

Cyber Tips

- 1) Think before you click on a link or open an attachment, become a human firewall and question every email.
- 2) Intrusion Detection Systems are a must but they will not stop everything as virus writers write in excess of 50,000 new viruses a day.
- 3) Separate passwords for mission critical accounts.
- 4) Strong passwords need to be longer than twelve characters in length with capital and lower case letters, numbers and a special symbol and NO dictionary words. Think passphrase instead of password.
- 5) Updated operating systems are a must as Microsoft doesn't support XP anymore.
- 6) Patch your system, Microsoft updates, java and adobe. www.secunia.com
- 7) Multifactor authentication is a must on Facebook, LinkedIn, Outlook 365, Gmail, LogMeIn, VPNs and financial accounts when offered. www.twofactorauth.org
- 8) Consider a separate computer for critical business functions. If you can access your client records on a computer that is used for Facebook and personal web surfing you are putting yourself at risk. If you are gaining remote access to your company and you are using a home computer that you share with your kids, you are putting your organization at great risk.
- 9) Do not surf the Internet as the Administrator on a computer. If you purchase a computer and you are the only user, chances are you are the administrator. Go to the control panel and create a new profile and give it administrator access and change your profile to regular user.
- 10) Back up your mission critical files on a daily basis. There have been numerous cases of ransomware that turns a company's critical data into useless information unless you send \$500 in bitcoin to a bad guy in Eastern Europe.
- 11) Have a plan for your organization, <https://transition.fcc.gov/cyber/cyberplanner.pdf>
- 12) Practice smart online banking <http://krebsonsecurity.com/online-banking-best-practices-for-businesses/>
- 13) Don't store your password in the browser, its the same as leaving your keys in the car for ease and convenience.
- 14) If you can access your information in the cloud and all you have is a password, be prepared for the info to be stolen. Use multifactor.
- 15) Once the bad guys get your stuff.....it's usually too late.
- 16) You need to have a strong password for your smart phone and if you are using an Android, consider an intrusion security suite.