# Steps To Increase Technology Security Practices In Your Organization

1. **Use alphanumeric passwords and change them frequently.**
   Alphanumeric passwords are a combination of upper and lower case letters, numbers, and symbols. Avoid using pet names, birthdays, or words in a dictionary. Do not automatically save your passwords to access your computer or email. Do change passwords frequently and keep them safe. Please do not keep passwords under the keyboard, taped to the monitor, or in your unlocked top desk drawer! **Use passwords to prevent access to your:**

   A. **Computers:** In addition to typing in a user name and password when you first turn on your computer, set your computer to revert to a password-protected screensaver if you leave it for several minutes. In Windows, you can go to: *Control Panel > Display > Screen Saver* tab and check to box to "*password protect.*"

   B. **Phone voicemail:** Remember, if you don't change the default password, anyone might call and access your work voicemail.

   C. **Cell phone or PDA (e.g. Blackberry, Palm):** You can set the phone screen to default to a password if your device is not in use for a time (5, 10, 20 minutes). Also, if you lose it, the contents are password-protected even if someone tries to sync your device. Check your phone menu for settings and security options.

   D. **Email programs:** Just like with web-based email accounts, you can prevent people from even opening your computer email programs (like Outlook Express) if you require a password to access an email identity. For example, to password protect Outlook Express, go to: http://email.about.com/od/outlookexpresstips/qt/et122504.htm

2. **Secure office and home wireless networks.**
   Use strong encryption and be sure to password-protect access to your wireless network. Then, all computers (including office visitors or people lurking in the hallway) will need a password to use your wireless network. Have staff secure home wireless networks before taking work home with them. For tips, search online for: "secure wireless networks."

3. **Update operating systems regularly.**
   Regularly download all the latest patches and updates for the operating systems on your computer (Windows, Mac) or PDA (blackberry, palm). Some systems can be set to automatically check for updates. If your automatic feature is not turned on, check for updates weekly. For example, check Windows Updates at: http://www.microsoft.com

4. **Use firewalls and check to see if they are enabled.**
   Firewalls help protect your computer and PDA against network attacks from the Internet or other computers. For Windows machines, a Windows Firewall is often found via the Control Panel or you can use Windows Firewall Check (see: http://technet.microsoft.com/en-us/library/bb926071.aspx). Once your firewall is on, you may need to configure it (change its settings) to allow certain programs like web browsers to access to the Internet. On Windows computers, this won't likely effect Microsoft products like Internet Explorer but may impact other programs. For example, see tips for Mozilla Firefox, at: http://support.mozilla.com/kb/Configuring+Windows+Firewall.

5. **Use antivirus software and keep the anti-virus definitions updated.**
   If your organization has not already purchased and loaded a standard anti-virus software like Symantec (www.symantec.com) or Mcafee (www.mcafee.com/anti-virus/default.asp), you can download free programs such as AVG (http://free.grisoft.com) or you can run a online scan using Bit Defender at: http://www.bitdefender.com/scan8/ie.html.

6. **If you use a laptop, consider purchasing a screen privacy filter.**
   A screen filter or a privacy filter is a plastic screen that slides right over your laptop screen. This filter prevents someone sitting next to you from easily reading what's on your laptop while you're sitting on the train or in a café.

7. **Keep any confidential information about victims in password-protected databases or files and on password-protected computers that are not connected to the Internet.**
   Even with passwords, firewalls, updated operating system patches, and anti-virus scans, if a computer is connected to the internet, any victim data on it is still vulnerable to hackers. To disconnect a computer from the Internet, remember not only to unplug your Ethernet cord but also to disable your wireless network card.

8. **Refrain from keeping victim email addresses in your computer or email address books.**
   In addition, if you send/receive an email to/from a survivor, print them out if you need to and then delete those emails as soon as possible. Take a day to clean out your email files, at least once a month or once a quarter. Certain viruses target email and email address books.

9. **When sending sensitive or confidential information about a survivor, call ahead to ensure your fax is getting to the appropriate person.**
   Get the survivor's informed consent and remove any unnecessary or revealing information (such as the header identifying what number the fax originally came from) before sending it on or filing it in your office. Call to make sure the person receiving the fax knows it is coming. Also block caller ID on fax lines when possible.

10. **When calling survivors, use line blocking to hide caller ID.**
    When calling back a survivor from the office phone, cell phone, or home phone, find out whether or not to use Caller ID Blocking. Unless a survivor tells you otherwise, staff and volunteers who make work calls from work or home, should either have caller ID line blocking or make sure to block each outgoing call made to victims.