

17 Things you can do at work and home to protect yourself and your company.

- 1. Backup your data! Use encryption with confidential data on laptops**
- 2. Change your passwords, make them strong, unique, private, use Last Pass**
- 3. Keep Anti-Virus, Operating System, Flash & Java up to date**
- 4. Configure Anti-Virus to scan anything plugged in to your computer**
- 5. Lock or logoff your computer**
- 6. Never e-mail work products to your personal email account**
- 7. Never use Flash Drives you “found” or ones given to you. Buy and use brand names only**
- 8. Smartphones: Beware of the apps you use. Delete the ones you don’t use**
- 9. Smartphones: Use biometrics & strong passwords. Wipe before discarding them**
- 10. Never use public USB charging stations- Always use your own charger**
- 11. Beware of phone scams – “I’m from the Help Desk, Microsoft, the IRS, your bank....”**
- 12. Always convert sensitive files to PDF before sending them to strip out metadata**
- 13. Only use secure portals (https://) when transmitting personal information**
- 14. Never use “free” music/video sharing sites**
- 15. Protect your wireless networks with passwords**
- 16. Beware of unsolicited links or attachments. Never open a link or attachment unless you are ABSOLUTELY sure it is safe. Report anything that is suspicious – DO NOT CLICK ON IT!**
- 17. Check your bank accounts daily / credit cards at least monthly, Freeze your credit reports**

