Cyber Security 101 Action Sheet

- **Firewalls:** Most ISP's (Internet Service Providers) like Frontier, Suddenlink and others, provide a Modem/Router that is usually set in a factory standard configuration with default username and passwords. In addition, they are never updated once they go on line. Security of your network is not their primary concern so most are not configured correctly and many are already hackable with known exploits. They can be configured to adequately protect your home networks, however when it comes to protecting a business they are often inadequate.
  You want to look for UTM (Unified Threat Management) firewalls that have logging, Anti-Virus, Intrusion Detection and prevention, NAT (Network Address Translation), VPN (Virtual Private Networking) and other more advanced technologies. Here are some of the leading small business firewalls:

  SonicWall, Sophos, Watchguard, Checkpoint, Fortinet, Cyberoam, Cisco, Astaro

- **Anti-Spam:** Spam filters will block unwanted mail and attachments from ever getting to your in box. They often use sophisticated math to determine what to block based on the millions of emails that pass through them. You have the ability to fully configure your individual tastes and "white list" senders that you always trust. They have the ability to learn as time goes on. In addition they often send you an email with all the crap that was caught and give you a chance to quickly view and accept or reject mail to insure you don't miss anything important.

- **Automated Backups:** If you manually backup your data to an external drive then (unless you are the exception) you will occasionally forget to do it or put it off. This can be a costly mistake. Your data should be backed up at least daily using an automatic backup routine. The backups should go to a local drive in your office and also go off site somehow. The business class backup software suites will encrypt your data and allow for "versioning." This means that you should be able to recover files or a database as it was going back several weeks. To properly protect your data, do not do a simple overwrite of the last backup. If a file is corrupted, you will back up the corrupted file. Examples for consumer grade:

  Carbonite, myPC Backup, Mozy, CrashPlan, OneDrive

- **Site wide Anti-Virus (AV):** For a business, it is best practice to have one standard AV solution running on all the workstations and laptops. Some of the vendors provide a central control panel to ensure that all the computers are updated and functional. Malware often attempts to disable AV software so it can do whatever it wants. You

P.O. Box 1047 Elkins, WV 26241
PH 304.614.0186
info@mitecwv.com

need to know if the AV is working. Free solutions work, however the best features you need to pay for. Examples of good AV protection:

Webroot, Bitdefender, Trend Micro

- **Malwarebytes:** A free malware scanner that you update and run manually, however it is the industry standard for scanning, detecting and removing troublesome infections.

  Malwarebytes.org/antimalware/

- **Run as User and not Administrator:** If you run your computers on a daily basis as "Administrator" then malware and viruses along with rogue websites and other code will run under your rights and immediately install. Running as admin on a daily basis is now considered very risky. If you are running as Admin, then go to control panel/users and create another user with admin rights and assign a password. Go to your normal account and drop it to "user" status. If you need to load something or update a program, your computer will prompt you for the admin password. If you are going about your normal work on the computer and the notice pops up, you have the chance to cancel the install if you wish.

- **Ad Blockers:** Although controversial with some websites, using an ad blocker such as "Ad Block Pro" will go a long way towards increasing security from rogue and malicious programs on websites trying to run code on your computer. You will see faster page loads and use less bandwidth on mobile devices.

  https://adblockplus.org/

- **Password Managers:** Let's face it… Passwords are a hassle and many of us use the same password for nearly everything. Trouble is, if someone gets or guesses that password then they can actually assume our identity and lock us out of our digital lives. A password manager such as "LastPass" allows you to store all your passwords in one place, encrypts them and allows you to transfer your encrypted passwords to any device you use. Best of all, you can use LastPass to automatically generate a complex password for your banking and business websites and it will remember them for you. All you need to remember is one password (and don't forget it) and LastPass will automatically load your username and password for any site you tell it to remember. This program has been vetted by some of the best crypto and security professionals out there.

  https://lastpass.com

- **DNS Service:** DNS (Domain Name Service) is the phone book of the internet. Computers are not human beings. We can remember names like "Yahoo" or "Google." But computers are binary, they understand numbers. So when we type "Google.com"

P.O. Box 1047 Elkins, WV 26241
PH 304.614.0186
info@mitecwv.com

into a browser, it checks with a DNS server that tells your browser where to find Google. In this case it is 74.125.226.38. Good thing we don't have to remember those numbers for every website!

DNS operates behind the scenes and most people don't ever think about it, it is automatic. Your DNS servers are usually supplied by your ISP. Unfortunately, DNS was never intended to be secure and can easily be hijacked. You may want to go to www.bankofamerica.com and you may get www.banksofamerica.com which may be a fake website that captures your logon and password information. Notice only one letter difference? Remember to always look for the https:// and the padlock symbol when conducting financial business and purchases online.

Consider programming your computers or routers to use a safer DNS server like:

Norton ConnectSafe, Comodo Secure DNS, Open DNS

- **Lock down Wi-Fi and add guest access:** Most home and business routers provided by your ISP come with Wi-Fi enabled. A majority of the devices on the internet today connect via wireless. This is very convenient for most of us and we now expect wireless connections in our homes and businesses. The ISP's and vendors who sell all this wireless "stuff" are primarily interested in the sale and not your security. They want you to just plug something in and have it work. Great, you say! But… do yourself a favor and change the administrator password. Then setup a secure SSID (the name broadcast by your wifi router) Use the option for 256bit AES Encryption and disable the ability to configure your router from the internet.
  After that, if your router has the ability, create a "guest" account and give it a password. This would be the password you hand out to friends and visitors.

- **Drive images:** So you have a computer that is running great, just the way you want it. Do yourself a favor and "clone" the drive. What this does is create a complete backup of EVERYTHING including programs, data, and settings and creates a full point in time backup of your computer. Now if your computer gets really messed up, you can recover the entire machine as it was the day you made your image. This will save countless hours and a lot of money. Disk images should be a part of your backup strategy. You only need a full image every so often. Use a good automated backup program to grab all your important stuff daily or hourly to an external drive and the cloud. Some free and paid versions of imaging software are:
  Acronis True Image, Clonezilla, Macrium Reflect, DriveImage XML, Paragon

- **VPN Service for on the road:** We all travel and when we do there are a lot of open Wi-Fi hotspots in café's, hotels, airports and restaurants. Now if your kids want to use it to play games or watch movies on their own devices they may be ok. However, if you plan

P.O. Box 1047 Elkins, WV 26241
PH 304.614.0186
info@mitecwv.com

to check your mail, do some banking or log into your workplace or applications, you are taking a huge risk. What basically happens with a VPN service is you load a bit of software on your device that encrypts your connection. Then you can choose where to "appear" on the Internet. This could be a city near you, across the country or around the world. The service will have servers in various locations around the world and will encrypt all your traffic between your device and their servers. This allows you to use public hot spots with a high degree of confidence knowing that nobody can "sniff" your passwords and data stream. You can also hide from your ISP who may be watching your activity and throttle your bandwidth based on where you go. (yes they can do this).
Look for services that do not keep logs of your activity on their servers. Two good ones are:

ProXPN and PIA (Private Internet Access)

For further information read this article http://www.howtogeek.com/221929/how-to-choose-the-best-vpn-service-for-your-needs/

- **2FA (2 Factor Authentication) :** Facebook and some other social media providers are starting to provide Two Factor Authentication. This usually involves you logging in with a username and password then waiting for a quick SMS text on your phone with a one-time code to enter. Other websites like banks can do this or they provide a key fob that you press to get a number that is generated. The whole idea is to make logging in to your sensitive stuff harder or near impossible for hackers. It relies on something you know and something you have.
  If you have the option to use 2FA, then by all means do it. Make sure that if your phone number changes, you update your 2FA settings.

- **Email or Text Alerts:** Most banks and credit cards give you the ability to monitor your accounts via sending a text or email to you whenever you make a purchase, change your password, go over your limit and other important information. TURN THIS FEATURE ON AND USE IT!
  If your bank does not offer this service, find one that does and move your account there.

P.O. Box 1047 Elkins, WV 26241
PH 304.614.0186
info@mitecwv.com