Cyber Security Tips

1. **Institute a good privacy policy.**
   Make protecting sensitive data a part of the company culture. Train employees in security principles and communicate the policies on a regular basis. Establish rules of behavior describing how to handle and protect customer information and other vital data. Security policies -- especially regarding the use of social media -- are vital.

2. **Identify sensitive information/ Isolate and segregate sensitive data**
   Inventory your potentially sensitive information (e.g., client info, credit card info, investments) and document on which computers, servers and laptops it's stored. Keep sensitive data on the fewest number of computers or serves, and be sure to segregate it from the rest of your data and network if possible. Limit employee access to data and information. Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs. Regularly backup the data on every computer used in your business, your Smartphones too.

3. **Encrypt, encrypt, encrypt!**
   Encrypt laptops and portable drives and backups. Encrypt data in motion. Encrypted data is considered secure.

4. **Keep anti-virus and anti-spy ware software up to date.**
   Most offices have anti-virus software in place, but forget or neglect to make sure it is running the latest version or the latest updates, which can open them up to all types of data security breaches.

5. **Install software updates for your operating systems and applications as they become available.** Vulnerabilities in software are constantly being discovered and they don't discriminate by vendor or platform. All operating system vendors regularly provide patches and updates to their products to correct security problems and improve functionality.

6. **Make sure you only download applications that come from reliable sources.**
   Because applications (e.g., games, mobile apps) may contain viruses, spy ware or Trojan horses, it's important to know and trust the source of an application; and limit authority to install software.

7. **Require individual user accounts for each employee**
   Set up a separate account for each individual and require that strong passwords be used for each account. Change passwords at least every three months. Administrative privileges should only be given to IT staff and key personnel. Password your Smartphones too.

8. **Provide firewall security for your internet connection**
   Install and maintain a professional grade firewall between your internal network and the internet. This pertains to computers used at home for business too.

9. **Secure your Wi-Fi networks**
   If you have a Wi-Fi network for your workplace make sure it is secure, hidden and it does not broadcast the network name. Turn on the encryption so that passwords are required for access. WEP is not acceptable – use WPA2. Change the default administrative password.

10. **Secure your browser**
    Known, legitimate websites are frequently being compromised and implanted with malicious JavaScript that foists malware onto visitors' computers. Disable JavaScript for all but the most essential of sites -- such as your banking or regular ecommerce sites. Employ web filtering that offers malware and botnet protection.

11. **Take control of your email**
    Avoid opening email attachments received unexpectedly – no matter who appears to have sent it. Make sure your email client isn't left open to infection. Reading email in plain text offers important security benefits that more than offset the loss of pretty colored fonts.

12. **Control physical access to your computers and network components**
    Prevent access or use of business computers by unauthorized individuals. Laptops and mobile devices can be particularly easy targets for theft, so make sure they are encrypted. When not attended, they should be stored and locked up. Lock filing cabinets and rooms where you keep sensitive data. Configure your smartphone to allow for a remote wipe of data in the event the device is lost or stolen.

13. **Keep abreast of Internet scams**
    Criminals think of clever ways to separate you from your hard earned cash. Don't get fooled by emails telling sad stories, or making unsolicited job offers, or promising lotto winnings. Likewise, beware of email masquerading as a security concern from your bank or other ecommerce site.

14. **Outsource security**
    Hire a consultant to make sure your business is safe and secure. You can outsource vulnerability management, patch management, firewall management, intrusion testing, and compliance management. Qualified managed security service can provide better security than you…and do so at a lower cost, while allowing your IT staff to concentrate on the business of maintaining your networking and hardware needs.