFA option types so be aware.
  - ***Good*** - SMS-text a code to your phone each time you login.
  - ***Better*** – send a code via an application on your phone.
  - ***Best*** – FIDO U2F based. You have to carry a security key like Google's Titan, Yubico's YubiKey, Thetis security key or CryptoTrust's OnlyKey.

3. PATCH YOUR COMPUTER

- For Microsoft users, every second Tuesday of each month is when the latest patches come out. Set a schedule and do it or just automate the process.
- Don't forget your drivers. DriverEasy makes updating drivers a breeze.
- For Apple users, it's done very secretively in the background. It's just the way they are.
- For Linux, it can be automated in some distributions or run apt regularly.

4. PATCH YOUR SOFTWARE

- Don't forget your application software.
- Office365 will usually ask to be patched when it needs patching.
- Sometimes Adobe and some of the bigger application providers will have popups tell you when a patch is available.
- Other third-party applications can be patched with PDQ Deploy or Ninite Pro.

5. SECURE YOUR WIFI

- Change your SSID – “FBI Listening Post” is always a good one, or maybe “It’s a Trap”
- Change the admin password for your WiFi router. Everyone has the list of default admin passwords.
- Use WPA2-PSK with AES encryption if possible, for home use.
- Change the Passphrase. The longer the better. Something like *drivE4llamAasF@stasy0uC4n!* the phrase is “Drive a llama as fast as you can!” There are limits to the number of characters in most routers but the more complex and longer, the harder it will be to capture and decode the key.

6. BACKUP YOUR IMPORTANT FILES AND IMAGE YOUR DRIVE IF YOU WANT AN EASY RECOVERY FROM RANSOMWARE OR AN OLD FASHIONED DRIVE CRASH.

- Don’t just use a file syncing tool as a backup because if a file gets corrupted on your PC, it will sync the corruption to the copy in the cloud.
- Software that can help.

EFFECTIVE CYBERSECURITY STARTS WITH A PROACTIVE STRATEGY.

These are some very basic personal cybersecurity tips. If you find yourself needing help navigating cybersecurity solutions for your business or organization, please reach out to us, we can help. Since 1964, Centriworks has been East Tennessee’s locally owned, nationally recognized business technology leader.

From identifying network security threats to data protection, web/email security and data encryption—we’ll help you develop and implement the right solutions to keep your data safe, secure and private. We’ll provide a cybersecurity program to deliver multi-layer protection, detect vulnerabilities, and protect your most critical business information.

We seek to identify potential threats that could be posed and take proactive measures of prevention, prioritizing security risks before they become a problem. Contact us today.